Mathe-Trainer

Carlos Camino

cfcamino@gmail.com

www.carlos-camino.de/projekte

Hallo!

Diese Datei enthält eine bunte Mischung aus allen Folien, die ich während meiner Zeit als Tutor an der TU München in den Tutorien benutzt habe. Sie enthalten einige Definitionen und Sätze aus den verschiedenen Mathematik-Vorlesungen für Informatiker kleine Übungsaufgaben und viele Beispiele.

Konstruktive Kritik, Ideen, Kommentare und Fehlermeldungen sind jederzeit herzlichst willkommen. Einfach per E-Mail an `cfcamino@gmail.com`.

Frohes Durchklicken!

Carlos

Themenübersicht

Themenübersicht

Themenübersicht

Mengen

Unter einer Menge verstehen wir jede Zusammenfassung von bestimmten wohl-unterschiedenen Objekten. Wichtig ist:

- Es werden geschweifte Klammern benutzt: $\{\ldots\}$.
- Elemente werden durch Kommas getrennt.
- Die Reihenfolge der Elemente ist irrelevant.
- Die Anzahl an Kopien desselben Elements ist irrelevant.
- Die Elemente einer Menge können beliebige Objekte sein, z.B. auch Mengen.

Beispiele

- Die Menge $\{1, 2, 3\}$ enthält die Elemente 1, 2 und 3. Außerdem gilt beispielsweise auch $A = \{2, 3, 1\}$ und $A = \{1, 2, 1, 3, 2, 1\}$.
- Die Menge $\{1, \{2, 3\}\}$ enthält zwei Elemente: die Zahl 1 und die Menge $\{2, 3\}$.
- Die Menge $\{\}$ enthält kein Element.

Info: Für die leere Menge benutzt man das Zeichen $\emptyset$. Es gilt $\emptyset = \{\}$.

Elementrelation

x ist Element von A (in Zeichen: $x \in A$), falls x in A enthalten ist. Falls x kein Element von A ist, dann schreibt man $x \notin A$.

Beispiel

- Es gilt $2 \in \{1, 2, 3\}$, aber $4 \notin \{1, 2, 3\}$.
- Es gilt $\{2, 3\} \in \{1, \{2, 3\}\}$, aber $2 \notin \{1, \{2, 3\}\}$ und $3 \notin \{1, \{2, 3\}\}$.
- Für jedes x gilt $x \notin \emptyset$.

Inklusion

A ist Teilmenge von B (in Zeichen: $A \subseteq B$), falls jedes Element aus A in B enthalten ist. B wird oft termObermenge von A gennant. Falls A keine Teilmenge von B ist, dann schreibt man $A \nsubseteq B$.

Beispiel

- Es gilt $\{\} \subseteq \{1,2,3\}$, $\{1,3\} \subseteq \{1,2,3\}$ und $\{1,2,3\} \subseteq \{1,2,3\}$, aber $\{3,4\} \not\subseteq \{1,2,3\}$.
- Es gilt $\{\} \subseteq \{1,\{2,3\}\}$, $\{1,3\} \subseteq \{1,\{2,3\}\}$ und $\{1,2,3\} \subseteq \{1,\{2,3\}\}$, aber $\{3,4\} \not\subseteq \{1,\{2,3\}\}$.
- Es gilt $\emptyset \subseteq \emptyset$. Für jede andere Menge X gilt $X \not\subseteq \emptyset$.

Mengengleichheit

Die Mengen A und B sind gleich (in Zeichen: $A = B$), falls $A \subseteq B$ und $B \subseteq A$ gelten. Falls A und B icht gleich sind, dann schreibt man $A \neq B$.

Beispiel

Es gilt $\{1, 2, 3\} = \{1, 2, 3\}$, aber $\{2, 3, 4\} \neq \{1, 2, 3\}$.

Echte Inklusion

A ist eine echte Teilmenge von B (in Zeichen: $A \subset B$), falls $A \subseteq B$ und $B \nsubseteq A$ gelten. B wird ann echte Obermenge von A gennant.

Beispiel

Es gilt $\{1, 3\} \subset \{1, 2, 3\}$, aber $\{1, 2, 3\} \not\subset \{1, 2, 3\}$.

Info

In vielen Vorlesungen und Büchern wird das Zeichen $\subset$ für die normale Inklusion benutzt. In solchen Fällen wird die echte Inklusion mit $\subsetneq$ oder $\subsetneqq$ notiert.

Kardinalität

Die Kardinalität oder Mächtigkeit $|A|$ einer Menge A gibt die Anzahl der Elemente in A an. Falls die Anzahl an Elementen in A unendlich ist, dann schreibt man $|A| = \infty$.

Alternative Schreibweisen für $|A|$ sind: $\text{card}(A)$, $\#(A)$, $n(A)$ und $\overline{\overline{A}}$.

Beispiele

Es gilt $|\{3,4,5\}| = 3$, $|\{\{2\},\{3,4,5\}\}| = 2$, $|\{\}| = 0$ und $|\{\{\}\}| = 1$.

Quizfrage

Sei A eine Menge mit

$$A = \{a, 6, \{3, c, \{4, 1\}\}, \{\{\}\}, 6, \{b, d, 5\}\}.$$

Welche Kardinalität $|A|$ besitzt A?

$$|A| = \left| \left\{ \underbrace{a}_{1}, \underbrace{6}_{2}, \underbrace{\{3, c, \{4, 1\}\}}_{3}, \underbrace{\{\{\}\}}_{4}, \not{\emptyset}, \underbrace{\{b, d, 5\}}_{5} \right\} \right| = 5$$

Extensionale Schreibweise

Man zählt die Elemente der Menge explizit auf:

$$A = \{x_1, x_2, x_3, x_4, \ldots\}.$$

Die extensionale Schreibweise ist eigentlich nur für endliche Mengen möglich. Wir benutzen sie aber auch für unendliche Mengen und schreiben „...“ wenn es ersichtlich ist, was damit gemeint ist.

Intensionale Schreibweise

Man kann Mengen auch durch diejenigen Elemente beschreiben, die eine Eigenschaft P haben. Die Menge

$$A = \{x \mid P(x)\}$$

enthält dann alle Elemente x, die die Aussage $P(x)$ erfüllen. Man schreibt oft auch $\{x \in U \mid P(x)\}$, um zu verdeutlichen, dass wir nur diejenigen Elemente aus der Menge U mit der Eigenschaft P betrachten.

Alternative Schreibweisen für $\{x \mid P(x)\}$ sind: $\{x : P(x)\}$ und $\{x \,;\, P(x)\}$.

Infos

- Für die intensionale Schreibweise kann man auch einen Doppelpunkt oder ein Semikolon als Trennzeichen benutzen. Folgende Darstellungen sind also gleichwertig:

$$\{x \in U \mid P(x)\}, \qquad \{x \in U : P(x)\}, \qquad \{x \in U ; P(x)\}.$$

  Ihr dürft natürlich alle drei Schreibweisen benutzen!

- Viele Mengen haben die Form

$$\{x \mid x = a(x_1, \ldots, x_k) \text{ für } x_1 \in A_1, \ldots, x_k \in A_k\},$$

  wobei $a(x_1, \ldots, x_k)$ ein mathematischer Ausdruck (eine Funktion) ist, welcher von den Parametern $x_1, \ldots, x_k$ abhängig ist. Für diese Mengen erlauben wir auch die Schreibweise:

$$\{a(x_1, \ldots, x_k) \mid x_1 \in A_1, \ldots, x_k \in A_k\}.$$

Beispiele

Folgende Mengen sind extensional definiert:

- Menge aller natürlichen Zahlen zwischen 11 und 15:

$$\{11, 12, 13, 14, 15\}.$$

- Menge aller Buchstaben des lateinischen Alphabets:

$$\{a, b, c, \ldots, z\}.$$

- Menge aller ungeraden Zahlen:

$$\{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, \ldots\}.$$

- Menge aller Zweierpotenzen:

$$\{1, 2, 4, 8, 16, 32, \ldots\}.$$

Beispiele

Dieselben Mengen können auch intensional wie folgt definiert werden:

- Menge aller natürlichen Zahlen zwischen 11 und 15:

$$\{x \in \mathbb{N} \mid 11 \leq x \leq 15\} \qquad \text{bzw.} \qquad \{10 + k \mid k \in [5]\}\,.$$

- Menge aller Buchstaben des lateinischen Alphabets:

$$\{x \mid x \text{ ist ein Buchstabe des lateinischen Alphabets}\}\,.$$

- Menge aller ungeraden Zahlen:

$$\{x \in \mathbb{Z} \mid x \text{ ungerade}\} \qquad \text{bzw.} \qquad \{2k + 1 \mid k \in \mathbb{Z}\}\,.$$

- Menge aller Zweierpotenzen:

$$\{x \in \mathbb{N} \mid x \text{ ist eine Zweierpotenz}\} \qquad \text{bzw.} \qquad \left\{2^k \,\middle|\, k \in \mathbb{N}_0\right\}.$$

Quizfragen

Wie sehen folgende Mengen in extensionaler Schreibweise aus?

1. $A = \left\{ n^2 \mid n \in [4]_0 \right\}$,
2. $B = \{|n-4| \mid n \in [5]\}$,
3. $C = \{n \in \mathbb{N} \mid |n-3| \leq 2\}$,
4. $D = \{n \in \mathbb{Z} \mid ||n-2| + |n+1|| = 5\}$,
5. $E = \{(-1)^n \mid n \in \mathbb{Z}\}$,
6. $F = \{i^n \mid n \in \mathbb{N}\}$.

Erinnerung: i ist die imaginäre Einheit. Für sie gilt: $i^2 = -1$.

1. $A = \{0^2, 1^2, 2^2, 3^2, 4^2\} = \{0, 1, 4, 9, 16\}$.
2. $C = \{|-3|, |-2|, |-1|, |0|, |1|\} = \{3, 2, 1, 0, 1\} = \{0, 1, 2, 3\}$.
3. $B = \{n \in \mathbb{Z} \mid -2 \leq n - 3 \leq 2\} = \{n \in \mathbb{Z} \mid 1 \leq n \leq 5\} = \{1, 2, 3, 4, 5\}$.
4. $D = \{-2, 3\}$.
5. $E = \{\ldots, -1, 1, -1, 1, -1, 1, -1, \ldots\} = \{-1, 1\}$.
6. $F = \{i, -1, -i, 1, i, -1, -i, 1, \ldots\} = \{i, -1, -i, 1\}$.

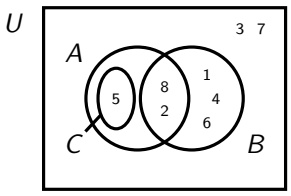
Graphische Darstellung von Mengen

Mengen und deren Beziehungen können mithilfe von Mengendiagrammen dargestellt werden. Das Universum U wird als Rechteck und die Mengen $A_1, \ldots, A_n$ als Kreise (bzw. Ovale) innerhalb des Rechtecks gezeichnet.

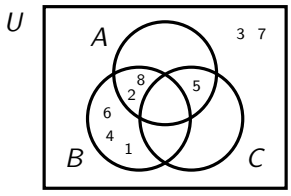
Bei Euler-Diagrammen werden nur die notwendigen Überlappungen der Flächen dargestellt. Bei Venn-Diagrammen dagegen werden alle möglichen Überlappungen eingezeichnet, selbst wenn einige davon leer bleiben.

Beispiel

Für $A = \{2, 5, 8\}$, $B = \{1, 2, 4, 6, 8\}$ und $C = \{5\}$ über $U = [8]$ erhält man:



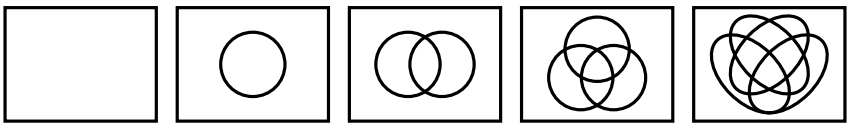
Euler-Diagram



Venn-Diagram

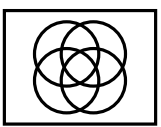
Info

Bei Euler-Diagrammen wird das Universum durch n Mengen in höchstens 2^n Bereichen aufgeteilt. Venn-Diagramme sind ein Spezialfall von Euler-Diagrammen, bei denen die Anzahl solcher Bereiche genau 2^n ist.



1 Bereich | 2 Bereiche | 4 Bereiche | 8 Bereiche | 16 Bereiche

Beispielsweise ist das Euler-Diagramm



kein Venn-Diagramm, weil die Anzahl der Bereiche 14 ist.

Potenzmenge

$\mathcal{P}(A)$ ist die Menge aller Teilmengen von A, d.h.:

$$\mathcal{P}(A) := \{X \mid X \subseteq A\}.$$

Alternative Schreibweisen für $\mathcal{P}(A)$ sind: $P(A)$, $\mathbb{P}(A)$, $\wp(A)$ und 2^A.

Beispiele

Es gilt:

$$
\begin{aligned}
\mathcal{P}(\emptyset) &= \{\emptyset\}, \\
\mathcal{P}(\{1\}) &= \{\emptyset, \{1\}\}, \\
\mathcal{P}(\{1,2\}) &= \{\emptyset, \{1\}, \{2\}, \{1,2\}\}, \\
\mathcal{P}(\{1,2,3\}) &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.
\end{aligned}
$$

Für jede endliche Menge A gilt: $|\mathcal{P}(A)| = 2^{|A|}$. Beispielsweise gilt für die Mengen aus der vorigen Folie:

$$\begin{array}{lcccl} |\mathcal{P}(\emptyset)| & = & 2^0 & = & 1, \\ |\mathcal{P}(\{1\})| & = & 2^1 & = & 2, \\ |\mathcal{P}(\{1,2\})| & = & 2^2 & = & 4, \\ |\mathcal{P}(\{1,2,3\})| & = & 2^3 & = & 8. \end{array}$$

Daher kommt die Schreibweise 2^A für die Potenzmenge von A. Mit ihr kann man sich die Regel $\left|2^A\right| = 2^{|A|}$ besser merken.

Wie viele Elemente enthalten folgende Mengen?

1. $\mathcal{P}([6])$,
2. $\mathcal{P}(\mathcal{P}([3]))$,
3. $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

Erinnerung: $[n] = \{1, 2, \ldots, n\}$.

Antworten

1. $|\mathcal{P}([6])| = 2^6 = 64$.
2. $|\mathcal{P}(\mathcal{P}([3]))| = 2^{2^3} = 2^8 = 256$.
3. $|\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))| = 2^{2^{2^0}} = 2^{2^1} = 2^2 = 4$.

Noch eine Quizfrage

Aus der letzten Quizfrage wissen wir, dass die Menge $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$ genau vier Elemente besitzt.

Welche sind das?

Es gilt:

$$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\mathcal{P}(\{\emptyset\})) = \mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$$

Die vier Elemente sind dann: $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$ und $\{\emptyset, \{\emptyset\}\}$.

Operationen

Die wichtigsten Operationen auf Mengen sind:

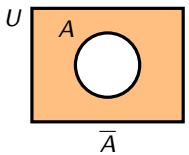
$\overline{A}$	$:=$	$\{x \in U \mid x \notin A\}$	(Komplement)
$A \cap B$	$:=$	$\{x \in U \mid x \in A \text{ und } x \in B\}$	(Schnitt)
$A \cup B$	$:=$	$\{x \in U \mid x \in A \text{ oder } x \in B\}$	(Vereinigung)
$A \setminus B$	$:=$	$\{x \in U \mid x \in A \text{ und } x \notin B\}$	(Differenz)
$A \triangle B$	$:=$	$\{x \in U \mid \text{entweder } x \in A \text{ oder } x \in B\}$	(symmetrische Differenz)

$\cap$ und $\cup$ sind assoziativ. Für mehrere Mengen schreiben wir:

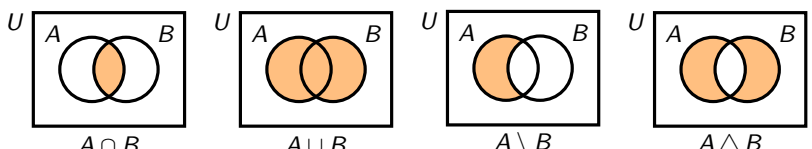
$$\bigcap_{i=1}^{n} A_i := A_1 \cap A_2 \cap \ldots \cap A_n, \qquad \bigcup_{i=1}^{n} A_i := A_1 \cup A_2 \cup \ldots \cup A_n.$$

Infos

- Man schreibt oft auch A^C oder A^0 statt $\overline{A}$ und $A - B$ statt $A \setminus B$.
- Die graphische Bedeutung des Komplements ist folgende:

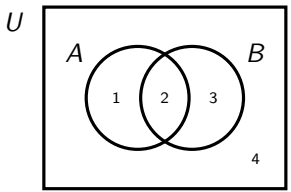


- Die graphische Bedeutung der zweistelligen Operationen $\cap$, $\cup$, $\setminus$ und $\triangle$ ist:



Beispiel

Seien $A = \{1, 2\}$ und $B = \{2, 3\}$ Mengen über dem Universum $U = [4]$.



Dann gilt:

$$
\begin{array}{lcll}
\overline{A} & = & \{x \in U \mid x \notin A\} & = \{3, 4\}, \\
A \cap B & = & \{x \in U \mid x \in A \text{ und } x \in B\} & = \{2\}, \\
A \cup B & = & \{x \in U \mid x \in A \text{ oder } x \in B\} & = \{1, 2, 3\}, \\
A \setminus B & = & \{x \in U \mid x \in A \text{ und } x \notin B\} & = \{1\}, \\
A \triangle B & = & \{x \in U \mid \text{entweder } x \in A \text{ oder } x \in B\} & = \{1, 3\}.
\end{array}
$$

Seien $A = \{1, 2, 3, 4\}$ und $B = \{3, 4, 5\}$ Mengen über dem Universum $U = [5]$. Was ist dann die Kardinalität folgender Mengen?

1. $\mathcal{P}((A \triangle B))$
2. $\mathcal{P}(\mathcal{P}(A \cap B))$
3. $\mathcal{P}(A) \cup \mathcal{P}(B)$

1. Es gilt:
$$|\mathcal{P}(A \triangle B)| = |\mathcal{P}(\{1,2,5\})| = 2^3 = 8.$$

2. Es gilt:
$$|\mathcal{P}(\mathcal{P}(A \cap B))| = 2^{|\mathcal{P}(\{3,4\})|} = 2^{2^2} = 16.$$

3. Die Mengen A und B haben genau 4 gemeinsame Teilmengen: $\emptyset$, $\{3\}$, $\{4\}$ und $\{3,4\}$. Diese sind sowohl in $\mathcal{P}(A)$ als auch in $\mathcal{P}(B)$ drin und dürfen daher nicht doppelt gezählt werden. Daraus folgt:
$$|\mathcal{P}(A) \cup \mathcal{P}(B)| = |\mathcal{P}(A)| + |\mathcal{P}(B)| - 4 = 2^{|A|} + 2^{|B|} - 4 = 2^4 + 2^3 - 4 = 20.$$

Disjunktheit

- Zwei Mengen Mengen A und B heißen disjunkt, falls sie keine Elemente gemeinsam haben, d.h. wenn gilt:
$$A \cap B = \emptyset.$$
- Eine beliebige Familie $A_1, \ldots, A_n$ von Mengen heißt disjunkt, falls die Mengen paarweise disjunkt sind, d.h. wenn für alle $i, j \in [n]$ mit $i \neq j$ gilt:
$$A_i \cap A_j = \emptyset.$$
- Für disjunkte Mengen $A_1, \ldots, A_n$ gilt:
$$|A_1 \cup \ldots \cup A_n| = |A_1| + \ldots + |A_n|.$$

Man schreibt auch $A_1 \uplus \ldots \uplus A_n$, um zu verdeutlichen, dass die Mengen $A_1, \ldots, A_n$ paarweise disjunkt sind.

Partitionen

Sei $k \in \mathbb{N}_0$. Eine k-Partition P einer Menge A ist eine Menge

$$P = \{A_1, \ldots, A_k\},$$

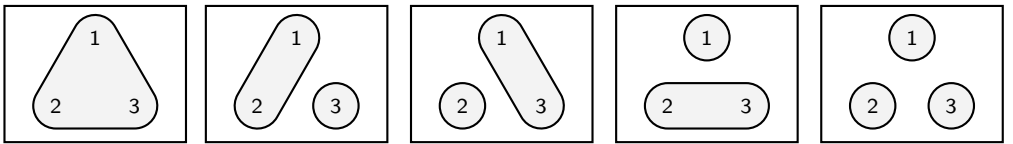
so dass $A = A_1 \cup \ldots \cup A_k$ gilt und die Mengen $A_1, \ldots, A_k$ alle nichtleer und paarweise disjunkt sind.

Infos

- Die Mengen $A_1, \ldots, A_k$ werden Partitionsklassen oder kurz Klassen genannt.
- Eine 2-Partition wird Bipartition genannt und eine 3-Partition Tripartition.
- Die einzige Partition P der leeren Menge $A = \emptyset$ ist die leere Partition $P = \{\}$.
- Die leere Partition ist die einzige 0-Partition.

Beispiel

Es gibt 5 verschiedene Partitionen der Menge [3]:



$P_1 = \{\{1,3,2\}\}$ $P_2 = \{\{1,2\},\{3\}\}$ $P_3 = \{\{1,3\},\{2\}\}$ $P_4 = \{\{1\},\{2,3\}\}$ $P_5 = \{\{1\},\{2\},\{3\}\}$

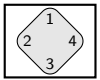
P_1 ist eine 1-Partition, P_2, P_3 und P_4 sind 2-Partitionen und P_5 ist eine 3-Partition.

Quizfrage

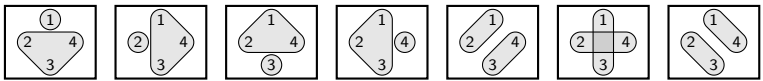
Wie viele verschiedene Partitionen besitzt die Menge $[4]$?

Es gibt 15 mögliche Partitionen der Menge [4]:

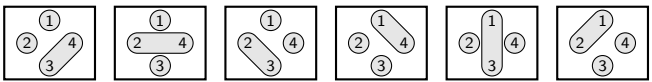
- eine 1-Partition,



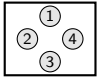
- sieben 2-Partitionen,



- sechs 3-Partitionen



- und eine 4-Partition.



Rezept

Frage: Wie kann eine Mengengleichung über beliebige Mengen $A_1, \ldots, A_n$ bewiesen oder widerlegt werden?
Methode:

1. Definiere Mengen $A_1, \ldots, A_n$ über einem Universum U, so dass im Venn-Diagramm jeder der 2^n Bereiche genau ein Element enthält.
2. Rechne linke und rechte Seite der Gleichung mit diesen Mengen aus und vergleiche die Ergebnisse.
3. Falls sie gleich sind, so wurde die Gleichung bewiesen. Sonst wurde ein Gegenbeispiel für die Gleichung gefunden.

Achtung!

Einige Dozenten/Übungsleiter erlauben diese Methode nur zum Widerlegen, aber nicht zum Beweisen. Wenn das bei euch der Fall ist, dann müsst ihr Mengengleichungen wie auf Folie 69 mit den Rechenregeln von Folie 67 beweisen.

Beispiel

Aufgabe: Beweise folgende Mengengleichung:

$$\overline{\overline{(A \cap B)} \cap \overline{(A \cap C)}} = A \cap (B \cup C).$$

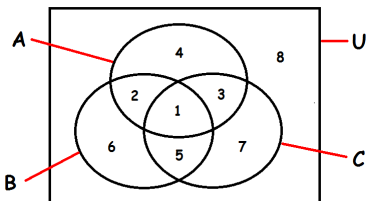
Lösung:

1. Definiere o.B.d.A. („ohne Beschränkung der Allgemeinheit“) Mengen

   $$A = \{1, 2, 3, 4\}, \qquad B = \{1, 2, 5, 6\}, \qquad C = \{1, 3, 5, 7\}$$

   über dem Universum $U = [8]$. Dies entspricht folgendem Venn-Diagramm:

Beispiel



Beispiel

2. Rechne:

$$\begin{aligned}\overline{\overline{(A \cap B)} \cap \overline{(A \cap C)}} &= \overline{\overline{\{1,2\}} \cap \overline{\{1,3\}}} \\ &= \overline{\{3,4,5,6,7,8\} \cap \{2,4,5,6,7,8\}} \\ &= \overline{\{4,5,6,7,8\}} \\ &= \{1,2,3\}\end{aligned}$$

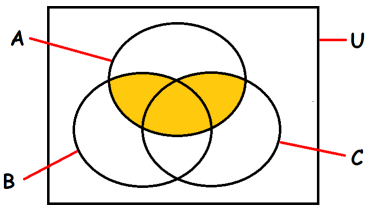
$$\begin{aligned}A \cap (B \cup C) &= \{1,2,3,4\} \cap (\{1,2,5,6\} \cup \{1,3,5,7\}) \\ &= \{1,2,3,4\} \cap \{1,2,3,5,6,7\} \\ &= \{1,2,3\}\end{aligned}$$

3. Wegen $\{1,2,3\} = \{1,2,3\}$ wurde die Mengengleichung bewiesen!

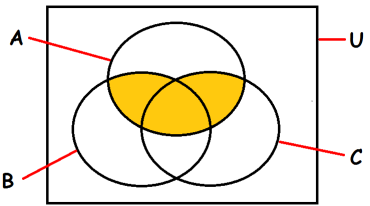
Wichtig!

Bitte nicht so:

„Die Gleichung gilt, weil die entsprechenden Venn-Diagramme gleich sind.“



$\overline{\overline{(A \cap B)} \cap \overline{(A \cap C)}}$



$A \cap (B \cup C)$

„Beweis durch schönes Bildchen“ ist kein Beweis!

Noch ein Beispiel

Aufgabe: Gilt die Mengengleichung

$$(B \cap C) \cup (A \setminus (B \cup C)) = A \cap (B \cup C)$$

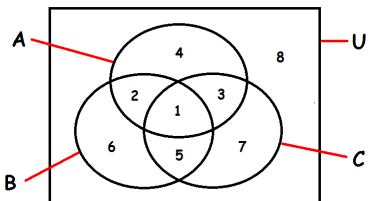
für beliebige Mengen A, B, C?
Lösung:

1. Definiere o.B.d.A. Mengen

$$A = \{1, 2, 3, 4\}, \qquad B = \{1, 2, 5, 6\}, \qquad C = \{1, 3, 5, 7\}$$

über dem Universum $U = [8]$. Dies entspricht folgendem Venn-Diagramm:

Noch ein Beispiel



Noch ein Beispiel

2. Rechne:

$$\begin{aligned}(B \cap C) \cup (A \setminus (B \cup C)) &= \{1,5\} \cup (\{1,2,3,4\} \setminus \{1,2,3,5,6,7\}) \\ &= \{1,5\} \cup \{4\} \\ &= \{1,4,5\}\end{aligned}$$

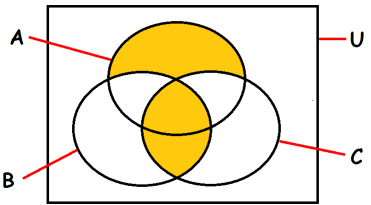
$$\begin{aligned}A \cap (B \cup C) &= \{1,2,3,4\} \cap (\{1,2,5,6\} \cup \{1,3,5,7\}) \\ &= \{1,2,3,4\} \cap \{1,2,3,5,6,7\} \\ &= \{1,2,3\}\end{aligned}$$

3. Wegen $\{1,4,5\} \neq \{1,2,3\}$ wurde die Mengengleichung durch Gegenbeispiel widerlegt.

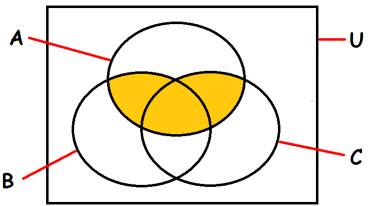
Wichtig!

Bitte nicht so:

„Die Gleichung gilt nicht, weil die entsprechende Venn-Diagramme ungleich sind.“



$(B \cap C) \cup (A \setminus (B \cup C))$



$A \cap (B \cup C)$

„Beweis durch schönes Bildchen“ ist auch hier kein Beweis!

Rezept

Frage: Was muss für Mengen $A_1, \ldots, A_n$ gelten, damit eine Mengengleichung stimmt?
Methode:

1. Führe die oben stehende Methode durch und bilde die symmetrische Differenz der Ergebnisse beider Seiten.
2. Entferne alle Elemente in der symmetrischen Differenz und interpretiere das Venn-Diagramm ohne die entsprechenden Bereiche.

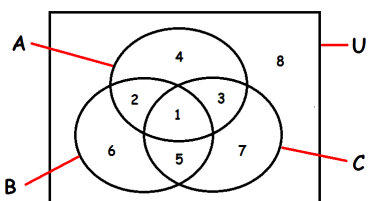
Beispiel (nochmal)

Aufgabe: Was muss für A, B, C gelten, damit die Mengengleichung

$$(B \cap C) \cup (A \setminus (B \cup C)) = A \cap (B \cup C)$$

stimmt?

Erinnerung: Im vorigen Beispiel erhielten wir für das Venn-Diagramm



die Ergebnisse $(B \cap C) \cup (A \setminus (B \cup C)) = \{1, 4, 5\}$ und $A \cap (B \cup C) = \{1, 2, 3\}$.

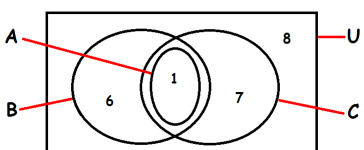
Beispiel (nochmal)

Lösung:

1. Rechne:

$$\{1,4,5\} \triangle \{1,2,3\} = \{2,3,4,5\}\,.$$

2. Nach dem Löschen der Elemente $2,3,4,5$ und der entsprechenden Bereiche erhalten wir:



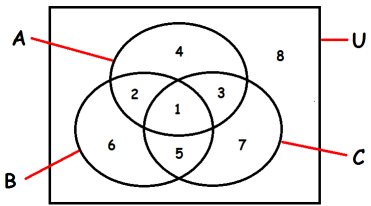
Damit die Gleichung stimmt, muss also $A = B \cap C$ gelten!

Aufgabe: Gilt die Mengengleichung

$$(\overline{A \cap B}) \cap C = (\overline{A} \cap C) \cup (B \cap C)$$

für beliebige Mengen A, B, C? Falls nicht, was müsste für A, B, C gelten, damit die Gleichung stimmt?

Hinweis: Benutze wieder die Mengen $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 5, 6\}$ und $C = \{1, 3, 5, 7\}$ über dem Universum $U = [8]$.



Rechne:

$$\begin{aligned}(\overline{A \cap B}) \cap C &= (\overline{\{1,2,3,4\} \cap \{1,2,5,6\}}) \cap \{1,3,5,7\} \\ &= \overline{\{1,2\}} \cap \{1,3,5,7\} \\ &= \{3,4,5,6,7,8\} \cap \{1,3,5,7\} \\ &= \{3,5,7\}\end{aligned}$$

$$\begin{aligned}(\overline{A} \cap C) \cup (B \cap C) &= (\overline{\{1,2,3,4\}} \cap \{1,3,5,7\}) \cup (\{1,2,5,6\} \cap \{1,3,5,7\}) \\ &= (\{5,6,7,8\} \cap \{1,3,5,7\}) \cup (\{1,2,5,6\} \cap \{1,3,5,7\}) \\ &= \{5,7\} \cup \{1,5\} \\ &= \{1,5,7\}\end{aligned}$$

Da $\{3,5,7\} \neq \{1,5,7\}$, gilt die Mengengleichung im Allgemeinen nicht.

Wegen

$$\{3,5,7\} \triangle \{1,5,7\} = \{1,3\}$$

entfernt man die Elemente 1 und 3 und die entsprechenden Bereiche aus dem Venn-Diagramm und interpretiert das Ergebnis.

Damit die Gleichung gilt muss also $A \cap C = \emptyset$ gelten!

Rechenregeln für Mengen

Seien $A, B, C \subseteq U$ beliebige Mengen über das Universum U. Ein paar nützliche Rechenregeln

Rechenregeln für Mengen

sind:

$A \cap U = A$	$A \cup \emptyset = A$	(Identität)
$A \cup U = U$	$A \cap \emptyset = \emptyset$	(Dominanz)
$A \cup A = A$	$A \cap A = A$	(Idempotenz)
$\overline{\overline{A}} = A$		(Doppeltes Komplement)
$A \cup B = B \cup A$	$A \cap B = B \cap A$	(Kommutativität)
$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$	(Assoziativität)
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	(Distributivität)
$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$	$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$	(De Morgan)
$A \cup \overline{A} = U$	$A \cap \overline{A} = \emptyset$	(U und $\emptyset$)
$A \setminus B = A \cap \overline{B}$		(Differenz)
$A \triangle B = (A \setminus B) \cup (B \setminus A)$		(symmetrische Differenz)
$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$	(Absorption)

Mit diesen Rechenregeln kann man auch Mengengleichungen beweisen.

Beispiel

Aufgabe: Beweise folgende Mengengleichung:

$$\overline{A \triangle B} = (\overline{A} \cap \overline{B}) \cup (A \cap B).$$

Beispiel

Lösung:

$$
\begin{aligned}
\overline{A \triangle B} &= \overline{(A \setminus B) \cup (B \setminus A)} && \text{(symmetrische Differenz)} \\
&= \overline{(A \setminus B)} \cap \overline{(B \setminus A)} && \text{(De Morgan)} \\
&= \overline{(A \cap \overline{B})} \cap \overline{(B \cap \overline{A})} && \text{(Differenz)} \\
&= (\overline{A} \cup \overline{\overline{B}}) \cap (\overline{B} \cup \overline{\overline{A}}) && \text{(De Morgan)} \\
&= (\overline{A} \cup B) \cap (\overline{B} \cup A) && \text{(Doppeltes Komplement)} \\
&= ((\overline{A} \cup B) \cap \overline{B}) \cup ((\overline{A} \cup B) \cap A) && \text{(Distributivität)} \\
&= ((\overline{A} \cap \overline{B}) \cup (B \cap \overline{B})) \cup ((\overline{A} \cap A) \cup (B \cap A)) && \text{(Distributivität)} \\
&= ((\overline{A} \cap \overline{B}) \cup \emptyset) \cup (\emptyset \cup (B \cap A)) && \text{(U und } \emptyset\text{)} \\
&= (\overline{A} \cap \overline{B}) \cup (A \cap B) && \text{(Identität)}
\end{aligned}
$$

Sei A die Menge aller Mengen, die sich nicht selbst als Element enthalten. D.h.

$$A = \{X \mid X \notin X\}.$$

Enthält A sich selbst?

Diese Frage kann leider nicht beantwortet werden, weil beide Antwortmöglichkeiten zu einem Widerspruch führen würden. Die Problematik dieser Frage wurde 1903 von dem britischen Mathematiker Bertrand Russell publiziert und ist eins von mehreren Paradoxien der naiven Mengenlehre.

Probleme wie dieses können mithilfe sogenannter axiomatischen Mengenlehren umgangen werden. Diese Arten von Mengenlehren sind leider etwas komplizierter und sind für uns nicht relevant.

Für Interessierte:

- `de.wikipedia.org/wiki/Naive_Mengenlehre`
- `de.wikipedia.org/wiki/Russellsche_Antinomie`

Themenübersicht

Tupel

Tupel stellen, im Gegensatz zu Mengen, geordnete Objekte dar. Wichtig ist:

- Es werden runde Klammern benutzt: $(\ldots)$.
- Komponenten werden durch Kommas getrennt.
- Die Reihenfolge der Komponenten ist relevant, z.B.: $(b, c, a) \neq (a, b, c)$.
- Die Anzahl an Kopien derselben Komponente ist auch relevant, z.B.: $(a, b, c, c, c, b) \neq (a, b, c)$.
- Die Komponenten eines Tupels können beliebige Objekte sein, z.B. Zahlen, Mengen oder wiederum Tupel.
- $()$ ist das leere Tupel. Es besitzt keine Komponenten.
- Mit $|\ldots|$ wird die Länge (die Anzahl an Komponenten) eines Tupels gekennzeichnet, z.B. $|(a, b, c)| = 3$.

Quizfrage

Sei a ein Tupel mit

$$a = (5, \{3, 4\}, 7, \{\{3, 4\}, 8\}, 1, 5, \emptyset).$$

Welche Länge $|a|$ besitzt a?

Die Länge $|a|$ von a ist

$$|a| = |(5, \{3, 4\}, 7, \{\{3, 4\}, 8\}, 1, 5, \emptyset)| = 7.$$

Kartesisches Produkt

Für ein beliebiges $n \in \mathbb{N}$ gilt:

$$A_1 \times \ldots \times A_n := \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}$$

Beispiel

Für $A = \{1, 2\}$, $B = \{3\}$, $C = \{4, 5, 6\}$ gilt:

$$A \times B \times C = \{(1, 3, 4), (1, 3, 5), (1, 3, 6), (2, 3, 4), (2, 3, 5), (2, 3, 6)\}$$

Infos

- Falls $|A_1|, \ldots, |A_n| < \infty$, dann gilt immer: $|A_1 \times \ldots \times A_n| = |A_1| \cdot \ldots \cdot |A_n|$.
- A^n ist eine Abkürzung für $\underbrace{A \times A \times \ldots \times A}_{n \text{ mal}}$.
- Das kartesische Produkt ist nicht assoziativ. Klammern machen nämlich schon einen Unterschied. Beispielsweise gilt für $A = \{a, b\}$, $B = \{c\}$, $C = \{d, e\}$ einerseits

$$\begin{aligned}(A \times B) \times C &= \{(a, c), (b, c)\} \times \{d, e\} \\ &= \{((a, c), d), ((a, c), e), ((b, c), d), ((b, c), e)\}\end{aligned}$$

und andererseits

$$\begin{aligned}A \times (B \times C) &= \{a, b\} \times \{(c, d), (c, e)\} \\ &= \{(a, (c, d)), (a, (c, e)), (b, (c, d)), (b, (c, e))\}.\end{aligned}$$

Seien $A = \{1, 2, 3, 4\}$ und $B = \{3, 4, 5\}$. Was ist dann die Kardinalität folgender Mengen?

1. $(A \cup B) \times (A \cap B)$
2. $\mathcal{P}(A) \times \mathcal{P}(B)$
3. $(A \times A) \cup (B \times B)$

1. Es gilt:

$$|(A \cup B) \times (A \cap B)| = |\{1,2,3,4,5\} \times \{3,4\}| = |\{1,2,3,4,5\}| \cdot |\{3,4\}| = 5 \cdot 2 = 10.$$

2. Es gilt:

$$|\mathcal{P}(A) \times \mathcal{P}(B)| = |\mathcal{P}(A)| \cdot |\mathcal{P}(B)| = 2^{|A|} \cdot 2^{|B|} = 2^4 \cdot 2^3 = 128.$$

3. Die Tupel $(3,3)$, $(3,4)$, $(4,3)$ und $(4,4)$ sind sowohl in $A \times A$ als auch in $B \times B$ drin und dürfen daher nicht doppelt gezählt werden. Daraus folgt:

$$|(A \times A) \cup (B \times B)| = |(A \times A)| + |(B \times B)| - 4 = |A| \cdot |A| + |B| \cdot |B| - 4 = 4 \cdot 4 + 3 \cdot 3 - 4 = 21.$$

Wörter und formale Sprachen

Bestehen die Komponenten der Tupel aus einzelnen Zeichen, so kann man die Klammern und die Kommas weglassen und die Zeichen nebeneinander schreiben. Beispielsweise kann man das Tupel (b, a, b, c, c) als Wort *babcc* notieren.

- Man nennt die Tupel dann Wörter.
- Die Menge aller Zeichen, die als Komponenten in den Tupeln vorkommen können, nennt man dann Alphabet Σ.
- Das leere Wort (das Wort ohne Zeichen bzw. mit Länge Null) ist ϵ.
- Σ^n ist die Menge aller Wörter über Σ der Länge n.
- $\Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^n$ ist die Menge aller Wörter über Σ mit beliebiger Länge
- Eine Menge $L \subseteq \Sigma^*$ von Wörtern nennt man eine formale Sprache.

Infos

- Nicht irritieren lassen! Das Σ („Sigma“) hier hat nichts mit dem Summenzeichen in z.B.

$$\sum_{i=0}^{n} a_i = a_0 + a_1 + a_2 + a_3 + \ldots + a_n$$

  zu tun. Das eine Σ ist eine Menge, das andere ist ein Operator.

- ϵ ist nur ein Zeichen, was man sich ausgedacht hat, um sich auf das leere Wort, (das leere Tupel () als Wort geschrieben) beziehen zu können.

- Um Verwirrungen zu vermeiden, wählt man Σ so, dass kein Zeichen Teil eines anderen Zeichens ist. Würde man beispielsweise $\Sigma = \{a, ab, b\}$ wählen, so wäre nicht eindeutig, ob das Wort aba für (a, b, a) oder (ab, a) steht.

Konkatenation

Für beliebige Wörter $u = u_1 \dots u_k$ und $v = v_1 \dots v_m$ gilt:

$$uv = u_1 \dots u_k v_1 \dots v_m.$$

Für beliebige Tupelmengen A, B gilt:

$$AB := \{uv \mid u \in A, v \in B\}.$$

Infos

- Konkateniert man A und B miteinander, so muss man jedes Wort aus A mit jedem aus B kombinieren. Die Ergebnisse sind alle in AB enthalten.
- Je nach Autor schreibt man für die Konkatenation aus A und B $A \circ B$ oder $A \parallel B$ statt AB.

Beispiele (mit Tupeln)

- Seien $A = \{(x), (x, y), (y, x)\}$ und $B = \{(), (z, y)\}$. Dann gilt:

$$AB = \{(x), (x, z, y), (x, y), (x, y, z, y), (y, x), (y, x, z, y)\}.$$

- Seien $A = \{(a), (a, b)\}$, $B = \{(c, b)\}$ und $C = \{(b), (b, c)\}$. Dann gilt:

$$ABC = \{(a, c, b, b), (a, c, b, b, c), (a, b, c, b, b), (a, b, c, b, b, c)\}.$$

- Konkatenieren macht mit Wörtern viel mehr Spaß als mit Tupeln (weniger Schreibarbeit). Fasst man $a = (a_1, \ldots, a_k)$ und $b = (b_1, \ldots, b_m)$ als Wörter $a = a_1 \ldots a_k$ und $b = b_1 \ldots b_m$ auf, so gilt für die Konkatenation von a und b:

$$ab = a_1 \ldots a_k b_1 \ldots b_m.$$

  Man „klebt“ also einfach die Wörter aneinander.

- Wir werden die Konkatenation so gut wie immer nur auf Wörtern anwenden!
- Für ein beliebiges Zeichen $a \in \Sigma$ gilt:

$$\epsilon a = a = a\epsilon.$$

Beispiele (mit Wörtern)

- Seien $A = \{x, xy, yx\}$ und $B = \{\epsilon, zy\}$ zwei Sprachen über dem Alphabet $\Sigma = \{x, y, z\}$. Dann gilt:
$$AB = \{x, xzy, xy, xyzy, yx, yxzy\}.$$
- Seien $A = \{a, ab\}$, $B = \{cb\}$ und $C = \{b, bc\}$ drei Sprachen über dem Alphabet $\Sigma = \{a, b, c\}$. Dann gilt:
$$ABC = \{acbb, acbbc, abcbb, abcbbc\}.$$

Quizfrage

Seien $\Sigma = \{x, y\}$ ein Alphabet und $A, B \subseteq \Sigma^*$ zwei Sprachen über Σ mit $A = \{\epsilon, x, xy, xyy\}$ und $B = \{\epsilon, y, yy\}$.

Wie sieht AB extensional aus?

$$
\begin{aligned}
AB &= \{\epsilon\epsilon, \epsilon y, \epsilon yy, x\epsilon, xy, xyy, xy\epsilon, xyy, xyyy, xyy\epsilon, xyyy, xyyyy\} \\
&= \{\epsilon, y, yy, x, xy, xyy, xy, xyy, xyyy, xyy, xyyy, xyyyy\} \\
&= \{\epsilon, y, yy, x, xy, xyy, xyyy, xyyyy\}\,.
\end{aligned}
$$

- Die Konkatenation ist assoziativ. Es gilt:

$$A(BC) = (AB)C.$$

  Man kann also die Klammern weglassen und einfach ABC schreiben!

- Für eine Sprache A definieren wir

$$A^n = \underbrace{AAA\ldots A}_{n \text{ mal}} \text{ mit } A^0 = \{\epsilon\}, \qquad A^+ = \bigcup_{n=1}^{\infty} A^n \qquad \text{und} \qquad A^* = \bigcup_{n=0}^{\infty} A^n.$$

- Bei der Konkatenation können Duplikate entstehen! Man kann also, im Gegensatz zum kartesischen Produkt, keine Formel für $|AB|$ in Abhängigkeit von $|A|$ und $|B|$ angeben. Es gilt lediglich:

$$|AB| \leq |A| \cdot |B|,$$

  d.h. $|A| \cdot |B|$ ist nur eine obere Schranke für $|AB|$.

Quizfrage

Was ist eine möglichst gute (= möglichst große) untere Schranke für $|AB|$ in Abhängigkeit von $|A|$ und $|B|$?

Leider habe ich noch keine tolle Antwort auf diese Frage. Falls Du einen Vorschlag hast, kannst Du ihn mir sehr gerne schicken. Ich werde mich sehr darüber freuen!

Einfach per E-Mail an `cfcamino@gmail.com`.

Themenübersicht

Wichtige Zahlenmengen

Wichtige endliche Zahlenmengen sind:

$$\begin{array}{lcll} [n] & = & \{1, 2, \ldots, n\} & \\ [n]_0 & = & \{0, 1, \ldots, n\} & \\ \mathbb{Z}_n & = & \{0, 1, \ldots, n-1\} & = \quad [n-1]_0 \end{array}$$

Wichtige unendliche Zahlenmengen sind:

$$\begin{array}{lcll} \mathbb{N} & = & \{1, 2, 3, \ldots\} & \text{(natürliche Zahlen)} \\ \mathbb{N}_0 & = & \{0, 1, 2, 3, \ldots\} & \text{(natürliche Zahlen mit Null)} \\ \mathbb{Z} & = & \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} & \text{(ganze Zahlen)} \\ \mathbb{Q} & = & \left\{ \frac{p}{q} \;\middle|\; p \in \mathbb{Z}, q \in \mathbb{N} \right\} & \text{(rationale Zahlen)} \\ \mathbb{R} & = & \{d, d_1 d_2 d_3 \ldots \mid d \in \mathbb{Z}, d_1, d_2, d_3, \ldots \in \mathbb{Z}_{10}\} & \text{(reelle Zahlen)} \\ \mathbb{C} & = & \{a + bi \mid a, b \in \mathbb{R}\} & \text{(komplexe Zahlen)} \end{array}$$

Info

Bei der Definition der sechs unendlichen Mengen in der vorherigen Folie habe ich mir das Leben sehr einfach gemacht. Die formalen Definitionen sind etwas komplizierter.

Deutlich komplizierter als für uns nötig ;-)

Summen und Produkte

Seien $m, n \in \mathbb{N}$ zwei natürliche Zahlen und $\{a_i \in \mathbb{C} \mid m \leq i \leq n\}$ eine endliche Teilmenge der komplexen Zahlen. Dann gilt:

$$\sum_{i=m}^{n} a_i = \begin{cases} 0 & \text{falls } m > n \\ \sum_{i=m}^{n-1} a_i + a_n & \text{falls } m \leq n \end{cases} \quad \text{und} \quad \prod_{i=m}^{n} a_i = \begin{cases} 1 & \text{falls } m > n \\ \prod_{i=m}^{n-1} a_i \cdot a_n & \text{falls } m \leq n \end{cases}$$

Beispiele

- Summe:

$$\sum_{i=3}^{5} i^2 = \sum_{i=3}^{4} i^2 + 5^2 = \sum_{i=3}^{3} i^2 + 4^2 + 5^2 = \sum_{i=3}^{2} i^2 + 3^2 + 4^2 + 5^2 = 3^2 + 4^2 + 5^2 = 50.$$

- Produkt:

$$\prod_{i=1}^{3} \frac{i}{i+1} = \prod_{i=1}^{2} \frac{i}{i+1} \cdot \frac{3}{4} = \prod_{i=1}^{1} \frac{i}{i+1} \cdot \frac{2}{3} \cdot \frac{3}{4} = \prod_{i=1}^{0} \frac{i}{i+1} \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} = \frac{1}{4}.$$

Info

Dass $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$ komplex sind, heißt nicht sofort, dass sie immer mit imaginären Einheiten i verseucht sind. Meistens sind das reelle Zahlen, aber die Definition soll so allgemein wie möglich gehalten werden.

Fakultät

Für die Fakultät $n!$ einer natürlichen Zahl $n \in \mathbb{N}_0$ gilt

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$$

mit $0! := 1$.

Beispiele

Die ersten Werte für $n!$ sind:

$$0! = 1$$
$$1! = 1$$
$$2! = 2 \cdot 1 = 2$$
$$3! = 3 \cdot 2 \cdot 1 = 6$$
$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$
$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$
$$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$$
$$7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$$

Steigende und fallende Faktorielle

Für beliebige $n, k \in \mathbb{Z}$ gilt:

$$n^{\underline{k}} = \prod_{i=0}^{k-1} (n-i) = \underbrace{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)}_{k \text{ Faktoren}} \qquad \text{(fallende Faktorielle)}$$

$$n^{\overline{k}} = \prod_{i=0}^{k-1} (n+i) = \underbrace{n \cdot (n+1) \cdot (n+2) \cdot \ldots \cdot (n+k-1)}_{k \text{ Faktoren}} \qquad \text{(steigende Faktorielle)}$$

mit $n^{\underline{0}} := 1$ und $n^{\overline{0}} := 1$.

Beispiele

Es gilt:

$$6^{\underline{4}} = 6 \cdot 5 \cdot 4 \cdot 3 = 360, \qquad 6^{\overline{4}} = 6 \cdot 7 \cdot 8 \cdot 9 = 3024,$$

$$2^{\underline{6}} = 2 \cdot 1 \cdot 0 \cdot (-1) \cdot (-2) \cdot (-3) = 0, \qquad 2^{\overline{6}} = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5040,$$

$$(-3)^{\underline{5}} = (-3) \cdot (-4) \cdot (-5) \cdot (-6) \cdot (-7) = -2520, \qquad (-3)^{\overline{5}} = (-3) \cdot (-2) \cdot (-1) \cdot 0 \cdot 1 = 0\ .$$

Seien a, b, c beliebige reelle Zahlen mit $a \neq 0, b, c > 0, b, c \neq 1$. Dann sind folgende drei Aussagen zueinander äquivalent:

$$\log_c b = a \quad \Longleftrightarrow \quad c^a = b \quad \Longleftrightarrow \quad \sqrt[a]{b} = c$$

Beispiele

$$\log_2 8 = 3 \iff 2^3 = 8 \iff \sqrt[3]{8} = 2$$
$$\log_3 \tfrac{1}{9} = -2 \iff 3^{-2} = \tfrac{1}{9} \iff \sqrt[-2]{\tfrac{1}{9}} = 3$$
$$\log_{\frac{1}{3}} 81 = -4 \iff \left(\tfrac{1}{3}\right)^{-4} = 81 \iff \sqrt[-4]{81} = \tfrac{1}{3}$$
$$\log_{\frac{1}{4}} \tfrac{1}{16} = 2 \iff \left(\tfrac{1}{4}\right)^{2} = \tfrac{1}{16} \iff \sqrt[2]{\tfrac{1}{16}} = \tfrac{1}{4}$$

Für Logarithmen gibt es folgende spezielle Basen:

$$\lg n = \log_{10} n, \qquad \ln n = \log_e n, \qquad \operatorname{lb} n = \log_2 n.$$

In der Schule wird $\log n$ als $\log_{10} n$ definiert. In der Uni kann $\log n$ entweder $\ln n$ bedeuten oder $\log_b n$ für irgendein b, was nicht relevant ist.

Logarithmusregeln

Für Logarithmen gibt es folgende Rechenregeln:

$$\log_a b = \frac{\log_c b}{\log_c a}$$
$$\log_a(n \cdot m) = \log_a n + \log_a m$$
$$\log_a \frac{n}{m} = \log_a n - \log_a m$$
$$\log_a n^m = m \cdot \log_a n$$
$$\log_{a^b} n = \frac{1}{b} \cdot \log_a n$$

Mit folgenden Spezialfällen:

$$\log_a 1 = 0, \quad \log_a a = 1, \quad \log_a a^n = n, \quad \log_a \sqrt[n]{a} = \tfrac{1}{n}.$$

Potenzregeln

Für Potenzen gibt es folgende Rechenregeln:

$$
\begin{aligned}
a^n \cdot a^m &= a^{n+m} \\
\frac{a^n}{a^m} &= a^{n-m} \\
(a^n)^m &= a^{n \cdot m} \\
a^{-n} &= \frac{1}{a^n} \\
a^n \cdot b^n &= (a \cdot b)^n \\
\frac{a^n}{b^n} &= \left(\frac{a}{b}\right)^n \\
a^{\frac{n}{m}} &= \sqrt[m]{a^n}
\end{aligned}
$$

Mit folgenden Spezialfällen:

$$a^0 = 1, \quad a^1 = a, \quad 0^n = 0, \quad 1^n = 1, \quad a^{\log_a n} = n.$$

Potenzregeln

0^0 ist, soweit ich weiß, nicht definiert. Manchmal wird es aber trotzdem nach Lust und Laune als 0 oder 1 festgelegt.

Wurzelregeln

Für Wurzeln gibt es folgende Rechenregeln:

$$\sqrt[n]{\sqrt[m]{a}} = \sqrt[n \cdot m]{a}$$
$$\sqrt[-n]{a} = \frac{1}{\sqrt[n]{a}}$$
$$\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{a \cdot b}$$
$$\frac{\sqrt[n]{a}}{\sqrt[n]{b}} = \sqrt[n]{\frac{a}{b}}$$

Mit den Spezialfällen:

$$\sqrt[1]{a} = a \quad \sqrt[n]{1} = 1 \quad \sqrt[n]{0} = 0 \quad \sqrt[n]{a^n} = a.$$

Info

Wurzelregeln sind eigentlich völlig nutzlos. Am besten ist es, wenn man Wurzeln $\sqrt[n]{a}$ als Potenzen $a^{\frac{1}{n}}$ schreibt und mit den Potenzregeln rechnet ;-)

z.B.:

$$(\mathrm{ld}\, n)^2 < n \iff \mathrm{ld}\, n < n^{1/2} \ .$$

1. Wieso gelten für beliebige $a, b, m, n \in \mathbb{R}^+$ mit $a, b \neq 1$ folgende Gleichungen?
   1.1 $n^{\log_b m} = m^{\log_b n}$,
   1.2 $\log_a b = \frac{1}{\log_b a}$,
   1.3 $\log_b(n+m) = \log_b n + \log_b\left(1 + \frac{m}{n}\right)$.
2. Was ist $\sqrt[2/3]{4}$?

1. 1.1 $n^{\log_b m} = b^{\log_b(n^{\log_b m})} = b^{(\log_b m)\cdot(\log_b n)} = b^{\log_b(m^{\log_b n})} = m^{\log_b n}$.

   1.2 Für ein beliebiges $c > 0$ mit $c \neq 1$ gilt: $\log_a b = \frac{\log_c b}{\log_c a} = \frac{1}{\frac{\log_c a}{\log_c b}} = \frac{1}{\log_b a}$. Am einfachsten wählt man $c = b$ und erhält:

$$\log_a b = \frac{\log_b b}{\log_b a} = \frac{1}{\log_b a}.$$

   1.3 $\log_b(n+m) = \log_b\left(n \cdot \left(1 + \frac{m}{n}\right)\right) = \log_b n + \log_b\left(1 + \frac{m}{n}\right)$.

2. $\sqrt[2/3]{4} = 4^{\frac{1}{2/3}} = 4^{\frac{3}{2}} = 4^{3\cdot\frac{1}{2}} = (4^3)^{\frac{1}{2}} = \sqrt{4^3} = \sqrt{64} = 8$.

Themenübersicht

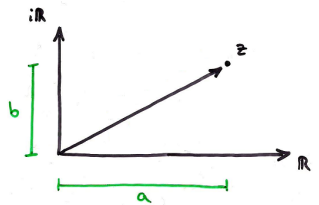
Komplexe Zahlen

Die Menge der komplexen Zahlen $\mathbb{C}$ ist definiert als

$$\mathbb{C} = \mathbb{R} + i\mathbb{R} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

Die imaginäre Einheit i besitzt die Eigenschaft $i^2 = -1$.

Reelle Zahlen lassen sich als Punkte auf einer Zahlengerade veranschaulichen. Eine komplexe Zahl $z = a + bi$ wird dagegen als Punkt (a, b) auf der Gauß'schen Zahlenebene dargestellt.



$\mathrm{Re}(z) = a$ wird Realanteil und $\mathrm{Im}(z) = b$ Imaginäranteil von z genannt. Wegen $\mathbb{R} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) = 0\}$ gilt $\mathbb{R} \subseteq \mathbb{C}$.

Betrag komplexer Zahlen

Sei $z \in \mathbb{C}$ eine komplexe Zahl mit $z = a + bi$.

- $\overline{z} = a - bi$ ist die zu z konjugiert-komplexe Zahl.
- $|z| = \sqrt{z\overline{z}} = \sqrt{(a+bi)(a-bi)} = \sqrt{a^2 - (bi)^2} = \sqrt{a^2 + b^2}$ ist der Betrag von z.
- Bei Summen oder Differenzen im Betrag benutzt man die Dreiecksungleichungen. Für beliebige komplexe Zahlen $z_1, z_2 \in \mathbb{C}$ gelten die Dreiecksungleichungen:

egal, ob $+$ oder $-$

$$||z_1| - |z_2|| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|.$$

„umgekehrte Dreiecksungleichung“ „normale Dreiecksungleichung“

- Bei Produkten und Quotienten kann man die Beträge einfach reinziehen, d.h.:

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2| \qquad \text{und} \qquad \left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}.$$

Infos

- Wegen $\mathbb{R} \subseteq \mathbb{C}$ gilt alles, was für komplexe Zahlen gilt, auch für reelle Zahlen. Die Dreiecksungleichungen sind da keine Ausnahme.
- $\mathbb{C}$ ist im Gegensatz zu $\mathbb{Q}$ und $\mathbb{R}$ kein angeordneter Körper. Man kann komplexe Zahlen z_1 und z_2 nicht mit $<$, $>$, $\leq$ oder $\geq$ vergleichen.
- Der Betrag einer komplexen Zahl ist jedoch immer eine (positive) reelle Zahl. Beträge komplexer Zahlen kann man alsosehr wohl miteinander vergleichen!

Elementare Operationen (ohne Division)

Für komplexe Zahlen $z_1, z_2 \in \mathbb{C}$ mit $z_1 = a_1 + b_1 i$ und $z_2 = a_2 + b_2 i$ sind folgende Operationen definiert.

- Addition:
$$z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)i,$$
- Subtraktion:
$$z_1 - z_2 = (a_1 - a_2) + (b_1 - b_2)i,$$
- Multiplikation:
$$z_1 \cdot z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i,$$
- Division:

Dürft ihr gleich selbst herleiten ;-).

Gegeben seien zwei komplexe Zahlen $z_1, z_2 \in \mathbb{C}$ mit $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$ und $z_2 \neq 0$. Was ist die algebraische Form von

$$z_3 = \frac{z_1}{z_2}$$

in Abhängigkeit von a_1, a_2, b_1 und b_2?

Sei $z_3 = a_3 + b_3 i$. Es muss gelten $z_1 = z_2 \cdot z_3$, d.h.:

$$a_1 + b_1 i = (a_2 + b_2 i) \cdot (a_3 + b_3 i) = \underbrace{(a_2 a_3 - b_2 b_3)}_{=a_1} + \underbrace{(a_2 b_3 + a_3 b_2)}_{=b_1}$$

Aus dem Gleichungssystem

$$\begin{aligned} a_2 a_3 - b_2 b_3 &= a_1 \\ a_2 b_3 + a_3 b_2 &= b_1 \end{aligned}$$

folgen die eindeutigen Werte $a_3 = \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2}$ und $b_3 = \frac{b_1 a_2 - a_1 b_2}{a_2^2 + b_2^2}$. Das ergibt:

$$z_3 = \left(\frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} \right) + \left(\frac{b_1 a_2 - a_1 b_2}{a_2^2 + b_2^2} \right) i$$

Tipp

Die Formel für die Division zweier komplexer Zahlen kann man sich sehr einfach merken. Man muss nur den Bruch $\frac{z_1}{z_2}$ um $\overline{z_2}$ erweitern und vereifachen.

Man erhält:

$$\begin{aligned}
\frac{z_1}{z_2} &= \frac{z_1\overline{z_2}}{z_2\overline{z_2}} \\
&= \frac{(a_1 + b_1 i)(a_2 - b_2 i)}{(a_2 + b_2 i)(a_2 - b_2 i)} \\
&= \frac{(a_1 a_2 + b_1 b_2) + (b_1 a_2 - a_1 b_2) i}{a_2^2 + b_2^2} \\
&= \left(\frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2}\right) + \left(\frac{b_1 a_2 - a_1 b_2}{a_2^2 + b_2^2}\right) i.
\end{aligned}$$

Elementare Operationen (Zusammenfassung)

Für komplexe Zahlen $z_1, z_2 \in \mathbb{C}$ mit $z_1 = a_1 + b_1 i$ und $z_2 = a_2 + b_2 i$ sind folgende Operationen definiert.

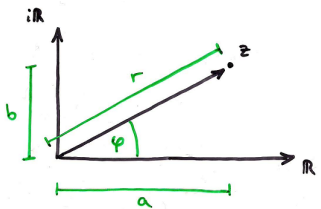
- Addition:
$$z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)i,$$
- Subtraktion:
$$z_1 - z_2 = (a_1 - a_2) + (b_1 - b_2)i,$$
- Multiplikation:
$$z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i,$$
- Division:
$$\frac{z_1}{z_2} = \frac{z_1 \overline{z_2}}{z_2 \overline{z_2}} = \left(\frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} \right) + \left(\frac{b_1 a_2 - a_1 b_2}{a_2^2 + b_2^2} \right) i.$$

Polarform

Jede komplexe Zahl $z \neq 0$ lässt sich eindeutig durch Polarkoordinaten (r, φ) mit $r, \varphi \in \mathbb{R}$ und $r \geq 0$ darstellen. Dabei wird $r = |z| = \sqrt{a^2 + b^2}$ die Länge und φ der Winkel von z genannt. Der Polarform liegt die Euler'sche Formel $e^{xi} = \cos x + i \sin x$ zugrunde. Aus ihr folgt die Beziehung

$$re^{\varphi i} = a + bi$$

mit $a = r \cos \varphi$ und $b = r \sin \varphi$.



Wichtig

Der Winkel φ wird in Bogenmaß (Radiant) und nicht in Gradmaß (Grad) gemessen. Eine Umdrehung (360°) entspricht genau 2π.

1. Was ist die algebraische Form folgender komplexen Zahlen?

$$2e^{\pi i}, \quad e^{\frac{\pi}{4} i}, \quad \sqrt{2}e^{\frac{3\pi}{4} i}, \quad 3e^{\frac{\pi}{2} i}, \quad 2e^{2\pi i}.$$

2. Was ist die Polarform folgender komplexen Zahlen?

$$1 - i, \quad 2 + 2i, \quad -5, \quad 3i, \quad 3i - 3$$

3. Was ist die algebraische Form von $e^{\pi i + 1}$?
4. Was sind Winkel und Länge von $e^{(3-2i)i}$?

Hinweis: Benutze die Wertetabelle auf Folie 1567.

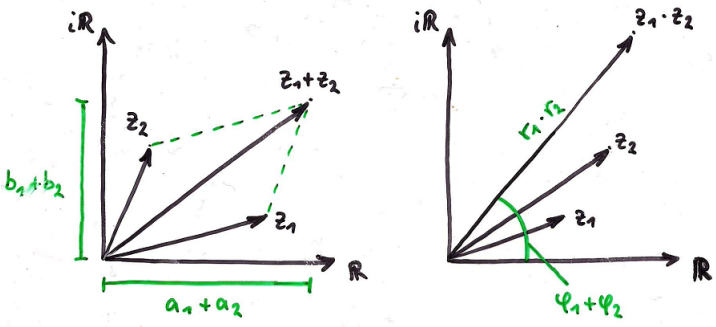
1. -2, $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$, $-1 + i$, $3i$, 2.
2. $\sqrt{2}e^{\frac{7\pi}{4}i}$, $2\sqrt{2}e^{\frac{\pi}{4}i}$, $5e^{\pi i}$, $3e^{\frac{\pi}{2}i}$, $3\sqrt{2}e^{\frac{3\pi}{4}i}$.
3. $e^{\pi i+1} = e \cdot e^{\pi i} = e \cdot (-1) = -e$.
4. $e^{(3-2i)i} = e^{3i-2i^2} = e^{2+3i} = e^2 \cdot e^{3i}$.

Länge: e^2 Winkel: 3

Multiplikation in Polarform

Für komplexe Zahlen $z_1 = r_1 \cdot e^{\varphi_1 i}$ und $z_2 = r_2 \cdot e^{\varphi_2 i}$ gilt:

$$z_1 \cdot z_2 = (r_1 \cdot r_2) e^{(\varphi_1 + \varphi_2) i}.$$

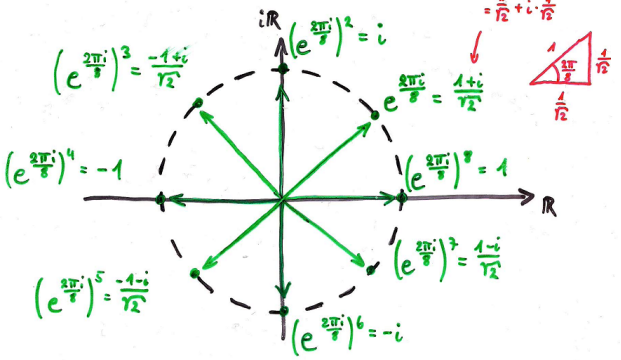


Info

Die Polarform macht nur beim Multiplizieren, Potenzieren, Dividieren oder Radizieren (Wurzelziehen) von komplexen Zahlen Sinn. Für Addition und Subtraktion sollte man die algebraische Form benutzen.

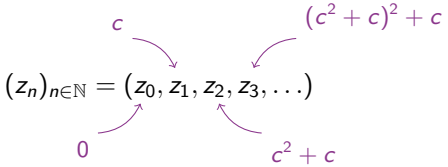
Beispiel

Die komplexe Zahl $z \in \mathbb{C}$ mit $z = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i = e^{\frac{\pi}{4} i} = e^{\frac{2\pi}{8} i}$ hat Länge 1. Die Zahlen $z, z^2, z^3, z^4, \ldots$ sind alle auf dem sogenannten komplexen Einheitskreis:



Sehr cool!

Gegeben sei die komplexe Zahlenfolge $(z_n)_{n\in\mathbb{N}}$ mit $z_0 = 0$ und $z_{n+1} = z_n^2 + c$.



Die Menge $\{c \in \mathbb{C} \,|\, (z_n)_{n\in\mathbb{N}_0}$ ist beschränkt$\}$ wird Mandelbrotmenge genannt und ist einfach verdammt schön.

Tolle Webseite zum Rumspielen und Nachlesen:

`www.renatofonseca.net/mandelbrotset.php`

Übrigens: Diese Menge hat nichts mit Weihnachtsgebäck zu tun. Sie wurde nach dem Mathematiker Benoit Mandelbrot benannt.

Themenübersicht

Aussagen

Eine Aussage ist ein sprachliches Konstrukt, dem man genau einen der Wahrheitswerte *wahr* oder *falsch* zuordnen kann. Eine Aussage gilt, wenn sie den Wahrheitswert *wahr* besitzt.

Die Negation einer Aussage ist wiederum eine Aussage. Durch die Negation einer Aussage wird ihr Wahrheitswert in sein Gegenteil gekehrt. Für die Negation einer Aussage A schreiben wir einfach:

$$\text{nicht } A.$$

Zwei Aussagen A und B sind äquivalent, wenn sie denselben Wahrheitswert besitzen.

UND-Aussagen

Sind F und G Aussagen, dann ist auch

$$F \text{ und } G$$

eine Aussage. Diese gilt genau dann, wenn sowohl F als auch G gelten.

Die Negation davon ist:

$$\text{nicht } F \text{ oder nicht } G.$$

ODER-Aussagen

Sind F und G Aussagen, dann ist auch

$$F \text{ oder } G$$

eine Aussage. Diese gilt genau dann, wenn mindestens eine der Aussagen F und G gilt. Die Negation davon ist:

$$\text{nicht } F \text{ und nicht } G.$$

WENN-DANN-Aussagen

Sind F und G Aussagen, dann ist auch

$$\text{Wenn } F \text{ dann } G$$

eine Aussage. Diese gilt genau dann, wenn F und G beide gelten oder wenn F nicht gilt. In dem Fall, dass F nicht gilt, ist der Wahrheitswert von G egal, weil über ihn nichts gesagt wurde, die gesamte Aussage ist dann wahr.

Man nennt diese Aussagen Implikationen und schreibt kurz:

$$F \implies G.$$

Diese sind äquivalent zu:

$$\text{nicht } F \text{ oder } G.$$

Gilt eine Implikation $F \implies G$ nicht, so schreibt man kurz $F \not\Longrightarrow G$.

GENAU-DANN-WENN-Aussagen

Sind F und G Aussagen, dann ist auch

$$F \text{ genau dann, wenn } G$$

eine Aussage. Diese ist genau dann wahr, wenn F und G beide wahr oder beide falsch sind. Diese Aussage kann auch wie folgt formuliert werden:

$$F \text{ dann und nur dann, wenn } G$$

Man nennt diese Aussagen Äquivalenzen und schreibt kurz:

$$F \iff G.$$

Diese sind äquivalent zu:

$$F \implies G \text{ und } G \implies F.$$

Gilt eine Äquivalenz $F \iff G$ nicht, so schreibt man kurz: $F \not\iff G$.

Allaussagen

Ist A eine Menge und F eine Aussage, die von ein Element x abhängig sein kann, dann ist

$$\text{Für alle } x \in A \text{ gilt } F$$

auch eine Aussage. Diese ist wahr, wenn F für alle $x \in A$ wahr ist. Die Negation dieser Aussage ist

$$\text{Es gibt ein } x \in A \text{ für das nicht } F \text{ gilt.}$$

Man nennt solche Aussagen Allaussagen und schreibt kurz:

$$\forall x \in A : F.$$

Gilt die Aussage $A(x)$ nicht für alle (aber vielleicht für einige) $x \in A$, dann schreiben wir:

$$\not\forall\, x \in A : F.$$

Existenzaussagen

Ist A eine Menge und F eine Aussage, die von einem Element x abhängig sein kann, dann ist

$$\text{Es gibt ein } x \in A \text{ für das } F \text{ gilt}$$

auch eine Aussage. Diese ist wahr, wenn F für mindestens ein $x \in A$ wahr ist. Die Negation dieser Aussage ist

$$\text{Für alle } x \in A \text{ gilt nicht } F.$$

Man nennt solche Aussagen Existenzaussagen und schreibt kurz:

$$\exists x \in A : F.$$

Gibt es gar kein $x \in A$ für das die Aussage F gilt, dann schreiben wir:

$$\nexists x \in A : F.$$

Wichtig

Die Symbole $\Longrightarrow$, $\Longleftrightarrow$, $\forall$ und $\exists$ sind keine formalen Operatoren, sondern nur Abkürzungen, um Aussagen kompakter darstellen zu können.

Für ihre Verwendung gibt es keine definierte Regeln. Wichtig ist nur, dass man sie so verwendet, dass der Leser versteht, was gemeint ist.

$\Longrightarrow$ und $\Longleftrightarrow$ machen nur bei Aussagen Sinn! Ausdrücke wie

$$\{1,2\} \cup \{2,3\} \Longleftrightarrow \{1,2,3\} \quad \text{oder} \quad (a+b)^2 \Longleftrightarrow a^2 + 2ab + b^2$$

sind nicht nur falsch, sondern es tut sogar weh sie zu lesen!

Beispiele

- Für beliebige Mengen $A, B \subseteq U$ über einem Universum U können $\subseteq$, $=$ und $\subset$ wie folgt kompakt definiert werden:

$$
\begin{aligned}
A \subseteq B &:\iff (\forall x \in U : x \in A \implies x \in B) \\
A = B &:\iff (\forall x \in U : x \in A \iff x \in B) \\
A \subset B &:\iff (\forall x \in U : x \in A \implies x \in B) \text{ und } (\exists x \in U : x \notin A \text{ und } x \in B)
\end{aligned}
$$

- Die Aussage

Es gibt beliebig große Primzahlen

könnte wie folgt kompakt formuliert werden:

$$\forall x \in \mathbb{N} : \exists y \in \mathbb{N} : (y \text{ prim und } y > x).$$

Wie kann man folgende Aussagen kompakt darstellen?

1. Es gibt eine ganze Zahl, die größer ist als alle anderen.
2. Es gibt keine ganze Zahl, die größer ist als alle anderen.
3. Die Summe von zwei geraden Zahlen ist wieder gerade.

Benutze ausschließlich folgende Bausteine: $\forall$, $\exists$, x, y, $\in$, $\mathbb{Z}$, :, (,), $\leq$, $<$, und, gerade, $\Longrightarrow$ und $+$.

1. $\exists x \in \mathbb{Z} : \forall y \in \mathbb{Z} : y < x$.
2. $\nexists x \in \mathbb{Z} : \forall y \in \mathbb{Z} : y < x$, was äquivalent ist zu: $\forall x \in \mathbb{Z} : \exists y \in \mathbb{Z} : x \leq y$.
3. $\forall x \in \mathbb{Z} : \forall y \in \mathbb{Z} : (x$ gerade und y gerade$) \implies x + y$ gerade, was auch wie folgt geschrieben werden kann: $\forall x, y \in \mathbb{Z} : x$ und y gerade $\implies x + y$ gerade.

Mehr Quizfragen (Männer sind Schweine ♪)

Sei M die Menge aller Menschen. Wie kann man folgende Aussagen kompakt darstellen?

1. Jeder Mann ist ein Schwein.
2. Nur Männer können Schweine sein.
3. Es gibt Männer, die keine Schweine sind.
4. Manche Schweine sind Männer.
5. Jeder Mann ist ein Schwein und jedes Schwein ist ein Mann.
6. Wenn alle Menschen Männer sind, dann sind sie auch alle Schweine.
7. Jeder Mensch ist ein Mann oder ein Schwein.
8. Es gibt keine Schweine.

Benutze ausschließlich folgende Bausteine: $\forall$, $\exists$, x, $\in$, M, $:$, $($, $)$, $\implies$, $\iff$, und, oder, ist Mann, ist Schwein, ist kein Mann, ist kein Schwein.

1. $\forall x \in M : x$ ist Mann $\implies$ x ist Schwein.
2. $\forall x \in M : x$ ist Schwein $\implies$ x ist Mann bzw.
   $\forall x \in M : x$ ist kein Mann $\implies$ x ist kein Schwein.
3. $\exists x \in M : x$ ist Mann und x ist kein Schwein.
4. $\exists x \in M : x$ ist Schwein und x ist Mann.
5. $(\forall x \in M : x$ ist Mann $\implies$ x ist Schwein) und $(\forall x \in M : x$ ist Schwein $\implies$ x ist Mann), bzw. $\forall x \in M : x$ ist Mann $\iff$ x ist Schwein.
6. $(\forall x \in M : x$ ist Mann) $\implies$ $(\forall x \in M : x$ ist Schwein)
7. $\forall x \in M : x$ ist Mann oder x ist Schwein.
8. $\nexists x \in M : x$ ist Schwein, bzw. $\forall x \in M : x$ ist kein Schwein.

Wichtige Terminologie aus der Mathematik

- Eine Annahme ist eine Aussage, bei der man davon ausgeht, dass sie wahr ist. Annahmen werde auch Postulate, Hypothesen, Prämissen oder Axiome genannt.
- Ein Satz ist eine Aussage, die aus den Annahmen folgt. Sätze werden auch Theoreme genannt.
- Ein Beweis ist die korrekte und vollständige (lückenlose) Argumentation dafür, dass ein Satz tatsächlich aus den Annahmen folgt.
- Ein Lemma ist ein Hilfssatz, der im Beweis eines anderen (wichtigeren) Satzes benutzt wird.
- Ein Korollar ist ein Theorem, das leicht als Folgerung eines wichtigen Theorems bewiesen werden kann.

Struktur mathematischer Aussagen

Mathematische Aussagen können als prädikatenlogische Formeln über einer geeigneten Basisstruktur S formuliert werden. Dabei werden einzelne Teilaussagen wie folgt übersetzt:

Aussage	Kompaktschreibweise	Prädikatenlogik
nicht F		$\neg F$
F und G		$F \wedge G$
F oder G		$F \vee G$
Wenn F, dann G	$F \implies G$	$F \to G$
F genau dann, wenn G	$F \iff G$	$F \leftrightarrow G$
Für alle $x \in A$ gilt F	$\forall x \in A : F$	$\forall x(A(x) \to F)$
Es gibt ein $x \in A$ für das F gilt	$\exists x \in A : F$	$\exists x(A(x) \wedge F)$

Hierbei entspricht die Menge A genau der Interpretation des Prädikats A unter S, d.h. $A_S = A$.

Beweisen von Implikationen

Die zu beweisende Aussage F und die Annahmen $A_1, \ldots, A_n$ werden als prädikatenlogische Formeln formalisiert. Dann wird, mithilfe einer festgelegten Menge von gültigen Inferenzregeln, eine Herleitung für

$$A_1, \ldots, A_n \vdash F$$

gesucht. Hier wird F Folgerung oder auch Conclusio genannt.

Leider sind formale Beweise viel zu kompliziert und aufwendig. Deswegen werden sie in einer Mischung aus natürlicher Sprache und Prädikatenlogik bewiesen. Ein informeller Beweis wird dann akzeptiert, wenn man der Meinung ist, dass er sich formalisieren ließe.

Grobe Vorgehensweise

Die Gestalt einer Aussage suggeriert, wie man vorgehen könnte. Die wichtigsten sind auf folgender Tabelle aufgelistet:

Gestalt	Vorgehensweise
nicht F	Zeige, dass F nicht gilt.
F und G	Zeige F und G in zwei getrennten Beweisen.
$F \implies G$	Füge F in die Menge der Annahmen hinzu und zeige G.
F oder G	Zeige: *nicht* $F \implies G$. (Alternativ zeige: *nicht* $G \implies F$.)
$F \iff G$	Zeige: $F \implies G$ *und* $G \implies F$.
$\forall x \in A : F$	Sei x ein beliebiges Element aus A. Zeige dann F.
$\exists x \in A : F$	Sei x ein konkretes Element aus A. Zeige dann F.

Auf diese Weise wächst im Laufe des Beweises die Menge der Annahmen.

Schreibweisen für Beweise

Beweise werden oft als Fließtext geschrieben. Ich persönlich bevorzuge es, Beweise wie folgt zu strukturieren:

Annahmen: $A_1, A_2, \ldots, A_n$.
Zu zeigen: Aussage F
Beweis: Es gelten $A_1, A_2, \ldots, A_n$.

$$
\begin{array}{lll}
\Longrightarrow & \text{Es folgt } F_1. & (\text{Begründung für } F_1) \\
\Longrightarrow & \text{Es folgt } F_2. & (\text{Begründung für } F_2) \\
\Longrightarrow & \text{Es folgt } F_3. & (\text{Begründung für } F_3) \\
 & \vdots &
\end{array}
$$

□

Zum Zeitpunkt, an dem die Folgerung F_i begründet werden muss, wurden alle Folgerungen $F_1, \ldots, F_{i-1}$ in die Menge der Annahmen hinzugefügt. D.h. man kann, um F_i zu begründen, alle Annahmen $A_1, \ldots, A_n$ und Folgerungen $F_1, \ldots, F_{i-1}$ benutzen.

Infos

- Man kann eine Folgerung kommentieren oder nicht (je nachdem wie trivial sie ist!)
- Man kann die benutzten Annahmen bzw. Aussagen über dem entsprechenden Implikationspfeil schreiben, z.B.:

$$\begin{aligned} &\xRightarrow{\text{Annahme 2}} && \dots \\ &\xRightarrow{\text{Lemma 25}} && \dots \\ &\xRightarrow{\text{Satz von Euler}} && \dots \end{aligned}$$

- Diese strukturierte Schreibweise wurde in Folien 276 - 325 oft benutzt. In den nächsten Beispielen wird sie für andere Beweise benutzt.

Erstes Beispiel

Satz:

> *Seien A und B endliche Mengen und $f : A \to B$ eine Funktion. Wenn f injektiv und nicht surjektiv ist, dann ist die Kardinalität von A kleiner als die von B.*

Annahmen:

- $|A|, |B| < \infty$,
- $f : A \to B$,
- f injektiv,
- f nicht surjektiv.

Zu zeigen: $|A| < |B|$.

Erstes Beispiel

Beweis: Aus den Annahmen folgt:

$$
\begin{array}{lll}
\Longrightarrow & \text{Für alle } b \in B \text{ gilt } |f^{-1}(b)| \leq 1. & (\text{da } f \text{ injektiv}) \\
\Longrightarrow & \text{Es gibt ein } b \in B \text{ mit } |f^{-1}(b)| = 0. & (\text{da } f \text{ nicht surjektiv}) \\
\Longrightarrow & |A| = \sum_{b \in B} |f^{-1}(b)| & (\text{s. Folie 498}) \\
& = \sum_{b \in B \setminus \{b'\}} |f^{-1}(b)| & (\text{sei } b' \in B \text{ mit } |f^{-1}(b')| = 0) \\
& \leq \sum_{b \in B \setminus \{b'\}} 1 & (\text{da } |f^{-1}(b)| \leq 1 \text{ für alle } b \in B) \\
& = |B| - 1 & (|B| - 1 \text{ Summanden in der Summe}) \\
& < |B|. & (\text{da } |A|, |B| < \infty)
\end{array}
$$

□

Zweites Beispiel

Satz:

Sei $n \in \mathbb{Z}$ ungerade. Dann ist auch n^2 ungerade.

Annahme: $n \in \mathbb{Z}$ ungerade.
Zu zeigen: $\exists k \in \mathbb{Z} : n^2 = 2k + 1$.
Beweis: Aus den Annahmen folgt:

$$
\begin{aligned}
&\Longrightarrow && \text{Es gibt ein } l \in \mathbb{Z} \text{ mit } n = 2l + 1. && \text{(da } n \text{ ungerade)} \\
&\Longrightarrow && n^2 = (2l+1)^2 \\
& && \quad = 4l^2 + 4l + 1 \\
& && \quad = 2(2l^2 + 2l) + 1. \\
&\Longrightarrow && \text{Es gibt ein } k \in \mathbb{Z} \text{ mit } n^2 = 2k + 1. && \text{(nämlich } k = (2l^2 + 2l).)
\end{aligned}
$$

□

Drittes Beispiel

Satz:

Sei $f : X \to Y$ eine Funktion und $M, N \subseteq Y$ beliebige Mengen. Dann gilt:

$$f^{-1}(M \cup N) \subseteq f^{-1}(M) \cup f^{-1}(N).$$

Annahmen:

- $f : X \to Y$,
- $M, N \subseteq Y$,
- $x \in f^{-1}(M \cup N)$ beliebig.

Zu zeigen: $f^{-1}(M \cup N) \subseteq f^{-1}(M) \cup f^{-1}(N)$.

Drittes Beispiel

Beweis: Sei $x \in f^{-1}(M \cup N)$ beliebig.

$$
\begin{array}{lll}
\Longrightarrow & x \in f^{-1}(M \cup N) & \text{(s. Folie 469)} \\
\Longrightarrow & f(x) \in M \cup N & \\
\Longrightarrow & f(x) \in M \text{ oder } f(x) \in N & \\
\Longrightarrow & x \in f^{-1}(M) \text{ oder } x \in f^{-1}(N) & \text{(s. Folie 469)} \\
\Longrightarrow & x \in f^{-1}(M) \cup f^{-1}(N) &
\end{array}
$$

□

Erinnerung: $A \subseteq B$ heißt nichts anderes als $\forall x \in A : x \in B$.

Viertes Beispiel

Satz:

Sei $f : X \to Y$ eine Funktion und $M, N \subseteq Y$ beliebige Mengen. Dann gilt:

$$M \subseteq N \implies f^{-1}(M) \subseteq f^{-1}(N).$$

Annahmen:

- $f : X \to Y$,
- $M, N \subseteq Y$,
- $M \subseteq N$,

Zu zeigen: $M \subseteq N \implies f^{-1}(M) \subseteq f^{-1}(N)$.

Viertes Beispiel

Beweis: Sei $x \in f^{-1}(M)$ beliebig.

$$\begin{array}{lll} \Longrightarrow & f(x) \in M & \text{(s. Folie 469)} \\ \Longrightarrow & f(x) \in N & \text{(wegen } M \subseteq N\text{)} \\ \Longrightarrow & x \in f^{-1}(N) & \text{(s. Folie 469)} \end{array}$$

□

Erinnerung: $A \subseteq B$ heißt nichts anderes als $\forall x \in A : x \in B$.

Wie kann man folgende Aussage beweisen?

Sei $f : X \to Y$ eine Funktion und $M \subseteq Y$ eine beliebige Menge. Dann gilt:

$$f^{-1}(\overline{M}) \subseteq \overline{f^{-1}(M)}.$$

Hinweise:

- Benutze Folie 469.
- Vergiss nicht, dass $A \subseteq B$ nichts anderes als $\forall x \in A : x \in B$ heißt.

Annahmen: $f : X \to Y$, $M \subseteq Y$ und $x \in f^{-1}(\overline{M})$ beliebig.
Zu Zeigen: $f^{-1}(\overline{M}) \subseteq \overline{f^{-1}(M)}$.
Beweis: Sei $x \in f^{-1}(\overline{M})$ beliebig.

$$
\begin{array}{lll}
\Longrightarrow & f(x) \in \overline{M}. & \text{(Folie 469)} \\
\Longrightarrow & f(x) \notin M. & \\
\Longrightarrow & x \notin f^{-1}(M). & \text{(Folie 469)} \\
\Longrightarrow & x \in \overline{f^{-1}(M)}. &
\end{array}
$$

□

Seien $f : A \to B$ und $g : B \to C$ beliebige Funktionen über Mengen A, B und C. Wie kann man folgende Implikationen beweisen?

1. f und g injektiv $\implies$ $g \circ f$ injektiv,
2. f und g surjektiv $\implies$ $g \circ f$ surjektiv,
3. $g \circ f$ injektiv $\implies$ f injektiv,
4. $g \circ f$ surjektiv $\implies$ g surjektiv.

Erinnerungen:

- Für ein beliebiges $x \in A$ gilt: $(g \circ f)(x) = g(f(x))$.
- Es gilt:

$$\begin{array}{lll} f \text{ injektiv} & \iff & (\forall a_1, a_2 \in A : f(a_1) = f(a_2) \implies a_1 = a_2) \\ f \text{ surjektiv} & \iff & \forall b \in B : \exists a \in A : f(a) = b \end{array}$$

1. Annahmen: $f : A \to B$ und $g : B \to C$ injektiv.
   Zu zeigen: $g \circ f$ injektiv, also:

$$\forall a_1, a_2 \in A : (g \circ f)(a_1) = (g \circ f)(a_2) \implies a_1 = a_2.$$

Beweis: Seien $a_1, a_2 \in A$ beliebige Elemente mit $(g \circ f)(a_1) = (g \circ f)(a_2)$.

$$\begin{array}{lll} \implies & g(f(a_1)) = g(f(a_2)). & \\ \implies & f(a_1) = f(a_2). & (\text{da } g \text{ injektiv}) \\ \implies & a_1 = a_2. & (\text{da } f \text{ injektiv}) \end{array}$$

□

2. Annahmen: $f : A \to B$ und $g : B \to C$ surjektiv.
   Zu zeigen: $g \circ f$ surjektiv, also:

$$\forall c \in C : \exists a \in A : (g \circ f)(a) = c.$$

Beweis: Sei $c \in C$ ein beliebiges Element.

$$\begin{array}{lll} \Longrightarrow & \text{Es gibt ein } b \in B \text{ mit } g(b) = c. & (\text{da } g \text{ surjektiv}) \\ \Longrightarrow & \text{Es gibt ein } a \in A \text{ mit } f(a) = b. & (\text{da } f \text{ surjektiv}) \\ \Longrightarrow & g(f(a)) = c. & \\ \Longrightarrow & \text{Es gibt also ein } a \in A \text{ mit } (g \circ f)(a) = g(f(a)) = c. & \end{array}$$

□

3. Annahme: $f : A \to B$ und $g : B \to C$ mit $g \circ f$ injektiv.
   Zu zeigen: f injektiv, also:

$$\forall a_1, a_2 \in A : f(a_1) = f(a_2) \implies a_1 = a_2.$$

Beweis: Seien $a_1, a_2 \in A$ beliebige Elemente mit $f(a_1) = f(a_2)$.

$$\begin{aligned} &\implies && g(f(a_1)) = g(f(a_2)). \\ &\implies && (g \circ f)(a_1) = (g \circ f)(a_2). \\ &\implies && a_1 = a_2. && \text{(da } g \circ f \text{ injektiv)} \end{aligned}$$

□

4. Annahme: $f : A \to B$ und $g : B \to C$ mit $g \circ f$ surjektiv.
   Zu zeigen: g surjektiv, also:

$$\forall c \in C : \exists b \in B : g(b) = c.$$

Beweis: Sei $c \in C$ ein beliebiges Element.

$$\begin{array}{lll} \Longrightarrow & \text{Es gibt ein } a \in A \text{ mit } (g \circ f)(a) = c. & (\text{da } g \circ f \text{ surjektiv}) \\ \Longrightarrow & g(f(a)) = c. & \\ \Longrightarrow & \text{Es gibt also ein } b \in B \text{ mit } g(b) = c. & (\text{nämlich } b = f(a)) \end{array}$$

□

Modus Ponens

Seien p und q beliebige Aussagen. Falls wir wissen, dass q aus p folgt und dass p gilt, dann wissen wir, dass q gelten muss:

$$\big((p \to q) \wedge p\big) \to q$$

Da der Modus Ponens eine Tautologie ist wird er häufig bei Beweisen als Schlussregel verwendet.

p	q	$((p$	$\to$	$q)$	$\wedge$	$p)$	$\to$	q
0	0	0	1	0	0	0	1	0
0	1	0	1	1	0	0	1	1
1	0	1	0	0	0	1	1	0
1	1	1	1	1	1	1	1	1

Beweistypen für Implikationen

Die meisten Aussagen in der Mathematik sind Implikationen, d.h. sie haben die Gestalt

$$F \implies G.$$

Solche Aussagen kann man auf verschiedenen Weisen beweisen:

- Direkter Beweis:

  „Füge F in die Menge der Annahmen hinzu und zeige G."

- Indirekter Beweis:

  „Füge *nicht* G in die Menge der Annahmen hinzu und zeige *nicht* F."

- Beweis durch Widerspruch:

  „Füge F und *nicht* G in die Menge der Annahmen hinzu und zeige ein Widerspruch."

Als logische Formeln formuliert, entspricht der direkte Beweis der Formel $F \to G$, der indirekte Beweis der Formel $\neg G \to \neg F$ und der Beweis durch Widerspruch der Formel $(F \wedge \neg G) \to \text{false}$.

Diese Beweismethoden sind korrekt, weil die drei Formeln äquivalent zueinander sind:

F	G	F	$\to$	G	$\neg G$	$\to$	$\neg F$	$(F$	$\wedge$	$\neg G)$	$\to$	false
0	0	0	1	0	1	1	1	0	0	1	1	0
0	1	0	1	1	0	1	1	0	0	0	1	0
1	0	1	0	0	1	0	0	1	1	1	0	0
1	1	1	1	1	0	1	0	1	0	0	1	0

Themenübersicht

Vollständige Induktion

Für Aussagen der Form

$$\text{„Für alle } n \in \mathbb{N}_0 \text{ mit } n \geq n_0 \text{ gilt die Aussage } A(n)\text{“}$$

reicht es, die Aussagen

$$A(n_0) \quad \text{und} \quad \forall n \geq n_0 : (A(n) \implies A(n+1))$$

zu beweisen. $A(n_0)$ wird Induktionsanfang (I.A.) und $\forall n \geq n_0 : A(n) \implies A(n+1)$ Induktionsschritt.

Um den Induktionsschritt zu zeigen, zeigen wir den Induktionsschluss (I.S.) $A(n+1)$, unter der Annahme, dass die Induktionsvoraussetzung (I.V.) $A(n)$ für ein beliebiges aber festes $n \geq n_0$ gilt.

Infos

- Bei Induktionsbeweisen beweisen eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$ nach folgendem Domino-Prinzip:

$$A(n_0) \implies A(n_0+1) \implies A(n_0+2) \implies A(n_0+3) \implies A(n_0+4) \implies \dots$$

- Man nennt den Induktionsanfang auch Induktionsbasis und die Induktionsvoraussetzung auch Induktionsannahme.

Beispiel

Satz:

Sei $x \in \mathbb{R}$ beliebig mit $x > -1$. Dann gilt für alle $n \in \mathbb{N}_0$: $(1+x)^n \geq 1 + nx$.

Beweis:

I.A. Für $n = 0$: $(1+x)^0 = 1 = 1 + 0x$. ✓

I.V. Angenommen, es gilt $(1+x)^n \geq 1 + nx$ für ein beliebiges aber festes $n \in \mathbb{N}_0$.

Beispiel

I.S.

$$
\begin{aligned}
(1+x)^{n+1} &= (1+x)\cdot(1+x)^n \\
&\overset{\text{I.V.}}{\geq} (1+x)\cdot(1+nx) \\
&= 1+x+nx+nx^2 \\
&\geq 1+x+nx && (nx^2 \geq 0 \text{ da } n, x^2 \geq 0) \\
&= 1+(n+1)x
\end{aligned}
$$

□

Noch ein Beispiel

Satz:

Für alle $n \in \mathbb{N}_0$ mit $n \geq 4$ gilt: $2^n \geq n^2$.

Beweis:

I.A. Für $n = 4$: $2^4 = 16 = 4^2$. ✓

I.V. Angenommen, es gilt $2^n \geq n^2$ für ein beliebiges aber festes $n \in \mathbb{N}_0$ mit $n \geq 4$.

I.S.

$$2^{n+1} = 2 \cdot 2^n \overset{\text{I.V.}}{\geq} 2 \cdot n^2 = n^2 + n \cdot n \overset{(*)}{\geq} n^2 + 4n = n^2 + 2n + 2n$$
$$\overset{(*)}{\geq} n^2 + 2n + 2 \cdot 4 \geq n^2 + 2n + 1 = (n+1)^2$$

Bei $(*)$ wurde die Annahme $n \geq 4$ benutzt. □

Ein letztes Beispiel

Satz:

> *Für alle $n \in \mathbb{N}_0$ gilt: Eine Pizza lässt sich mit n geraden Schnitten in höchstens $\frac{n(n+1)}{2} + 1$ Stücken teilen.*

Beweis:

I.A. Für $n = 0$: Mit keinem Schnitt ist die Pizza noch ganz, d.h. sie besteht aus einem Stück. Tatsächlich gilt: $\frac{0(0+1)}{2} + 1 = 1$. ✓

I.V. Angenommen, für ein beliebiges, aber festes $n \in \mathbb{N}_0$ lässt sich die Pizza mit n geraden Schnitten in höchstens $\frac{n(n+1)}{2} + 1$ Stücken teilen.

Ein letztes Beispiel

I.S. Der $(n+1)$-te Schnitt schneidet jeden der ersten n Schnitte höchstens einmal. In diesem Fall würde man genau $n+1$ Stücke zweiteilen. Durch den $(n+1)$-ten Schnitt, kommen also zu den höchstens $\frac{n(n+1)}{2}+1$ Stücken höchstens $n+1$ dazu. Das ergibt:

$$\begin{aligned}\frac{n(n+1)}{2}+1+n+1 &= \frac{n(n+1)+2(n+1)}{2}+1\\ &= \frac{n^2+3n+2}{2}+1\\ &= \frac{(n+1)(n+2)}{2}+1\end{aligned}$$

Pizzastücke.

Ein letztes Beispiel

Wieso entstehen $n+1$ neue Stücke, wenn man mit dem $(n+1)$-ten Schnitt alle anderen n Schnitte trifft?

Zwischen je zwei getroffenen Schnitten befindet sich ein Stück Pizza und vor dem ersten und nach dem letzten Schnitt jeweils auch eins. Im Bild haben wir mit dem 5. Schnitt alle anderen 4 getroffen. Dadurch sind 5 neue Stücke entstanden.

Rezept

Frage: Wie beweist man eine Aussage $A(n)$ über eine Summe $\sum_{k=n_0}^{n} a_k$ bzw. über ein Produkt $\prod_{k=n_0}^{n} a_k$?

Methode:

I.A. n_0 für n einsetzen und die Aussage $A(n_0)$ überprüfen.

I.V. „Angenommen, es gilt $A(n)$ für ein beliebiges, aber festes $n \geq n_0$."

Rezept

I.S. Die Aussage $A(n+1)$ auf $A(n)$ mit folgendem Trick zurückführen und die I.V. auf $\sum_{k=n_0}^{n} a_k$ bzw. $\prod_{k=n_0}^{n} a_k$ anwenden:

$$\sum_{k=n_0}^{n+1} a_k = \underbrace{a_1 + \ldots + a_n}_{\sum_{k=n_0}^{n} a_k} + a_{n+1} = \sum_{k=n_0}^{n} a_k + a_{n+1}$$

$$\prod_{k=n_0}^{n+1} a_k = \underbrace{a_1 \cdot \ldots \cdot a_n}_{\prod_{k=n_0}^{n} a_k} \cdot a_{n+1} = \prod_{k=n_0}^{n} a_k \cdot a_{n+1}$$

Beispiel

Satz:

Für alle $n \in \mathbb{N}_0$ gilt: $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.

Beweis:

I.A. Für $n = 0$: $\sum_{k=0}^{0} 2^k = 2^0 = 1 = 2 - 1 = 2^{0+1} - 1$. ✓

I.V. Angenommen, es gilt $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$ für ein beliebiges, aber festes $n \in \mathbb{N}_0$.

I.S.

$$\sum_{k=0}^{n+1} 2^k = \sum_{k=0}^{n} 2^k + 2^{n+1} \overset{\text{I.V.}}{=} (2^{n+1} - 1) + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1.$$

□

Noch ein Beispiel

Satz:

Für alle $n \in \mathbb{N}$ gilt: $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Beweis:

I.A. Für $n = 1$: $\sum_{k=1}^{1} k = 1 = \frac{1 \cdot (1+1)}{2}$. ✓

I.V. Angenommen, es gilt $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ für ein beliebiges, aber festes $n \in \mathbb{N}$.

I.S.

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + n + 1 \overset{\text{I.V.}}{=} \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}.$$

□

Ein letztes Beispiel

Satz:

Für alle $n \in \mathbb{N}_0$ gilt: $\prod_{k=0}^{n} 9^k = 3^{n(n+1)}$.

Beweis:

I.A. Für $n = 0$: $\prod_{k=0}^{0} 9^k = 9^0 = 1 = 3^0 = 3^{0(0+1)}$. ✓

I.V. Angenommen, es gilt $\prod_{k=0}^{n} 9^k = 3^{n(n+1)}$ für ein beliebiges, aber festes $n \in \mathbb{N}$.

I.S.

$$\prod_{k=0}^{n+1} 9^k = \prod_{k=0}^{n} 9^k \cdot 9^{n+1} \overset{\text{I.V.}}{=} 3^{n(n+1)} \cdot 9^{n+1} = 3^{n(n+1)} \cdot 3^{2(n+1)}$$
$$= 3^{n(n+1)+2(n+1)} = 3^{n^2+3n+2} = 3^{(n+1)(n+2)}.$$

□

Quizfrage

Wie kann folgender Satz mit vollständiger Induktion bewiesen werden?

Für alle $n \in \mathbb{N}_0$ *gilt:* $\sum_{k=0}^{n} \frac{1}{2^{k+1}} = 1 - \frac{1}{2^{n+1}}$.

Beweis:

I.A. Für $n = 0$: $\sum_{k=0}^{0} \frac{1}{2^{k+1}} = \frac{1}{2^{0+1}} = \frac{1}{2} = 1 - \frac{1}{2^{0+1}}$ ✓

I.V. Angenommen, es gilt $\sum_{k=0}^{n} \frac{1}{2^{k+1}} = 1 - \frac{1}{2^{n+1}}$ für ein beliebiges, aber festes $n \in \mathbb{N}_0$.

I.S.

$$\begin{aligned}\sum_{k=0}^{n+1} \frac{1}{2^{k+1}} &= \sum_{k=0}^{n} \frac{1}{2^{k+1}} + \frac{1}{2^{n+2}} \overset{\text{I.V.}}{=} \left(1 - \frac{1}{2^{n+1}}\right) + \frac{1}{2^{n+2}} \\ &= 1 - \frac{2}{2^{n+2}} + \frac{1}{2^{n+2}} = 1 - \frac{1}{2^{n+2}}\end{aligned}$$

□

Wie kann folgender Satz mit vollständiger Induktion bewiesen werden?

Für alle $n \in \mathbb{N}$ gilt: $\sum_{k=1}^{n}(2k-1) = n^2$.

Beweis:

I.A. Für $n =: \sum_{k=1}^{1}(2k-1) = 2 \cdot 1 - 1 = 1 = 1^2$ ✓

I.V. Angenommen, es gilt $\sum_{k=1}^{n}(2k-1) = n^2$ für ein beliebiges, aber festes $n \in \mathbb{N}$.

I.S.

$$\sum_{k=1}^{n+1}(2k-1) = \sum_{k=1}^{n}(2k-1) + 2(n+1) - 1 \overset{\text{I.V.}}{=} n^2 + 2(n+1) - 1 = (n+1)^2.$$

□

Sei $q \in \mathbb{R} \setminus \{0, 1\}$ beliebig. Wie kann folgender Satz mit vollständiger Induktion bewiesen werden?

Für alle $n \in \mathbb{N}_0$ *gilt:* $\sum_{k=0}^{n} q^k = \frac{q^{n+1}-1}{q-1}$.

Beweis: Sei $q \in \mathbb{R} \setminus \{0, 1\}$ beliebig.

I.A. Für $n = 0$: $\sum_{k=0}^{0} q^k = q^0 = 1 = \frac{q^{0+1}-1}{q-1}$. ✓

I.V. Angenommen, es gilt $\sum_{k=0}^{n} q^k = \frac{q^{n+1}-1}{q-1}$ für ein beliebiges, aber festes $n \in \mathbb{N}_0$.

I.S.

$$\sum_{k=0}^{n+1} q^k = \sum_{k=0}^{n} q^k + q^{n+1} \overset{\text{I.V.}}{=} \frac{q^{n+1}-1}{q-1} + q^{n+1} = \frac{q^{n+1}-1+q^{n+1}(q-1)}{q-1} = \frac{q^{n+2}-1}{q-1}.$$

□

Wie kann folgender Satz mit vollständiger Induktion bewiesen werden?

Für alle $n \in \mathbb{N}$ *gilt:* $\sum_{k=1}^{n}(2k-1)^2 = \frac{4n^3-n}{3}$.

Beweis:

I.A. Für $n = 1$: $\sum_{k=1}^{1}(2k-1)^2 = (2\cdot 1 - 1)^2 = 1 = \frac{4\cdot 1^3 - 1}{3}$. ✓

I.V. Angenommen, es gilt $\sum_{k=1}^{n}(2k-1)^2 = \frac{4n^3-n}{3}$ für ein beliebiges, aber festes $n \in \mathbb{N}$.

I.S.

$$\begin{aligned}\sum_{k=1}^{n+1}(2k-1)^2 &= \sum_{k=1}^{n}(2k-1)^2 + (2(n+1)-1)^2 \overset{\text{I.V.}}{=} \frac{4n^3-n}{3} + (2(n+1)-1)^2 \\ &= \frac{4n^3 - n + 3(2n+1)^2}{3} = \frac{4n^3 + 12n^2 + 12n - n + 3}{3} \\ &= \frac{4(n^3+3n^2+3n+1) - (n+1)}{3} = \frac{4(n+1)^3 - (n+1)}{3}.\end{aligned}$$

□

Quizfrage

Wie kann folgender Satz mit vollständiger Induktion bewiesen werden?

Für alle $n \in \mathbb{N}$ *gilt:* $\prod_{k=1}^{n} \left(1 + \frac{2}{k}\right) = \frac{(n+1)(n+2)}{2}$.

Beweis:

I.A. Für $n = 1$: $\prod_{k=1}^{1}\left(1+\frac{2}{k}\right) = 1+\frac{2}{1} = 3 = \frac{(1+1)(1+2)}{2}$. ✓

I.V. Angenommen, es gilt $\prod_{k=1}^{n}\left(1+\frac{2}{k}\right) = \frac{(n+1)(n+2)}{2}$ für ein beliebiges, aber festes $n \in \mathbb{N}$.

I.S.

$$\begin{aligned}\prod_{k=1}^{n+1}\left(1+\frac{2}{k}\right) &= \left(\prod_{k=1}^{n}\left(1+\frac{2}{k}\right)\right)\cdot\left(1+\frac{2}{n+1}\right) \overset{\text{I.V.}}{=} \frac{(n+1)(n+2)}{2}\cdot\left(1+\frac{2}{n+1}\right)\\ &= \frac{(n+1)(n+2)}{2}\cdot\left(\frac{n+1}{n+1}+\frac{2}{n+1}\right) = \frac{(n+1)(n+2)}{2}\cdot\left(\frac{n+3}{n+1}\right)\\ &= \frac{(n+2)(n+3)}{2}.\end{aligned}$$

□

Wie kann folgender Satz mit vollständiger Induktion bewiesen werden?

Für alle $n \in \mathbb{N}_0$ *und* $x \in \mathbb{R} \setminus \{1\}$ *gilt:* $\prod_{k=0}^{n} \left(1 + x^{2^k}\right) = \frac{1-x^{2^{n+1}}}{1-x}$.

Vorsicht:

$$a^{b^c} = a^{(b^c)} \neq (a^b)^c = a^{b \cdot c}.$$

Beweis: Sei $x \in \mathbb{R} \setminus \{1\}$ beliebig.

I.A. Für $n = 0$: $\prod_{k=0}^{0}\left(1 + x^{2^k}\right) = 1 + x^{2^0} = 1 + x = \frac{(1+x)(1-x)}{1-x} = \frac{1-x^{2^{0+1}}}{1-x}$. ✓

I.V. Angenommen, es gilt $\prod_{k=0}^{n}\left(1 + x^{2^k}\right) = \frac{1-x^{2^{n+1}}}{1-x}$ für ein beliebiges, aber festes $n \in \mathbb{N}_0$.

I.S.

$$\prod_{k=0}^{n+1}\left(1 + x^{2^k}\right) = \prod_{k=0}^{n}\left(1 + x^{2^k}\right) \cdot \left(1 + x^{2^{n+1}}\right) \overset{\text{I.V.}}{=} \frac{1 - x^{2^{n+1}}}{1 - x} \cdot \left(1 + x^{2^{n+1}}\right)$$

$$= \frac{\left(1 - x^{2^{n+1}}\right)\left(1 + x^{2^{n+1}}\right)}{1 - x} \overset{(*)}{=} \frac{1 - \left(x^{2^{n+1}}\right)^2}{1 - x} = \frac{1 - x^{\left(2^{n+2}\right)}}{1 - x}.$$

Bei $(*)$ wurde die dritte binomische Formel benutzt: $(a + b)(a - b) = a^2 - b^2$. □

Seien $a_1, \ldots, a_n \in \mathbb{R}$ beliebige reelle Zahlen mit $a_1, \ldots, a_n > 0$. Wie kann folgender Satz mit vollständiger Induktion bewiesen werden?

Für alle $n \in \mathbb{N}$ *mit* $n \geq 2$ *gilt:* $\prod_{k=1}^{n}(1 + a_k) > 1 + \prod_{k=1}^{n} a_k$.

Beweis: Seien $a_1, \ldots, a_n \in \mathbb{R}$ beliebige reelle Zahlen mit $a_1, \ldots, a_n > 0$.

I.A. Für $n = 2$: $(1 + a_1) \cdot (1 + a_2) = 1 + \underbrace{a_1 + a_2}_{>0} + a_1 \cdot a_2 > 1 + a_1 \cdot a_2$. ✓

I.V. Angenommen, es gilt $\prod_{k=1}^{n}(1 + a_k) > 1 + \prod_{k=1}^{n} a_k$ für ein beliebiges aber festes $n \geq 2$.

I.S.

$$\begin{aligned}\prod_{k=1}^{n+1}(1+a_k) &= \prod_{k=1}^{n}(1+a_k)\cdot(1+a_{n+1}) \\ &\overset{\text{I.V.}}{>} \left(1+\prod_{k=1}^{n}a_k\right)\cdot(1+a_{n+1}) \\ &= 1+\underbrace{\prod_{k=1}^{n}a_k+a_{n+1}}_{>0}+\prod_{k=1}^{n+1}a_k > 1+\prod_{k=1}^{n+1}a_k\end{aligned}$$

□

Seien $A_1, \ldots, A_n$ beliebige Mengen. Wie kann folgender Satz mit vollständiger Induktion bewiesen werden?

Für alle $n \in \mathbb{N}$ gilt:

$$\overline{\bigcup_{k=1}^{n} A_k} = \bigcap_{k=1}^{n} \overline{A_k}.$$

Hinweise:

- Der Fall $n = 2$ entspricht genau der Regel von De Morgan: $\overline{A \cup B} = \overline{A} \cap \overline{B}$. Diese darf als bewiesen angenommen und im Beweis benutzt werden.
- Der Ausdruck $\bigcup_{k=1}^{n} A_k$ ist zwar weder eine Summe noch ein Produkt, aber das Prinzip lässt sich hier auch anwenden ;-)

Beweis: Sei $A_1, A_2, \ldots$ eine Folge beliebiger Mengen.

I.A. Für $n = 1$: $n \in \mathbb{N}$: $\overline{\bigcup_{k=1}^{1} A_k} = \overline{A_1} = \bigcap_{k=1}^{1} \overline{A_k}$. ✓

I.V. Angenommen, es gilt $\overline{\bigcup_{k=1}^{n} A_k} = \bigcap_{k=1}^{n} \overline{A_k}$ für ein beliebiges, aber festes $n \in \mathbb{N}$.

I.S.

$$\overline{\bigcup_{k=0}^{n+1} A_k} = \overline{\bigcup_{k=0}^{n} A_k \cup A_{n+1}} \overset{(*)}{=} \overline{\bigcup_{k=0}^{n} A_k} \cap \overline{A_{n+1}} \overset{\text{I.V.}}{=} \bigcap_{k=0}^{n} \overline{A_k} \cap \overline{A_{n+1}} = \bigcap_{k=0}^{n+1} \overline{A_k}.$$

Bei $(*)$ wurde die Regel von De Morgan benutzt. □

Rekursionsgleichungen

Sei $f : \mathbb{N}_0 \to \mathbb{R}$ eine beliebige Funktion und $n \in \mathbb{N}_0$. Eine Rekursionsgleichung vom Grad d ist eine Gleichung, die den Funktionswert $f(n+1)$ in Abhängigkeit von $f(n), f(n-1), \ldots, f(n-d+1)$ darstellt. Gibt man zu einer solchen Rekursionsgleichung auch die sogenannten Anfangsbedingungen $f(0), f(1), \ldots, f(d-1)$ mit an, so wird f eindeutig definiert.

Beispiel

Die Funktion $f(n) = n^2$ kann durch die Rekursionsgleichung

$$f(n+1) = 3f(n) - 3f(n-1) + f(n-2)$$

vom Grad 3 mit Anfangsbedingungen $f(0) = 0$, $f(1) = 1$ und $f(2) = 4$ definiert werden.

Es gilt $f(0) = 0$, $f(1) = 1$, $f(2) = 4$ und:

$$\begin{array}{rcccl} f(3) & = & 3f(2) - 3f(1) + f(0) & = & 9 \\ f(4) & = & 3f(3) - 3f(2) + f(1) & = & 16 \\ f(5) & = & 3f(4) - 3f(3) + f(2) & = & 25 \\ f(6) & = & 3f(5) - 3f(4) + f(3) & = & 36 \\ f(7) & = & 3f(6) - 3f(5) + f(4) & = & 49 \\ f(8) & = & 3f(7) - 3f(6) + f(5) & = & 64 \\ & \vdots & & & \end{array}$$

Rezept

Frage: Sei $f : \mathbb{N}_0 \to \mathbb{R}$ eine Funktion. Wie beweist man, zu einer gegeben Rekursionsgleichung von Grad d für f mit Anfangsbedingungen $f(0), f(1), \ldots, f(d-1)$, eine Aussage $A(n)$ über $f(n)$?

Methode:

I.A. $A(n)$ für $n = 0, \ldots, d-1$ mithilfe der Anfangsbedingungen überprüfen.

I.V. „Angenommen, es gelten $A(n), A(n-1), \ldots, A(n-d+1)$ für ein beliebiges, aber festes $n \geq d-1$."

I.S. Mithilfe der Rekursionsgleichung $f(n+1)$ auf $f(n), f(n-1), \ldots, f(n-d+1)$ zurückführen und die I.V. auf sie alle anwenden.

Der entstehende Domino-Effekt bei solchen Beweisen ist:

$$
\begin{aligned}
A(0), \ldots, A(d-1) &\overset{A(0),\ldots,A(d-1)}{\Longrightarrow} A(d) \\
&\overset{A(1),\ldots,A(d)}{\Longrightarrow} A(d+1) \\
&\overset{A(2),\ldots,A(d+1)}{\Longrightarrow} A(d+2) \\
&\overset{A(3),\ldots,A(d+2)}{\Longrightarrow} A(d+3) \\
&\overset{A(4),\ldots,A(d+3)}{\Longrightarrow} A(d+4) \\
&\vdots
\end{aligned}
$$

Beispiel

Satz:

Sei $f : \mathbb{N}_0 \to \mathbb{N}_0$ *eine Funktion mit* $f(0) = 0$ *und*

$$f(n+1) = f(n) + 2n + 1$$

für alle $n \geq 0$. *Dann gilt für alle* $n \in \mathbb{N}_0$: $f(n) = n^2$.

Der Grad dieser Rekursionsgleichung ist 1.

Beweis:

I.A. Für $n = 0$: $f(0) = 0 = 0^2$. ✓

I.V. Angenommen, es gilt $f(n) = n^2$ für ein beliebiges aber festes $n \in \mathbb{N}_0$.

I.S.

$$f(n+1) = f(n) + 2n + 1 \overset{\text{I.V.}}{=} n^2 + 2n + 1 = (n+1)^2. \qquad \square$$

Noch ein Beispiel

Satz:

Sei $f : \mathbb{N}_0 \to \mathbb{N}_0$ *eine Funktion mit* $f(0) = 1$, $f(1) = 3$, $f(2) = 5$ *und*

$$f(n+1) = 3f(n) - 3f(n-1) + f(n-2)$$

für alle $n \geq 3$. *Dann gilt für alle* $n \in \mathbb{N}_0$: $f(n) = 2n + 1$.

Der Grad dieser Rekursionsgleichung ist 3.

Noch ein Beispiel

Beweis:

I.A.

$$\begin{aligned} n = 0: &\quad f(0) = 2 \cdot 0 + 1 = 1 \quad \checkmark \\ n = 1: &\quad f(1) = 2 \cdot 1 + 1 = 3 \quad \checkmark \\ n = 2: &\quad f(2) = 2 \cdot 2 + 1 = 5 \quad \checkmark \end{aligned}$$

I.V. Angenommen, es gelten die Gleichungen

$$f(n) = 2n + 1, \quad f(n-1) = 2(n-1) + 1, \quad f(n-2) = 2(n-2) + 1$$

für ein beliebiges, aber festes $n \in \mathbb{N}_0$ mit $n \geq 3$.

I.S.

$$\begin{aligned} f(n+1) &= 3f(n) - 3f(n-1) + f(n-2) \\ &\overset{\text{I.V.}}{=} 3(2n+1) - 3(2(n-1)+1) + (2(n-2)+1) = 2n + 3 = 2(n+1) + 1. \quad \square \end{aligned}$$

Ein letztes Beispiel

Satz:

Sei $f : \mathbb{N}_0 \to \mathbb{N}_0$ *eine Funktion mit* $f(0) = 0$, $f(1) = 4$ *und*

$$f(n+1) = 2f(n) + 3f(n-1)$$

für alle $n \geq 2$. *Dann ist* $f(n)$ *für alle* $n \in \mathbb{N}_0$ *gerade.*

Der Grad dieser Rekursionsgleichung ist 2.

Ein letztes Beispiel

Beweis:

I.A.

$$\begin{aligned} n = 0: &\quad f(0) = 0 \text{ ist gerade} \quad \checkmark \\ n = 1: &\quad f(1) = 4 \text{ ist gerade} \quad \checkmark \end{aligned}$$

I.V. Angenommen, $f(n)$ und $f(n-1)$ sind für ein beliebiges, aber festes $n \in \mathbb{N}_0$ mit $n \geq 2$ beide gerade.

I.S. Weil $f(n)$ und $f(n-1)$ laut I.V. gerade sind, sind auch $2f(n)$ und $3f(n-1)$ gerade. Daraus folgt, dass $f(n+1) = 2f(n) + 3f(n-1)$ ebenfalls gerade ist, da die Summe von geraden Zahlen wieder gerade ist. □

Sei $f : \mathbb{N}_0 \to \mathbb{N}_0$ eine Funktion mit $f(0) = 0$, $f(1) = 2$ und

$$f(n+1) = 3f(n) - 2f(n-1)$$

für alle $n \geq 1$.

Wie kann man mit vollständiger Induktion beweisen, dass $f(n) = 2^{n+1} - 2$ für alle $n \in \mathbb{N}_0$ gilt?

Hinweis: Die Rekursionsgleichung hat Grad 2.

Beweis:

I.A.

$$\begin{aligned} n = 0: &\quad f(0) = 2^1 - 2 = 2 - 2 = 0 \qquad \checkmark \\ n = 1: &\quad f(1) = 2^2 - 2 = 4 - 2 = 2 \qquad \checkmark \end{aligned}$$

I.V. Angenommen, es gelten die Gleichungen

$$f(n) = 2^{n+1} - 2 \quad \text{und} \quad f(n-1) = 2^n - 2$$

für ein beliebiges, aber festes $n \geq 1$.

I.S.

$$\begin{aligned} f(n+1) &= 3f(n) - 2f(n-1) \overset{\text{I.V.}}{=} 3(2^{n+1} - 2) - 2(2^n - 2) \\ &= 3 \cdot 2^{n+1} - 6 - 2 \cdot 2^n + 4 = 3 \cdot 2^{n+1} - 2^{n+1} - 2 \\ &= (3-1)2^{n+1} - 2 = 2 \cdot 2^{n+1} - 2 = 2^{n+2} - 2 \end{aligned}$$

□

Ein Gartenzaun besteht aus n nebeneinander stehenden Pfählen. Jeder Pfahl soll mit einer der Farben gelb, rot und blau so gestrichen werden, dass die Anzahl an blauen Pfählen gerade ist. Sei $f(n)$ die Anzahl an Farbkombinationen bei n Pfählen.

1. Wieso gilt $f(n+1) = f(n) + 3^n$ mit $f(1) = 2$?
2. Wie kann man mit vollständiger Induktion die Gleichung $f(n) = \frac{3^n+1}{2}$ für alle $n \in \mathbb{N}$ zeigen?

Hinweise zu 1.:

- Stell $f(n+1)$ zunächst in Abhängigkeit von $f(n)$ dar.
- Für n Pfähle gibt es insgesamt 3^n Farbkombinationen. Bei $f(n)$ davon ist die Anzahl an blauen Pfählen gerade, bei $3^n - f(n)$ ungerade.

1. Möchte man $n+1$ Pfähle farbig streichen, so muss man für den $(n+1)$-ten Pfahl folgende drei Fälle betrachten:

$$(\underbrace{?,?,\ldots,?}_{\text{blau gerade}},g) \qquad (\underbrace{?,?,\ldots,?}_{\text{blau gerade}},r) \qquad (\underbrace{?,?,\ldots,?}_{\text{blau ungerade}},b).$$

Für die ersten zwei Fälle gibt es jeweils $f(n)$ Möglichkeiten, für den dritten sind es $3^n - f(n)$. Wir erhalten also die Formel

$$f(n+1) = f(n) + f(n) + 3^n - f(n).$$

Es folgt $f(n+1) = f(n) + 3^n$ mit $f(1) = 2$.

2. Beweis:

I.A. Für $n = 1$: $f(1) = 2 = \frac{3^1+1}{2}$. ✓

I.V. Angenommen, es gilt $f(n) = \frac{3^n+1}{2}$ für ein beliebiges aber festes $n \in \mathbb{N}$.

I.S.

$$f(n+1) = f(n) + 3^n \overset{\text{I.V.}}{=} \frac{3^n+1}{2} + 3^n = \frac{3^n+1+2\cdot 3^n}{2} = \frac{3\cdot 3^n+1}{2} = \frac{3^{n+1}+1}{2}.$$

□

Info

Noch nicht genug gehabt? Noch durstig nach Induktionsaufgaben? Versuchts doch hiermit:

`http://www.emath.de/Referate/induktion-[]aufgaben-[]loesungen.pdf`

Themengebiete A-E sind für uns interessant.

Starke Induktion

Die starke Induktion funktioniert analog zur vollständigen Induktion mit dem Unterschied, dass der Induktionsschritt die Gestalt

$$\forall n \geq n_0 : (A(n_0), \ldots, A(n)) \implies A(n+1)$$

hat. D.h. man hat eine Menge $\{A(n_0), \ldots, A(n)\}$ von Annahmen zur Verfügung.

Die starke Induktion ist ein Spezialfall der vollständigen Induktion bei der man die Aussage $A(n)$ aus Folie 169 durch $\forall k \leq n$: $A(k)$ ersetzt wird.

Beispiel

Satz:

Sei $f : \mathbb{N}_0 \to \mathbb{N}_0$ eine Funktion mit $f(0) = 1$ und $f(n+1) = 1 + \sum_{k=0}^{n} f(k)$. Dann gilt für alle $n \in \mathbb{N}_0$: $f(n) = 2^n$.

Beweis:

I.A. Für $n = 0$: $f(0) = 1 = 2^0$. ✓

I.V. Angenommen, es gilt für ein beliebiges aber festes $n \in \mathbb{N}_0$ die Gleichung $f(k) = 2^k$ für alle $k = 0, \ldots, n$, d.h.: $f(0) = 1, f(1) = 2, f(2) = 4, \ldots, f(n) = 2^n$.

I.S.

$$f(n+1) = 1 + \sum_{k=0}^{n} f(k) \overset{\text{I.V.}}{=} 1 + \sum_{k=0}^{n} 2^k \overset{(*)}{=} 1 + (2^{n+1} - 1) = 2^{n+1}. \qquad \square$$

$(*)$ siehe Folie 179.

Themenübersicht

Relationen

- R ist eine binäre Relation über den Mengen A und B, falls gilt:

$$R \subseteq A \times B.$$

  Man nennt dann A die Quellmenge und B die Zielmenge von R.

- R ist eine homogene binäre Relation über der Menge A, falls gilt:

$$R \subseteq A \times A.$$

  Man nennt dann A die Grundmenge von R.

Infos

- Weil wir in der Vorlesung nur binäre Relationen betrachten, lassen wir das Wort *binär* immer weg!
- Homogene Relationen sind Relationen, bei denen die Quell- und die Zielmenge gleich sind.

Beispiele

- Eine abstrakte Relation über [2] und [4] ist:

$$R = \{(1,1),(1,3),(2,3),(2,4)\}\,.$$

- Eine abstrakte homogene Relation über [3] ist:

$$R = \{(1,1),(1,3),(2,3),(3,1),(3,3)\}\,.$$

- Bekannte homogene Relationen über $\mathbb{Z}$ sind $=$, $\neq$, $\leq$, und $<$.
- Sei A eine beliebige Menge. Bekannte homogene Relationen über $\mathcal{P}(A)$ sind $=$, $\neq$, $\subseteq$, $\not\subseteq$, $\subset$ und $\not\subset$.
- Sei A wieder eine beliebige Menge. Eine bekannte Relation über A und $\mathcal{P}(A)$ ist die Elementrelation $\in$.

Infos

Wir benutzen oft die Infixnotation $a\,R\,b$ anstatt der normalen Notation $(a, b) \in R$. Wir benutzen die Infixnotation vor allem dann, wenn wir ein tolles Relationensymbol für R haben. Beispielsweise ist $3 \leq 5$ nichts anderes als die Infixnotation für $(3, 5) \in \leq$, was zwar eigentlich korrekt wäre, aber schrecklich aussieht!

Für $(a, b) \notin R$ benutzen wir einfach $a \not R\ b$. So kann beispielsweise $5 \neq 7$ sowohl für $(5, 7) \notin =$ als auch für $(5, 7) \in \neq$ stehen, falls man $\neq$ als eigene Relation auffassen möchte.

Quizfrage

Wie viele verschiedene Relationen über [3] und [4] gibt es?

So viele, wie es Teilmengen von $[3] \times [4]$ gibt. Insgesamt gibt es also

$$|\mathcal{P}([3] \times [4])| = 2^{|[3]\times[4]|} = 2^{12} = 4096$$

solche Relationen.

Einschränkung

Oft möchte man nur einen Teil der Relation betrachten. Hierfür sind Einschränkungen hilfreich.

- Seien A, A', B, B' Mengen mit $A' \subseteq A$ und $B' \subseteq B$ und R eine Relation über A und B. Dann ist die Einschränkung von R auf A' und B' gegeben durch:

$$R \cap (A' \times B').$$

- Seien A und A' zwei Mengen mit $A' \subseteq A$ und R eine homogene Relation über A. Dann ist die Einschränkung von R auf A' gegeben durch:

$$R \cap (A' \times A').$$

Beispiele

- Die Einschränkung von $=$ auf $[5]$ ist

$$\{(1,1),(2,2),(3,3),(4,4),(5,5)\}.$$

- Die Einschränkung von $\neq$ auf $[3]$ ist

$$\{(1,2),(1,3),(2,1),(2,3),(3,1),(3,2)\}.$$

- Die Einschränkung von $\leq$ auf $[3]$ ist

$$\{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}.$$

Quizfragen

1. Was ist die Einschränkung der Kleiner-Relation $<$ auf $[4]$?
2. Was ist die Einschränkung der Echte-Teilmenge-Relation $\subset$ auf $\mathcal{P}([2])$?
3. Was ist die Einschränkung der Element-Relation $\in$ auf $[2]$ und $\mathcal{P}([2])$?

1. Die Einschränkung von $<$ auf $[4]$ ist

$$\{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}.$$

2. Die Einschränkung von $\subset$ auf $\mathcal{P}([2])$ ist

$$\{(\emptyset,\{1\}),(\emptyset,\{2\}),(\emptyset,\{1,2\}),(\{1\},\{1,2\}),(\{2\},\{1,2\})\}.$$

3. Die Einschränkung von $\in$ auf $[2]$ und $\mathcal{P}([2])$ ist:

$$\{(1,\{1\}),(1,\{1,2\}),(2,\{2\}),(2,\{1,2\})\}.$$

Graphische Darstellung endlicher Relationen

Jede endliche Relation R über A und B kann als Graph dargestellt werden. Die Elemente aus A werden links und die aus B rechts als Punkte (Knoten) gezeichnet. Die Tupel aus R werden als Pfeile (Kanten) dargestellt: „$a \longrightarrow b$“ bedeutet „$(a, b) \in R$“.

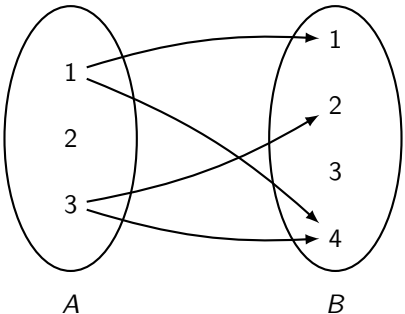
Ist R homogen, dann kann man auch jedes Element nur einmal als Knoten zeichnen.

Beispiel

Die Relation R über [3] und [4] mit

$$R = \{(1,1),(1,4),(3,2),(3,4)\}$$

kann graphisch wie folgt dargestellt werden:



Beispiel

Die homogene Relation R über [3] mit

$$R = \{(1,1),(1,2),(2,3),(3,2),(3,3)\}$$

kann graphisch wie folgt dargestellt werden:

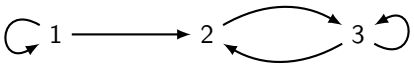


Bild und Urbild einer Relation

Seien A und B Mengen und R eine Relation über A und B. Das Bild und das Urbild von R sind definiert als:

$$\begin{aligned} \text{Bild}(R) &:= \{b \in B \mid \exists a \in A : (a, b) \in R\} \\ \text{Urbild}(R) &:= \{a \in A \mid \exists b \in B : (a, b) \in R\} \end{aligned}$$

Info

Intuitiv enthält

- das Urbild von R alle Elemente $a \in A$, die in mindestens einem Tupel (a, b) als erste Komponente vorkommen (bzw. von mindestens einer Kante verlassen werden) und
- das Bild von R alle Elemente $b \in B$, die in mindestens einem Tupel (a, b) als zweite Komponente vorkommen (bzw. von mindestens einer Kante getroffen werden).

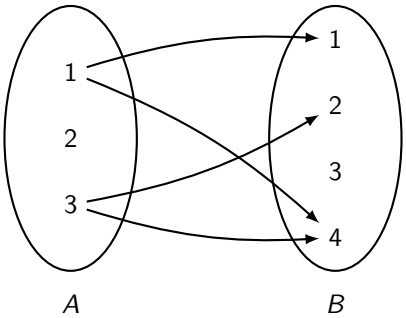
Wichtig!

Man benutzt das Zeichen $:=$ um zu verdeutlichen, dass der Ausdruck auf der rechten Seite der Gleichung per Definition gleich dem auf der linken Seite ist.

Gleichungen, die einen Doppelpunkt vor dem Gleichheitszeichen haben, sind insbesondere nicht beweisbar. Sie können nur angenommen werden.

Beispiel

Sei R wieder folgende Relation:



Das Bild und Urbild von R sind:

$$\text{Bild}(R) = \{1, 2, 4\} \quad \text{und} \quad \text{Urbild}(R) = \{1, 3\}\,.$$

Umkehr- und Komplementärrelation

Seien A und B zwei Mengen und R eine Relation über A und B. Wir definieren:

$$\begin{array}{lcll} R^{-1} & := & \{(a,b) \mid (b,a) \in R\} & (\text{Umkehrrelation}), \\ \overline{R} & := & \{(a,b) \mid (a,b) \notin R\} & (\text{Komplementärrelation}). \end{array}$$

Infos

- Es gilt $\overline{R} \subseteq A \times B$, aber $R^{-1} \subseteq B \times A$.
- Insbesondere gelten die Gleichungen $|R^{-1}| = |R|$ und $|\overline{R}| = |A| \cdot |B| - |R|$.
- Haben wir für R ein tolles Relationensymbol (z.B. „$\leq$“), dann kann man R^{-1} bzw. $\overline{R}$ darstellen, indem man das Symbol für R umdreht (z.B. „$\geq$“) bzw. durchstreicht (z.B. „$\not\leq$“).

Beispiel

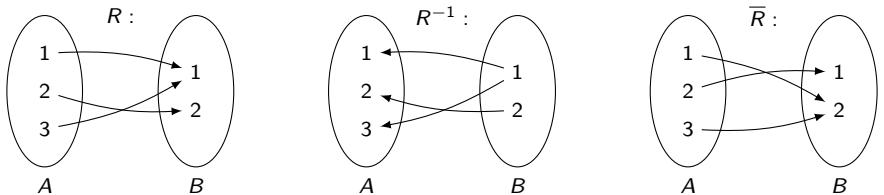
Sei R eine Relation über [3] und [2] mit

$$R = \{(1,1),(2,2),(3,1)\}\,.$$

Dann gilt für R^{-1} und $\overline{R}$:

$$R^{-1} = \{(1,1),(1,3),(2,2)\} \quad \text{und} \quad \overline{R} = \{(1,2),(2,1),(3,2)\}\,.$$

Graphisch:



Eigenschaften von Relationen

Seien A und B Mengen und R eine Relation über A und B. Dann heißt R:

- linkstotal, falls für alle $a \in A$ gilt:

$$|\{b \in B \,|\, (a,b) \in R\}| \geq 1,$$

- rechtseindeutig, falls für alle $a \in A$ gilt:

$$|\{b \in B \,|\, (a,b) \in R\}| \leq 1.$$

In kompakter Schreibweise heißt das:

$$\begin{array}{lll} R \text{ linkstotal} & :\Longleftrightarrow & \forall a \in A : |\{b \in B \,|\, (a,b) \in R\}| \geq 1 \\ R \text{ rechtseindeutig} & :\Longleftrightarrow & \forall a \in A : |\{b \in B \,|\, (a,b) \in R\}| \leq 1 \end{array}$$

Info

Intuitiv ist eine Relation R über A und B

- linkstotal, falls jedes Element aus A in mindestens einem Tupel vorkommt (bzw. von mindestens einer Kante verlassen wird) und
- rechtseindeutig, falls jedes Element aus A in höchstens einem Tupel vorkommt (bzw. von höchstens einer Kante verlassen wird).

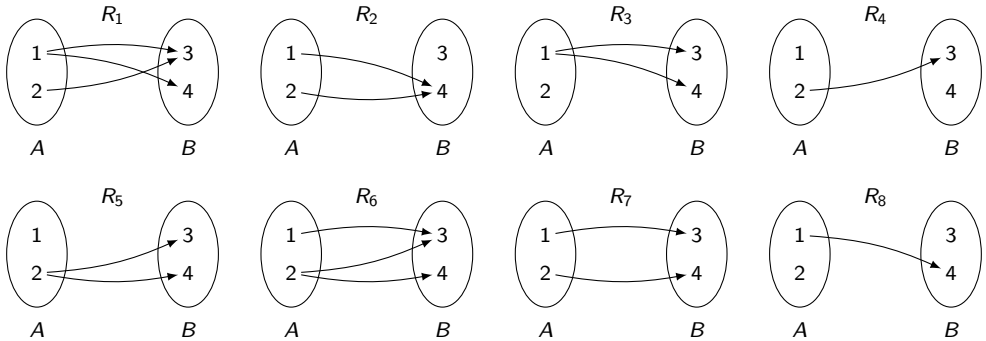
Wichtig!

Man benutzt das Zeichen $:\Longleftrightarrow$ um zu verdeutlichen, dass die Aussage auf der rechten Seite des Äquivalenzzeichens per Definition äquivalent zu der auf der linken Seite ist.

Äquivalenzen, die einen Doppelpunkt vor dem Äquivalenzzeichen haben, sind insbesondere nicht beweisbar. Sie können, analog zu den Gleichungen mit dem Zeichen $:=$, nur angenommen werden.

Beispiele

Seien $R_1, \ldots, R_8$ folgende Relationen über $A = \{1, 2\}$ und $B = \{3, 4\}$:



R_1, R_2, R_6 und R_7 sind linkstotal. R_2, R_4, R_7 und R_8 sind rechtseindeutig.

Relationenprodukt

Seien A, B und C drei Mengen, R eine Relation über A und B und S eine Relation über B und C. Dann gilt:

$$R \circ S := \{(a, c) \in A \times C\} \exists b \in B : (a, b) \in R \text{ und } (b, c) \in S$$

$R \circ S$ ist dann eine Relation über A und C.

Damit $R \circ S$ definiert ist muss $R \subseteq A \times B$ und $S \subseteq B \times C$ gelten!

Beispiel

Gegeben seien Mengen $A = \{1, 2\}$, $B = \{3, 4\}$ und $C = \{5, 6\}$ und Relationen

$$\begin{array}{rcll} R & = & \{(1,3),(1,4),(2,3)\} & \text{über } A \text{ und } B \text{ und} \\ S & = & \{(3,5),(4,5),(4,6)\} & \text{über } B \text{ und } C. \end{array}$$

Dann folgt für $R \circ S$:

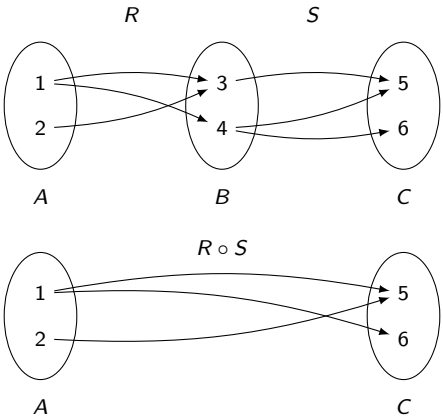
	$(3,5)$	$(4,5)$	$(4,6)$
$(1,3)$	$(1,5)$		
$(1,4)$		$(1,5)$	$(1,6)$
$(2,3)$	$(2,5)$		

Nach der Entfernung von Duplikaten erhalten wir:

$$R \circ S = \{(1,5),(1,6),(2,5)\}.$$

Beispiel

Graphisch:



Infos

- Folgende Intuition kann hilfreich sein: Kommt man im Graph von R in einem Schritt von a nach b und im Graph von S in einem Schritt von b nach c, dann kommt man im Graph von $R \circ S$ in einem Schritt von a nach c.
- Statt $R \circ S$ schreibt man oft nur RS, was aber gefährlich ist, weil man es mit der Konkatenation aus Folie 84 verwechseln kann.
- Das Relationenprodukt ist assoziativ. Für beliebige Relationen R, S, T gilt nämlich:

$$(R \circ S) \circ T = R \circ (S \circ T).$$

Aus diesem Grund lassen wir oft einfach die Klammern weg.

Quizfrage

Gegeben seien Mengen $A = \{1, 2, 3\}$ und $B = \{4, 5, 6\}$ und Relationen

$$\begin{array}{lcll} R & = & \{(1,4),(1,5),(2,4),(3,6)\} & \text{über } A \text{ und } B \text{ und} \\ S & = & \{(4,2),(5,2),(5,3),(6,1)\} & \text{über } B \text{ und } A. \end{array}$$

1. Wie sieht $R \circ S$ aus?
2. Wie sieht $S \circ R$ aus?

1. $R \circ S = \{(1,2),(1,3),(2,2),(3,1)\}$.

	$(4,2)$	$(5,2)$	$(5,3)$	$(6,1)$
$(1,4)$	$(1,2)$			
$(1,5)$		$(1,2)$	$(1,3)$	
$(2,4)$	$(2,2)$			
$(3,6)$				$(3,1)$

2. $S \circ R = \{(4,4),(5,4),(5,6),(6,4),(6,5)\}$.

	$(1,4)$	$(1,5)$	$(2,4)$	$(3,6)$
$(4,2)$			$(4,4)$	
$(5,2)$			$(5,4)$	
$(5,3)$				$(5,6)$
$(6,1)$	$(6,4)$	$(6,5)$		

Themenübersicht

Eigenschaften homogener Relationen

Seien A eine Menge und R eine homogene Relation über A. Dann heißt R:

- reflexiv, falls für alle $a \in A$ gilt:
$$(a, a) \in R,$$
- symmetrisch, falls für alle $a, b \in A$ gilt:
$$\text{wenn } (a, b) \in R, \text{ dann } (b, a) \in R,$$
- asymmetrisch, falls für alle $a, b \in A$ gilt:
$$\text{wenn } (a, b) \in R, \text{ dann } (b, a) \notin R,$$

Eigenschaften homogener Relationen

- antisymmetrisch, falls für alle $a, b \in A$ gilt:

$$\text{wenn } (a, b) \in R \text{ und } (b, a) \in R, \text{ dann } a = b,$$

- total, falls für alle $a, b \in A$ gilt:

$$\text{wenn } (a, b) \notin R, \text{ dann } (b, a) \in R,$$

- transitiv, falls für alle $a, b, c \in A$ gilt:

$$\text{wenn } (a, b) \in R \text{ und } (b, c) \in R, \text{ dann } (a, c) \in R.$$

Eigenschaften homogener Relationen

In kompakter Schreibweise heißt das:

$$
\begin{array}{lll}
R \text{ reflexiv} & :\iff & \forall a \in M : (a,a) \in R \\
R \text{ symmetrisch} & :\iff & \forall a,b \in M : (a,b) \in R \implies (b,a) \in R \\
R \text{ asymmetrisch} & :\iff & \forall a,b \in M : (a,b) \in R \implies (b,a) \notin R \\
R \text{ antisymmetrisch} & :\iff & \forall a,b \in M : ((a,b) \in R \text{ und } (b,a) \in R) \implies a = b \\
R \text{ total} & :\iff & \forall a,b \in M : (a,b) \notin R \implies (b,a) \in R \\
R \text{ transitiv} & :\iff & \forall a,b,c \in M : ((a,b) \in R \text{ und } (b,c) \in R) \implies (a,c) \in R
\end{array}
$$

Infos

- Um zu zeigen, dass eine Eigenschaft nicht gilt, reicht es, eine Kombination von konkreten Elementen zu finden, die die Bedingung nicht erfüllt. Es gilt nämlich:

R nicht reflexiv	$\iff$	$\exists a \in M : (a, a) \notin R$
R nicht symmetrisch	$\iff$	$\exists a, b \in M : (a, b) \in R$ und $(b, a) \notin R$
R nicht asymmetrisch	$\iff$	$\exists a, b \in M : (a, b) \in R$ und $(b, a) \in R$
R nicht antisymmetrisch	$\iff$	$\exists a, b \in M : (a, b) \in R$, $(b, a) \in R$ und $a \neq b$
R nicht total	$\iff$	$\exists a, b \in M : (a, b) \notin R$ und $(b, a) \notin R$
R nicht transitiv	$\iff$	$\exists a, b, c \in M : (a, b) \in R$, $(b, c) \in R$ und $(a, c) \notin R$

- Um zu zeigen, dass eine Eigenschaft gilt, muss man leider für alle Kombinationen ausprobieren, dass die Bedingung erfüllt ist.

Reflexivität

Die Reflexivität besagt, dass jedes Element $a \in A$ mit sich selbst in Relation stehen muss. Die Aussage

$$(a, a) \in R$$

ist nur dann nicht erfüllt, wenn $(a, a) \notin R$ gilt, d.h. wenn mindestens ein Element nicht mit sich selbst in Relation steht.

Symmetrie

Die Symmetrie besagt, dass zwei verschiedene Elemente entweder in beiden Richtungen oder gar nicht in Relation stehen dürfen.

- Falls $a = b$, ist die Implikation

$$(a, a) \in R \implies (a, a) \in R$$

  immer erfüllt, egal ob $(a, a) \in R$ oder $(a, a) \notin R$ gilt.

- Falls $a \neq b$, ist die Implikation

$$(a, b) \in R \implies (b, a) \in R$$

  nur dann nicht erfüllt, falls $(a, b) \in R$ und $(b, a) \notin R$ oder $(a, b) \notin R$ und $(b, a) \in R$ gilt, d.h. falls von den Tupeln (a, b) und (b, a) genau eins in R enthalten ist.

Asymmetrie

Die Asymmetrie besagt, dass zwei verschiedene Elemente entweder in nur eine Richtung oder gar nicht in Relation stehen dürfen. Außerdem darf kein Element mit sich selbst in Relation stehen.

- Falls $a = b$, ist die Implikation

$$(a, a) \in R \implies (a, a) \notin R$$

nur dann nicht erfüllt, falls $(a, a) \in R$ gilt. Deshalb darf kein Element mit sich selbst in Relation stehen.

- Falls $a \neq b$, ist die Implikation

$$(a, b) \in R \implies (b, a) \notin R$$

nur dann nicht erfüllt, falls $(a, b) \in R$ und $(b, a) \in R$ gilt, d.h. falls beide Tupeln (a, b) und (b, a) in R enthalten sind.

Antisymmetrie

Die Antisymmetrie besagt, dass zwei verschiedene Elemente entweder in nur eine Richtung oder gar nicht in Relation stehen dürfen. Im Gegensatz zur Asymmetrie dürfen Elemente schon mit sich selbst in Relation stehen. (Müssen sie aber nicht!)

- Falls $a = b$, ist die Implikation

$$((a, a) \in R \text{ und } (a, a) \in R) \implies a = a$$

  immer erfüllt, da $a = a$ eine wahre Aussage ist. Deshalb dürfen Elemente mit sich selbst in Relation stehen oder auch nicht.

- Falls $a \neq b$, ist die Implikation

$$(a, b) \in R \implies (b, a) \notin R$$

  nur dann nicht erfüllt, falls $(a, b) \in R$ und $(b, a) \in R$ gilt, d.h. falls beide Tupeln (a, b) und (b, a) in R enthalten sind.

Totalität

Die Totalität besagt, dass zwei verschiedene Elemente in mindestens eine Richtung in Relation stehen sollen. Außerdem muss jedes Element mit sich selbst in Relation stehen.

- Falls $a = b$, ist die Implikation

$$(a, a) \notin R \implies (a, a) \in R$$

  nur dann erfüllt, falls $(a, a) \in R$ gilt. Deshalb muss jedes Element mit sich selbst in Relation stehen.

- Falls $a \neq b$, ist die Implikation

$$(a, b) \notin R \implies (b, a) \in R$$

  nur dann nicht erfüllt, falls $(a, b) \notin R$ und $(b, a) \notin R$ gilt, d.h. falls beide Tupeln (a, b) und (b, a) nicht in R enthalten sind.

Transitivität

Die Transitivität besagt, dass es für jeden indirekten Weg zwischen zwei Knoten im Graph der Relation immer auch einen direkten Weg gibt.

- Falls a, b und c alle gleich sind, ist die Implikation

$$((a, a) \in R \text{ und } (a, a) \in R) \implies (a, a) \in R$$

  immer erfüllt, egal ob $(a, a) \in R$ oder $(a, a) \notin R$ gilt.

- Falls nur a und b gleich sind, ist die Implikation

$$((a, a) \in R \text{ und } (a, c) \in R) \implies (a, c) \in R$$

  auch immer erfüllt, egal ob $(a, c) \in R$ oder $(a, c) \notin R$ gilt.

- Falls nur b und c gleich sind, ist die Implikation

$$((a, b) \in R \text{ und } (b, b) \in R) \implies (a, b) \in R$$

  auch immer erfüllt, egal ob $(a, b) \in R$ oder $(a, b) \notin R$ gilt.

Transitivität

- Falls nur a und c gleich sind, ist die Implikation

$$((a, b) \in R \text{ und } (b, a) \in R) \implies (a, a) \in R$$

nur dann nicht erfüllt, wenn $(a, b) \in R$, $(b, a) \in R$ und $(a, a) \notin R$ gilt, d.h. wenn zwei Element in beiden Richtungen verbunden sind, aber eins davon nicht mit sich selbst.

- Falls a, b und c alle unterschiedlich sind, ist die Implikation

$$((a, b) \in R \text{ und } (b, c) \in R) \implies (a, c) \in R$$

nur dann nicht erfüllt, falls $(a, b) \in R$, $(b, c) \in R$ und $(a, c) \notin R$, d.h. falls a mit b verbunden ist, b mit c, aber nicht a mit c.

Graphische Bedeutung der Reflexivität, Symmetrie, Asymmetrie, Antisymmetrie und Totalität

Um die Eigenschaften einer homogenen Relation R über A erkennen zu können ist es hilfreich zu wissen, was jede Eigenschaft für Elemente $a, b \in M$ erlaubt (✓) bzw. verbietet (✗). Aus den Überlegungen der letzten Folien entsteht folgende Tabelle:

Infos

- An der linken Hälfte der Tabelle erkennt man, ob Elemente eine Kante zu sich selbst (eine *Schleife*) haben dürfen und an der rechten Seite, ob es erlaubt ist, dass zwischen je zwei verschiedenen Elementen keine, eine oder zwei Kanten verlaufen.
- Ob ein Element zu sich selbst in Relation steht oder nicht, ist in der rechten Hälfte der Tabelle egal. Daher die grauen, gestrichenen Schleifen.
- Ein Häkchen (✓) heißt nur, dass der jeweilige Fall eintreten kann, aber nicht, dass er notwendigerweise eintreten muss!

Graphische Bedeutung der Transitivität

Die Transitivität ist leider ein bisschen komplizierter. Eine Relation ist genau dann transitiv, wenn man keine der folgenden zwei Situationen vorfindet:

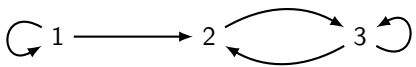
1. Es gibt bei zwei verschiedenen Elementen eine Doppelkante, aber es fehlt mindestens eine der beiden Schleifen (1. Punkt auf Folie 258):

2. Es gibt bei drei verschiedenen Elementen einen indirekten Weg von einem Element zu einem anderen, aber keinen direkten (2. Punkt auf Folie 258):

Findet man keine der beiden Situationen, so kann man mit Sicherheit sagen, dass die Relation transitiv ist!

Beispiel

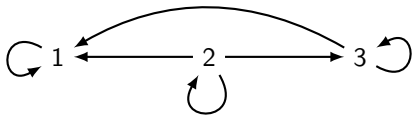
Sei R wieder folgende homogene Relation über $[3]$:



- R ist nicht reflexiv.
- R ist nicht symmetrisch.
- R ist nicht asymmetrisch.
- R ist nicht antisymmetrisch.
- R ist nicht total.
- R ist nicht transitiv.

Noch ein Beispiel

Sei R folgende homogene Relation über [3]:



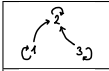
- R ist reflexiv.
- R ist nicht symmetrisch.
- R ist nicht asymmetrisch.
- R ist antisymmetrisch.
- R ist total.
- R ist transitiv.

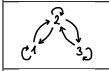
Ein letztes Beispiel

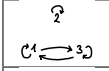
Es gibt $2^{2 \cdot 2} = 16$ verschiedene homogene Relationen über $[2]$:

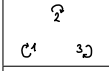
	ref	sym	asy	ant	tot	tra
	✗	✓	✓	✓	✗	✓
	✗	✓	✗	✓	✗	✓
	✗	✗	✓	✓	✗	✓
	✗	✗	✓	✓	✗	✓
	✗	✓	✗	✓	✗	✓
	✗	✗	✗	✓	✗	✓
	✗	✗	✗	✓	✗	✓
	✓	✓	✗	✓	✗	✓

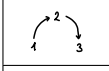
	ref	sym	asy	ant	tot	tra
	✗	✓	✗	✗	✗	✗
	✗	✗	✗	✓	✗	✓
	✗	✗	✗	✓	✗	✓
	✗	✓	✗	✗	✗	✗
	✓	✗	✗	✓	✓	✓
	✓	✗	✗	✓	✓	✓
	✗	✓	✗	✗	✗	✗
	✓	✓	✗	✗	✓	✓

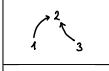


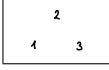


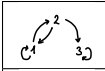


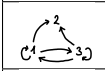


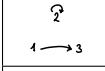


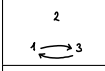


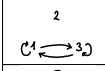


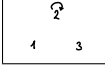












Quizfrage

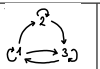
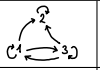
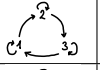
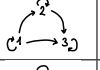
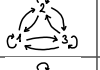
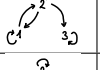
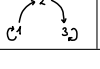
Welche Eigenschaften besitzen folgende homogene Relationen über [3]?

	ref	sym	asy	ant	tot	tra

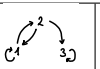
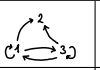
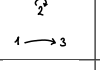
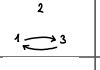
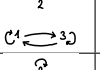
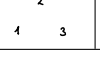
	ref	sym	asy	ant	tot	tra

	ref	sym	asy	ant	tot	tra

Antwort

	ref	sym	asy	ant	tot	tra
	✓	✗	✗	✗	✓	✗
	✓	✗	✗	✗	✓	✓
	✓	✗	✗	✓	✓	✗
	✓	✗	✗	✓	✓	✓
	✓	✓	✗	✗	✓	✓
	✓	✗	✗	✗	✗	✗
	✓	✗	✗	✓	✗	✗

	ref	sym	asy	ant	tot	tra
	✓	✗	✗	✓	✗	✓
	✓	✓	✗	✗	✗	✗
	✓	✓	✗	✗	✗	✓
	✓	✓	✗	✓	✗	✓
	✗	✗	✓	✓	✗	✗
	✗	✗	✓	✓	✗	✓
	✗	✓	✓	✓	✗	✓

	ref	sym	asy	ant	tot	tra
	✗	✗	✗	✗	✗	✗
	✗	✗	✗	✗	✗	✓
	✗	✗	✗	✓	✗	✗
	✗	✗	✗	✓	✗	✓
	✗	✓	✗	✗	✗	✗
	✗	✓	✗	✗	✗	✓
	✗	✓	✗	✓	✗	✓

Mehr Quizfragen

1. Welche Eigenschaften besitzen folgende homogene Relationen über den ganzen Zahlen?

	ref	sym	asy	ant	tot	tra
$=$						
$\neq$						
$\leq$						
$<$						

2. Welche Eigenschaften besitzen folgende homogene Relationen über der Potenzmenge einer beliebigen Menge?

	ref	sym	asy	ant	tot	tra
$=$						
$\neq$						
$\subseteq$						
$\not\subseteq$						
$\subset$						
$\not\subset$						

1. Für $=$, $\neq$, $\leq$ und $<$ über den ganzen Zahlen gilt:

	ref	sym	asy	ant	tot	tra
$=$	✓	✓	✗	✓	✗	✓
$\neq$	✗	✓	✗	✗	✗	✗
$\leq$	✓	✗	✗	✓	✓	✓
$<$	✗	✗	✓	✓	✗	✓

2. Für $=$, $\neq$, $\subseteq$, $\not\subseteq$, $\subset$ und $\not\subset$ über der Potenzmenge einer beliebigen Menge gilt:

	ref	sym	asy	ant	tot	tra
$=$	✓	✓	✗	✓	✗	✓
$\neq$	✗	✓	✗	✗	✗	✗
$\subseteq$	✓	✗	✗	✓	✗	✓
$\not\subseteq$	✗	✗	✗	✗	✗	✗
$\subset$	✗	✗	✓	✓	✗	✓
$\not\subset$	✓	✗	✗	✗	✓	✗

Wichtige homogene Relationen

Für eine beliebige Menge A sind folgende homogene Relationen über A wichtig:

$$
\begin{array}{lcll}
\emptyset & := & \{\} & \text{(leere Relation)} \\
\mathrm{id}_A & := & \{(a,a) \mid a \in A\} & \text{(Identitätsrelation)} \\
A \times A & := & \{(a,b) \mid a,b \in A\} & \text{(kartesisches Produkt)}
\end{array}
$$

Infos

- In $\emptyset$ steht jedes Element mit keinem Element in Relation.
- In id_A steht jedes Element nur mit sich selbst in Relation. Beispielsweise ist die Gleichheitsrelation $=$ über ganze Zahlen nichts anderes als $\mathrm{id}_{\mathbb{Z}}$.
- In $A \times A$ steht jedes Element mit jedem anderen in Relation.

Welche Eigenschaften besitzen folgende homogene Relationen über einer beliebigen, nichtleeren Menge A?

	ref	sym	asy	ant	tot	tra
$\emptyset$						
id_A						
$A \times A$						

Es gilt:

	ref	sym	asy	ant	tot	tra
$\emptyset$	✗	✓	✓	✓	✗	✓
id_A	✓	✓	✗	✓	✗	✓
$A \times A$	✓	✓	✗	✗	✓	✓

Quizfragen

1. Kann eine reflexive Relation auch asymmetrisch sein?
2. Ist jede antisymmetrische Relation, die nicht reflexiv ist, automatisch asymmetrisch?
3. Ist jede asymmetrische Relation automatisch antisymmetrisch?
4. Kann eine symmetrische Relation auch asymmetrisch sein?
5. Ist jede totale Relation automatisch reflexiv?

1. Ja! Die leere Relation $\emptyset$ über der leeren Menge $\emptyset$. Diese besitzt alle 6 Eigenschaften ;-)
2. Nein! Damit eine antisymmetrische Relation auch asymmetrisch ist, darf kein Element zu sich selbst in Relation stehen. Stehen jedoch einige mit sich selbst in Relation und einige nicht, dann ist die Relation weder reflexiv noch asymmetrisch. Gegenbeispiel: $R = \{(1,1),(1,2)\}$ über $[2]$.
3. Ja! Man erkennt an der Tabelle auf Folie 259, dass die Antisymmetrie eine Abschwächung der Asymmetrie ist.
4. Ja! Die leere Relation $\emptyset$.
5. Ja! Man erkennt an der Tabelle auf Folie 259, dass die Reflexivität eine Abschwächung der Totalität ist.

Infos

- Die leere Relation $\emptyset$ über einer beliebigen Menge A ist symmetrisch, asymmetrisch, antisymmetrisch und transitiv. Gilt außerdem $A = \emptyset$, so ist sie auch reflexiv und total!
- Für jede Relation R über einer beliebigen Menge A gilt:

$$\begin{array}{lcl} R \text{ total} & \Longrightarrow & R \text{ reflexiv} \\ R \text{ asymmetrisch} & \Longrightarrow & R \text{ antisymmetrisch} \end{array}$$

  Das sind auch die einzigen Implikationen, die immer gelten.
- Eine Relation über einer nichtleeren Menge kann nicht gleichzeitig reflexiv und asymmetrisch sein.
- Eine nichtleere Relation über einer nichtleeren Menge kann nicht gleichzeitig symmetrisch und asymmetrisch sein.

Eigenschaften homogener Relationen beweisen

Die Definitionen aller Eigenschaften homogener Relationen sind Aussagen der Art

$$\forall \ldots : B \implies F$$

für eine Bedingung B und eine Folgerung F. Die Negation einer solchen Aussage hat folgende Form:

$$\exists \ldots : B \text{ und nicht } F.$$

Daher werden diese Aussagen

- mit einem Beweis für beliebige Elemente gezeigt, aber
- mit einem konkreten Gegenbeispiel widerlegt.

Wie man diese 6 Eigenschaften beweist oder widerlegt wird anhand der nächsten 6 Relationen gezeigt.

Bei der Reflexivität gibt es keine Bedingung. Die Aussage ist lediglich

$$\forall a \in A : (a, a) \in R$$

und ihre Negation

$$\exists a \in A : (a, a) \notin R.$$

Präfixrelation $\sqsubseteq_p$

Sei Σ ein Alphabet und Σ^* die Menge aller Wörter über Σ. Für beliebige Wörter $u, v \in \Sigma^*$ gilt $u \sqsubseteq_p v$ genau dann, wenn es ein Wort $w \in \Sigma^*$ gibt mit $v = uw$. In kompakter Schreibweise heißt das:

$$u \sqsubseteq_p v \quad :\Longleftrightarrow \quad \exists w \in \Sigma^* : v = uw \ .$$

Somit ist $\sqsubseteq_p$ ebenfalls eine homogene Relation über Σ^*.

Beispiele

Für $\Sigma = \{a, b, c\}$ gilt beispielsweise $ab \sqsubseteq_p abaca$, $\epsilon \sqsubseteq_p abc$ und $bc \sqsubseteq_p bc$, aber $ca \not\sqsubseteq_p abcaa$, $abba \not\sqsubseteq_p ab$ und $abc \not\sqsubseteq_p bca$.

Infos

- Für $u \sqsubseteq_p v$ sagen wir „u ist Präfix von v“.
- Intuitiv heißt $u \sqsubseteq_p v$, dass das Wort u am Anfang von v vorkommt.

Eigenschaften der Präfixrelation

Für die Präfixrelation $\sqsubseteq_p$ gilt:

1. $\sqsubseteq_p$ ist reflexiv.
2. $\sqsubseteq_p$ ist nicht symmetrisch.
3. $\sqsubseteq_p$ ist nicht asymmetrisch.
4. $\sqsubseteq_p$ ist antisymmetrisch.
5. $\sqsubseteq_p$ ist nicht total.
6. $\sqsubseteq_p$ ist transitiv.

Diese Aussagen werden in den nächsten 6 Folien gezeigt.

Eigenschaften der Präfixrelation

1. $\sqsubseteq_p$ ist reflexiv.

   Zu zeigen ist:

   $$\forall a \in \Sigma^* : a \sqsubseteq_p a.$$

   Beweis:

   Sei $a \in \Sigma^*$ ein beliebiges Wort.

   $\Longrightarrow$ $a = a\epsilon$.

   $\Longrightarrow$ Es gibt also ein Wort $w \in \Sigma^*$ mit $a = aw$, nämlich $w = \epsilon$.

   $\Longrightarrow$ $a \sqsubseteq_p a$.

   $\square$.

Eigenschaften der Präfixrelation

2. $\sqsubseteq_p$ ist nicht symmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \sqsubseteq_p b \text{ und } b \not\sqsubseteq_p a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \sqsubseteq_p b$ und $b \not\sqsubseteq_p a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = x$ und $b = xy$. □

Eigenschaften der Präfixrelation

3. $\sqsubseteq_p$ ist nicht asymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \sqsubseteq_p b \text{ und } b \sqsubseteq_p a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \sqsubseteq_p b$ und $b \sqsubseteq_p a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xy$ und $b = xy$. □

Eigenschaften der Präfixrelation

4. $\sqsubseteq_p$ ist antisymmetrisch.

   Zu zeigen ist:

$$\forall a, b \in \Sigma^* : (a \sqsubseteq_p b \text{ und } b \sqsubseteq_p a) \implies a = b.$$

   Beweis:

   Seien $a, b \in \Sigma^*$ beliebige Wörter mit $a \sqsubseteq_p b$ und $b \sqsubseteq_p a$.

   $\implies$ Es gibt Wörter $w_1, w_2 \in \Sigma^*$ mit $b = aw_1$ und $a = bw_2$.

   $\implies$ Durch Einsetzen von $b = aw_1$ in $a = bw_2$ erhalten wir:

$$a = aw_1w_2.$$

   $\implies$ w_1 und w_2 müssen beide leer sein.

   $\implies$ $b = a\epsilon$ und $a = b\epsilon$.

   $\implies$ $a = b$.

□

Eigenschaften der Präfixrelation

5. $\sqsubseteq_p$ ist nicht total.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \not\sqsubseteq_p b \text{ und } b \not\sqsubseteq_p a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \not\sqsubseteq_p b$ und $b \not\sqsubseteq_p a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xy$ und $b = yx$. □

Eigenschaften der Präfixrelation

6. $\sqsubseteq_p$ ist transitiv.

   Zu zeigen ist:

$$\forall a, b, c \in \Sigma^* : (a \sqsubseteq_p b \text{ und } b \sqsubseteq_p c) \implies a \sqsubseteq_p c.$$

   Beweis:

   Seien $a, b, c \in \Sigma^*$ beliebige Wörter mit $a \sqsubseteq_p b$ und $b \sqsubseteq_p c$.

   $\implies$ Es gibt Wörter $w_1, w_2 \in \Sigma^*$ mit $b = aw_1$ und $c = bw_2$.

   $\implies$ Durch Einsetzen von $b = aw_1$ in $c = bw_2$ erhalten wir:

$$c = aw_1w_2.$$

   $\implies$ Also gibt es ein Wort $w_3 \in \Sigma^*$ mit $c = aw_3$ (nämlich $w_3 = w_1w_2$).

   $\implies$ $a \sqsubseteq_p c$

□

Suffixrelation $\sqsubseteq_s$

Sei Σ ein Alphabet und Σ^* die Menge aller Wörter über Σ. Für beliebige Wörter $u, v \in \Sigma^*$ gilt $u \sqsubseteq_s v$ genau dann, wenn es ein Wort $w \in \Sigma^*$ gibt mit $v = wu$. In kompakter Schreibweise heißt das:

$$u \sqsubseteq_s v \quad :\Longleftrightarrow \quad \exists w \in \Sigma^* : v = wu \ .$$

Somit ist auch $\sqsubseteq_s$ eine homogene Relation über Σ^*.

Beispiele

Für $\Sigma = \{a, b, c\}$ gilt beispielsweise $ab \sqsubseteq_s acab$, $\epsilon \sqsubseteq_s acb$ und $bab \sqsubseteq_s bab$, aber $ca \not\sqsubseteq_s cabaa$, $abcc \not\sqsubseteq_s cc$ und $bca \not\sqsubseteq_s bac$.

Infos

- Für $u \sqsubseteq_s v$ sagen wir „u ist Suffix von v“.
- Intuitiv heißt $u \sqsubseteq_s v$, dass das Wort u am Ende von v vorkommt.

Eigenschaften der Suffixrelation

Für die Suffixrelation $\sqsubseteq_s$ gilt:

1. $\sqsubseteq_s$ ist reflexiv.
2. $\sqsubseteq_s$ ist nicht symmetrisch.
3. $\sqsubseteq_s$ ist nicht asymmetrisch.
4. $\sqsubseteq_s$ ist antisymmetrisch.
5. $\sqsubseteq_s$ ist nicht total.
6. $\sqsubseteq_s$ ist transitiv.

Diese Aussagen werden in den nächsten 6 Folien gezeigt.

Eigenschaften der Suffixrelation

1. $\sqsubseteq_s$ ist reflexiv.

   Zu zeigen ist:

   $$\forall a \in \Sigma^* : a \sqsubseteq_s a.$$

   Beweis:

   Sei $a \in \Sigma^*$ ein beliebiges Wort.

   $\Longrightarrow$ $a = \epsilon a$.

   $\Longrightarrow$ Es gibt also ein Wort $w \in \Sigma^*$ mit $a = wa$, nämlich $w = \epsilon$.

   $\Longrightarrow$ $a \sqsubseteq_s a$.

   $\square$.

Eigenschaften der Suffixrelation

2. $\sqsubseteq_s$ ist nicht symmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \sqsubseteq_s b \text{ und } b \not\sqsubseteq_s a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \sqsubseteq_s b$ und $b \not\sqsubseteq_s a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = y$ und $b = xy$. □

Eigenschaften der Suffixrelation

3. $\sqsubseteq_s$ ist nicht asymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \sqsubseteq_s b \text{ und } b \sqsubseteq_s a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \sqsubseteq_s b$ und $b \sqsubseteq_s a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xy$ und $b = xy$. □

Eigenschaften der Suffixrelation

4. $\sqsubseteq_s$ ist antisymmetrisch.

   Zu zeigen ist:

$$\forall a, b \in \Sigma^* : (a \sqsubseteq_s b \text{ und } b \sqsubseteq_s a) \implies a = b.$$

   Beweis:

   Seien $a, b \in \Sigma^*$ beliebige Wörter mit $a \sqsubseteq_s b$ und $b \sqsubseteq_s a$.

   $\implies$ Es gibt Wörter $w_1, w_2 \in \Sigma^*$ mit $b = w_1 a$ und $a = w_2 b$.

   $\implies$ Durch Einsetzen von $b = w_1 a$ in $a = w_2 b$ erhalten wir:

$$a = w_2 w_1 a.$$

   $\implies$ w_1 und w_2 müssen beide leer sein.

   $\implies$ $b = \epsilon a$ und $a = \epsilon b$.

   $\implies$ $a = b$.

□

Eigenschaften der Suffixrelation

5. $\sqsubseteq_s$ ist nicht total.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \not\sqsubseteq_s b \text{ und } b \not\sqsubseteq_s a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \not\sqsubseteq_s b$ und $b \not\sqsubseteq_s a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xy$ und $b = yx$. □

Eigenschaften der Suffixrelation

6. $\sqsubseteq_s$ ist transitiv.

   Zu zeigen ist:

$$\forall a, b, c \in \Sigma^* : (a \sqsubseteq_s b \text{ und } b \sqsubseteq_s c) \implies a \sqsubseteq_s c.$$

   Beweis:

   Seien $a, b, c \in \Sigma^*$ beliebige Wörter mit $a \sqsubseteq_s b$ und $b \sqsubseteq_s c$.

   $\implies$ Es gibt Wörter $w_1, w_2 \in \Sigma^*$ mit $b = w_1 a$ und $c = w_2 b$.

   $\implies$ Durch Einsetzen von $b = w_1 a$ in $c = w_2 b$ erhalten wir:

$$c = w_2 w_1 a.$$

   $\implies$ Also gibt es ein Wort $w_3 \in \Sigma^*$ mit $c = w_3 a$ (nämlich $w_3 = w_2 w_1$).

   $\implies$ $a \sqsubseteq_s c$

□

Teilwortrelation $\sqsubseteq$

Sei Σ ein Alphabet und Σ^* die Menge aller Wörter über Σ. Für beliebige Wörter $u, v \in \Sigma^*$ gilt $u \sqsubseteq v$ genau dann, wenn es Wörter $w_1, w_2 \in \Sigma^*$ gibt mit $v = w_1 u w_2$. In kompakter Schreibweise heißt das:

$$u \sqsubseteq v \quad :\Longleftrightarrow \quad \exists w_1, w_2 \in \Sigma^* : v = w_1 u w_2 \ .$$

Somit ist $\sqsubseteq$ eine homogene Relation über Σ^*.

Beispiele

Für $\Sigma = \{a, b, c\}$ gilt beispielsweise $ab \sqsubseteq acabca$, $\epsilon \sqsubseteq acc$ und $baa \sqsubseteq baa$, aber $ca \not\sqsubseteq acba$, $cbac \not\sqsubseteq ab$ und $acbc \not\sqsubseteq bcac$.

Infos

- Für $u \sqsubseteq v$ sagen wir „u ist Teilwort von v“.
- Intuitiv heißt $u \sqsubseteq v$, dass das Wort u irgendwo in v vorkommt.

Eigenschaften der Teilwortrelation

Für die Teilwortrelation $\sqsubseteq$ gilt:

1. $\sqsubseteq$ ist reflexiv.
2. $\sqsubseteq$ ist nicht symmetrisch.
3. $\sqsubseteq$ ist nicht asymmetrisch.
4. $\sqsubseteq$ ist antisymmetrisch.
5. $\sqsubseteq$ ist nicht total.
6. $\sqsubseteq$ ist transitiv.

Eigenschaften der Teilwortrelation

1. $\sqsubseteq$ ist reflexiv.

   Zu zeigen ist:

   $$\forall a \in \Sigma^* : a \sqsubseteq a.$$

   Beweis:

   Sei $a \in \Sigma^*$ ein beliebiges Wort.

   $\Longrightarrow$ $a = \epsilon a \epsilon$.

   $\Longrightarrow$ Es gibt also Wörter $w_1, w_2 \in \Sigma^*$ mit $a = w_1 a w_2$, nämlich $w_1 = \epsilon$ und $w_2 = \epsilon$.

   $\Longrightarrow$ $a \sqsubseteq a$.

   $\square$.

Eigenschaften der Teilwortrelation

2. $\sqsubseteq$ ist nicht symmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \sqsubseteq b \text{ und } b \not\sqsubseteq a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \sqsubseteq b$ und $b \not\sqsubseteq a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xy$ und $b = xxyy$. □

Eigenschaften der Teilwortrelation

3. $\sqsubseteq$ ist nicht asymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \sqsubseteq b \text{ und } b \sqsubseteq a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \sqsubseteq b$ und $b \sqsubseteq a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xy$ und $b = xy$. $\square$

Eigenschaften der Teilwortrelation

4. $\sqsubseteq$ ist antisymmetrisch.

   Zu zeigen ist:

$$\forall a, b \in \Sigma^* : (a \sqsubseteq b \text{ und } b \sqsubseteq a) \implies a = b.$$

   Beweis:

   Seien $a, b \in \Sigma^*$ beliebige Wörter mit $a \sqsubseteq b$ und $b \sqsubseteq a$.

   $\implies$ Es gibt Wörter $w_1, w_2, w_3, w_4 \in \Sigma^*$ mit $b = w_1 a w_2$ und $a = w_3 b w_4$.

   $\implies$ Durch Einsetzen von $b = w_1 a w_2$ in $a = w_3 b w_4$ erhalten wir:

$$a = w_3 w_1 a w_2 w_4.$$

   $\implies$ w_1, w_2, w_3 und w_4 müssen alle leer sein.

   $\implies$ $b = \epsilon a \epsilon$ und $a = \epsilon b \epsilon$.

   $\implies$ $a = b$.

□

Eigenschaften der Teilwortrelation

5. $\sqsubseteq$ ist nicht total.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \not\sqsubseteq b \text{ und } b \not\sqsubseteq a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \not\sqsubseteq b$ und $b \not\sqsubseteq a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xy$ und $b = yx$. $\square$

Eigenschaften der Teilwortrelation

6. $\sqsubseteq$ ist transitiv.

   Zu zeigen ist:

$$\forall a, b, c \in \Sigma^* : (a \sqsubseteq b \text{ und } b \sqsubseteq c) \implies a \sqsubseteq c.$$

   Beweis:

   Seien $a, b, c \in \Sigma^*$ beliebige Wörter mit $a \sqsubseteq b$ und $b \sqsubseteq c$.

   $\implies$ Es gibt Wörter $w_1, w_2, w_3, w_4 \in \Sigma^*$ mit $b = w_1 a w_2$ und $c = w_3 b w_4$.

   $\implies$ Durch Einsetzen von $b = w_1 a w_2$ in $c = w_3 b w_4$ erhalten wir:

$$c = w_3 w_1 a w_2 w_4.$$

   $\implies$ Also gibt es Wörter $w_5, w_6 \in \Sigma^*$ mit $c = w_5 a w_6$ (nämlich $w_5 = w_3 w_1$ und $w_6 = w_2 w_4$).

   $\implies$ $a \sqsubseteq c$

□

Wortlängenrelation $\|$

Sei Σ ein Alphabet und Σ^* die Menge aller Wörter über Σ. Für beliebige Wörter $u, v \in \Sigma^*$ gilt $u \parallel v$ genau dann, wenn u und v dieselbe Länge haben. In kompakter Schreibweise heißt das:

$$u \parallel v \quad :\Longleftrightarrow \quad |u| = |v| \ .$$

Auch $\parallel$ ist also eine homogene Relation über Σ^*.

Beispiele

Für $\Sigma = \{a, b, c\}$ gilt beispielsweise $ab \parallel bc$, $b \parallel c$ und $abc \parallel bcc$, aber $ab \nparallel bac$, $cb \nparallel c$ und $ac \nparallel bcac$.

Infos

Für $u \parallel v$ sagen wir „u und v sind gleich lang“.

Eigenschaften der Wortlängenrelation

Für die Wortlängenrelation $\|$ gilt:

1. $\|$ ist reflexiv.
2. $\|$ ist symmetrisch.
3. $\|$ ist nicht asymmetrisch.
4. $\|$ ist nicht antisymmetrisch.
5. $\|$ ist nicht total.
6. $\|$ ist transitiv.

Diese Aussagen werden in den nächsten 6 Folien gezeigt.

Eigenschaften der Wortlängenrelation

1. $\parallel$ ist reflexiv.

   Zu zeigen ist:

   $$\forall a \in \Sigma^* : a \parallel a.$$

   Beweis:

   Sei $a \in \Sigma^*$ ein beliebiges Wort.

   $\Longrightarrow$ $|a| = |a|$.

   $\Longrightarrow$ $a \parallel a$.

□

Eigenschaften der Wortlängenrelation

2. $\parallel$ ist symmetrisch.

   Zu zeigen ist:

$$\forall a, b \in \Sigma^* : a \parallel b \implies b \parallel a.$$

   Beweis:

   Seien $a, b \in \Sigma^*$ beliebige Wörter mit $a \parallel b$.

$\implies$ $|a| = |b|$.

$\implies$ $|b| = |a|$.

$\implies$ $b \parallel a$.

□

Eigenschaften der Wortlängenrelation

3. $\parallel$ ist nicht asymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \parallel b \text{ und } b \parallel a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \parallel b$ und $b \parallel a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xy$ und $b = xy$. $\square$

Eigenschaften der Wortlängenrelation

4. $\parallel$ ist nicht antisymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \parallel b, b \parallel a \text{ und } a \neq b.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \parallel b$, $b \parallel a$ und $a \neq b$ gelten, z.B. $\Sigma = \{x, y\}$, $a = xx$ und $b = yy$. □

Eigenschaften der Wortlängenrelation

5. $\parallel$ ist nicht total.

   Zu zeigen ist:

   $$\exists a, b \in \Sigma^* : a \nparallel b \text{ und } b \nparallel a.$$

   Beweis:

   Als Gegenbeispiel sind zwei Wörter $a, b \in \Sigma^*$ gesucht, für die $a \nparallel b$ und $b \nparallel a$ gelten, z.B. $\Sigma = \{x, y\}$, $a = x$ und $b = yyy$. $\square$

Eigenschaften der Wortlängenrelation

6. $\parallel$ ist transitiv.

   Zu zeigen ist:

$$\forall a, b, c \in \Sigma^* : (a \parallel b \text{ und } b \parallel c) \implies a \parallel c.$$

   Beweis:

   Seien $a, b, c \in \Sigma^*$ beliebige Wörter mit $a \parallel b$ und $b \parallel c$.

$\implies$ $|a| = |b|$ und $|b| = |c|$.

$\implies$ $|a| = |b| = |c|$.

$\implies$ $|a| = |c|$.

$\implies$ $a \parallel c$.

□

Tipp

Wenn man selber entscheiden muss, ob eine Eigenschaft gilt oder nicht, dann sollte man sich die Relation (bzw. einen Teil davon) graphisch vorstellen und die Tricks auf Folien 259 und 261 benutzen.

Quizfragen

Sei $\bowtie$ eine homogene Relation über Zahlenpaare aus $\mathbb{Z} \times \mathbb{Z}$ mit

$$(a, b) \bowtie (c, d) \quad :\Longleftrightarrow \quad a \cdot d = b \cdot c$$

für alle $a, b, c, d \in \mathbb{Z}$.

1. Ist $\bowtie$ reflexiv?
2. Ist $\bowtie$ symmetrisch?
3. Ist $\bowtie$ asymmetrisch?
4. Ist $\bowtie$ antisymmetrisch?
5. Ist $\bowtie$ total?
6. Ist $\bowtie$ transitiv?

Beweise deine Antworten!

1. $\bowtie$ ist reflexiv.

   Seien $a, b \in \mathbb{Z}$ beliebige ganze Zahlen.

   $\implies$ $a \cdot b = b \cdot a$.

   $\implies$ $(a, b) \bowtie (a, b)$.

   □

2. $\bowtie$ ist symmetrisch.

   Seien $a, b, c, d \in \mathbb{Z}$ beliebige ganze Zahlen mit $(a, b) \bowtie (c, d)$.

   $\implies$ $a \cdot d = b \cdot c$.

   $\implies$ $c \cdot b = a \cdot d$.

   $\implies$ $(c, d) \bowtie (a, b)$

   □

3. $\bowtie$ ist nicht asymmetrisch.

   Als Gegenbeispiel sind ganze Zahlen $a, b, c, d \in \mathbb{Z}$ gesucht, für die $(a, b) \bowtie (c, d)$ und $(c, d) \bowtie (a, b)$ gelten, z.B. $a = 1$, $b = 2$, $c = 2$ und $d = 4$. □

4. $\bowtie$ ist nicht antisymmetrisch.

   Als Gegenbeispiel sind ganze Zahlen $a, b, c, d \in \mathbb{Z}$ gesucht, für die $(a, b) \bowtie (c, d)$, $(c, d) \bowtie (a, b)$ und $(a, b) \neq (c, d)$ gelten, z.B. $a = 1$, $b = 2$, $c = 2$ und $d = 4$. □

5. $\bowtie$ ist nicht total.

   Als Gegenbeispiel sind ganze Zahlen $a, b, c, d \in \mathbb{Z}$ gesucht, für die $(a, b) \not\bowtie (c, d)$ und $(c, d) \not\bowtie (a, b)$ gelten, z.B. $a = 1$, $b = 2$, $c = 3$ und $d = 4$. □

6. $\bowtie$ ist transitiv.

   Seien $a, b, c, d, e, f \in \mathbb{Z}$ beliebige ganze Zahlen mit $(a, b) \bowtie (c, d)$ und $(c, d) \bowtie (e, f)$.

   $\Longrightarrow$ Es gilt $a \cdot d = b \cdot c$ und $c \cdot f = d \cdot e$.

   $\Longrightarrow$ Durch Gleichsetzen erhalten wir:

$$a \cdot d \cdot c \cdot f = b \cdot c \cdot d \cdot e.$$

   $\Longrightarrow$ Kürzen von $c \cdot d$ auf beiden Seiten liefert: $a \cdot f = b \cdot e$.

   $\Longrightarrow$ $(a, b) \bowtie (e, f)$.

   □

Knifflige Quizfragen

Sei $\wr$ eine homogene Relation über den ganzen Zahlen $\mathbb{Z}$ mit

$$x \wr y \quad :\Longleftrightarrow \quad \exists k \in \mathbb{Z} : y^2 = k \cdot x$$

für alle $x, y \in \mathbb{Z}$.

1. Ist $\wr$ reflexiv?
2. Ist $\wr$ symmetrisch?
3. Ist $\wr$ asymmetrisch?
4. Ist $\wr$ antisymmetrisch?
5. Ist $\wr$ total?
6. Ist $\wr$ transitiv?

Beweise deine Antworten!

1. $\wr$ ist reflexiv.

   Sei $a \in \mathbb{Z}$ eine beliebige ganze Zahl.

   $\Longrightarrow$ Es gibt ein $k \in \mathbb{Z}$ mit $a^2 = k \cdot a$, nämlich $k = a$.

   □

2. $\wr$ ist nicht symmetrisch.

   Als Gegenbeispiel sind ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \wr b$ und $b \not\wr a$ gelten, z.B. $a = 4$ und $b = 6$. □

3. $\wr$ ist nicht asymmetrisch.

   Als Gegenbeispiel sind ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \wr b$ und $b \wr a$ gelten, z.B. $a = 2$ und $b = 4$. □

4. $\wr$ ist nicht antisymmetrisch.

   Als Gegenbeispiel sind ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \wr b$, $b \wr a$ und $a \neq b$ gelten, z.B. $a = 2$ und $b = 4$. □

5. $\wr$ ist nicht total.

   Als Gegenbeispiel sind ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \not\wr b$ und $b \not\wr a$ gelten, z.B. $a = 2$ und $b = 3$. □

6. $\wr$ ist nicht transitiv. Als Gegenbeispiel sind ganze Zahlen $a, b, c \in \mathbb{Z}$ gesucht, für die $a \wr b$, $b \wr c$ und $a \not\wr c$ gelten, z.B. $a = 8$, $b = 4$ und $c = 2$. □

Komposition von Relationen

Sei R eine homogene Relation über einer Menge A. Dann gilt für ein beliebiges $n \in \mathbb{N}_0$:

$$\begin{array}{lcl} R^0 & = & \{(x,x)\}\, x \in A \quad = \quad \mathrm{id}_A \\ R^{n+1} & = & R^n \circ R \end{array}$$

Aus dieser Definition und $\mathrm{id}_A \circ R = R = R \circ \mathrm{id}_A$ folgt sofort:

$$R^1 = R^0 \circ R = \mathrm{id}_A \circ R = R.$$

Beispiel

Für eine beliebige homogene Relation R gilt:

$$\begin{aligned} R^4 &= R^3 \circ R \\ &= (R^2 \circ R) \circ R \\ &= ((R^1 \circ R) \circ R) \circ R \\ &= ((R \circ R) \circ R) \circ R. \end{aligned}$$

Aufgrung der Assoziativität des Relationenprodukts schreiben wir oft auch einfach:

$$R^4 = R \circ R \circ R \circ R.$$

Aus dieser formalen Definition von R^n folgt, zusammen mit der Assoziativität des Relationenprodukts, die etwas intuitivere Variante:

$$R^n = \underbrace{R \circ R \circ \ldots \circ R}_{n \text{ mal}}.$$

Graphische Bedeutung

Intuitiv enthält R^n alle Abkürzungen für Wege der Länge genau n in der graphischen Darstellung von R. Es gilt nämlich:

$$R^0 = \{(a,b) \in A \times A\}\ a = b$$
$$R^n = \{(a,b) \in A \times A\}\ \exists x_1, \ldots, x_{n-1} \in M : (a,x_1), (x_1,x_2), \ldots, (x_{n-1},b) \in R$$

D.h., falls der Graph von R folgende Kanten enthält:

$$\underbrace{a \longrightarrow x_1 \longrightarrow x_2 \longrightarrow \ldots \longrightarrow x_{n-1} \longrightarrow b}_{\text{Weg der Länge } n \text{ von a nach b in } R},$$

dann enthält der Graph von R^n die Kante

$$\underbrace{a \longrightarrow b}_{\text{Kante von } a \text{ nach } b \text{ in } R^n} .$$

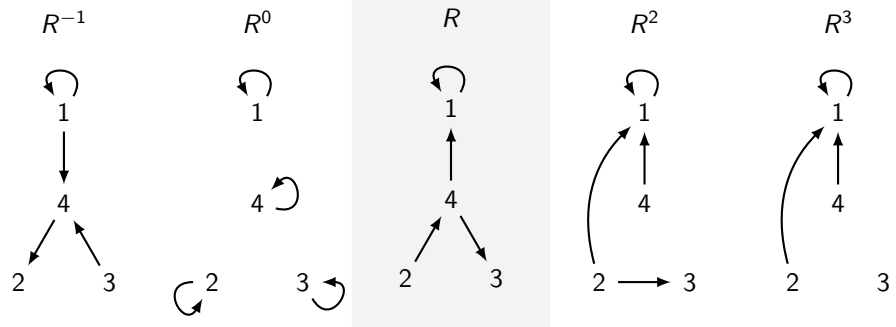
$x_1, \ldots, x_{n-1}$, a und b müssen nicht unbedingt alle verschieden sein!

Beispiel

Sei R eine homogene Relation über $[4]$ mit

$$R = \{(1,1),(2,4),(4,1),(4,3)\}\,.$$

Die Graphische Darstellungen von R^{-1}, R^0, R, R^2 und R^3 sind:



$R^4, R^5, R^6, \ldots$ gleichen alle R^3.

Hüllen von Relationen

Sei R eine homogene Relation über einer Menge A. Die reflexive Hülle R^{ref} von R ist die kleinste Relation, die R enthält und reflexiv ist. Es muss gelten:

(1) $R \subseteq R^{\text{ref}}$,

(2) R^{ref} reflexiv und

(3) $\forall R' \subseteq A \times A : (R \subseteq R' \text{ und } R' \text{ reflexiv } \implies R^{\text{ref}} \subseteq R')$

Analog sind die symmetrische Hülle R^{sym}, die transitive Hülle R^+ und die reflexive transitive Hülle R^* definiert.

Die Definitionen sind aber für uns kaum wichtig. Wichtig ist, wie man die Hüllen berechnet. Hierfür gibt es folgende Formeln:

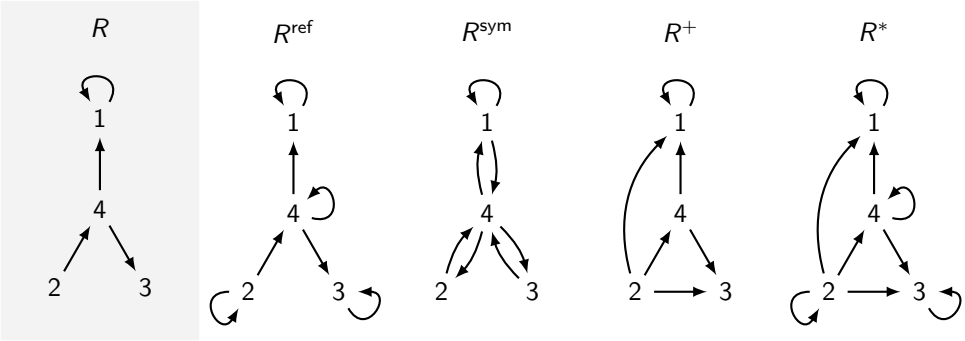
$$\begin{array}{lcll} R^{\text{ref}} & = & R^0 \cup R, & \\ R^{\text{sym}} & = & R \cup R^{-1}, & \\ R^+ & = & R \cup R^2 \cup R^3 \cup R^4 \cup \ldots & = \bigcup_{i=1}^{\infty} R^i, \\ R^* & = & R^0 \cup R \cup R^2 \cup R^3 \cup R^4 \cup \ldots & = \bigcup_{i=0}^{\infty} R^i. \end{array}$$

Beispiel

Sei R wieder die homogene Relation über [5] aus Folie 332 mit

$$R = \{(1,1),(2,4),(3,5),(4,1),(4,3)\}\,.$$

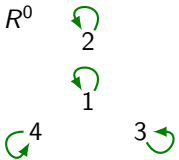
Die Graphische Darstellung von R, R^{ref}, R^{sym}, R^{+} und R^{*} sind:

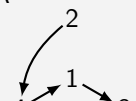


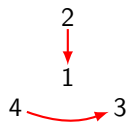
Buntes Beispiel

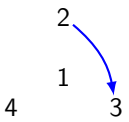
Sei $R = \{(1,3),(2,4),(4,1)\}$ eine homogene Relation über $[4]$. Dann gilt:

R^{-1} 

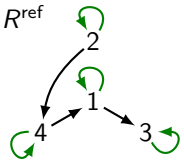
R^0 

R 

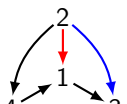
R^2 

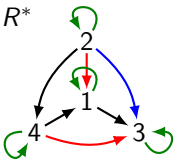
R^3 

Wegen $R^4 = R^5 = R^6 = \ldots = \emptyset$ gilt für die Hüllen:

R^{ref} 

R^{sym} 

R^+ 

R^* 

Quizfrage

Sei R eine homogene Relation über $[3]$ mit

$$R = \{(1,2),(2,3),(3,1)\}\,.$$

Was sind R^{ref}, R^{sym}, R^{+} und R^{*}?

Es gilt:

$$R^{\text{ref}} = \{(1,1),(1,2),(2,2),(2,3),(3,1),(3,3)\}, \tag{1}$$
$$R^{\text{sym}} = \{(1,2),(1,3),(2,1),(2,3),(3,2),(3,1)\}, \tag{2}$$
$$R^{+} = R^{*} = [3] \times [3]. \tag{3}$$

Quizfrage

Wieso gibt es keine asymmetrische, antisymmetrische oder totale Hüllen?

Weil sie keinen Sinn machen würden!

- Eine Relation, die nicht asymmetrisch (bzw. nicht antisymmetrisch) ist, kann durch das Hinzufügen von Tupeln nicht asymmetrisch (bzw. antisymmetrisch) gemacht werden.
- Für eine nicht totale Relation R gibt es mehrere totale Relationen, die R enthalten und minimal wären.

Themenübersicht

Äquivalenzrelationen

Seien A eine Menge und R eine homogene Relation über A. Dann gilt:

$$R \text{ Äquivalenzrelation} \quad :\Longleftrightarrow \quad R \text{ reflexiv, symmetrisch und transitiv}$$

Wichtig: Diese Definition schließt nicht aus, dass R mehr als diese drei Eigenschaften besitzen kann.

Beispiele

- Die Gleichheitsrelation $=$ (bzw. id_A) über einer beliebigen Menge A ist eine Äquivalenzrelation über A.
- Das kartesische Produkt $A \times A$ ist für jede Menge A eine Äquivalenzrelation.
- Die Kongruenzrelation $\equiv_n$ modulo n ist eine Äquivalenzrelation über $\mathbb{Z}$ (s. Folie 419).
- Die Wortlängenrelation $\parallel$ ist für jedes Alphabet Σ eine Äquivalenzrelation über Σ^* (s. Folie 311).

Info

Für Äquivalenzrelationen benutzt man typischerweise Symbole mit geraden Strichen und Schlangen, z.B.: $=$, $\equiv$, $\sim$, $\simeq$ und $\cong$.

Äquivalenzrelationen und Partitionen

Jede Äquivalenzrelation $\sim$ über einer Grundmenge A induziert genau eine Partition von A. Diese Partition wird Faktormenge oder Quotientenmenge genannt und mit $A/\sim$ notiert. Die Klassen in $A/\sim$ heißen dann Äquivalenzklassen und die Anzahl $|A/\sim|$ der Äquivalenzklassen wird Index der Äquivalenzrelation genannt. Innerhalb einer Äquivalenzklasse steht also jedes Element mit jedem anderen in Relation. Dagegen stehen zwei Elemente aus verschiedenen Äquivalenzklassen nie in Relation.

Definiert man $[x]_\sim = \{y \mid x \sim y\}$ als die Menge aller Elemente zu denen x in Relation steht, dann gilt für alle $a, b \in A$:

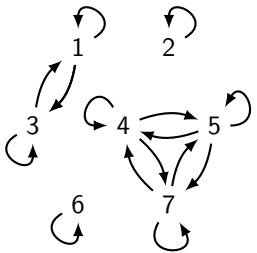
$$a \sim b \iff [a]_\sim = [b]_\sim$$

und

$$A/\sim = \{[a]_\sim \mid a \in A\}\,.$$

Beispiel

Sei $\sim$ die folgende Äquivalenzrelation über $[7]$.



Dann gilt:

$$[7]/\sim = \{\{1,3\},\{2\},\{4,5,7\},\{6\}\}.$$

Gegeben seien folgende Äquivalenzrelationen $R_1, \ldots, R_5$ über $[4]$:

1. $R_1 = \{(1,1),(1,2),(2,1),(2,2),(3,3),(4,4)\}$,
2. $R_2 = \{(1,1),(1,4),(2,2),(2,3),(3,2),(3,3),(4,1),(4,4)\}$,
3. $R_3 = \{(1,1),(1,3),(1,4),(2,2),(3,1),(3,3),(3,4),(4,1),(4,3),(4,4)\}$,
4. $R_4 = [4] \times [4]$,
5. $R_5 = \mathrm{id}_{[4]}$.

Wie sehen die Faktormengen $[4]/R_i$ für $i = 1, 2, 3, 4, 5$ aus?

Antworten

1. $[4]/R_1 = \{\{1,2\},\{3\},\{4\}\}$.
2. $[4]/R_2 = \{\{1,4\},\{2,3\}\}$.
3. $[4]/R_3 = \{\{1,3,4\},\{2\}\}$
4. $[4]/R_4 = \{\{1,2,3,4\}\}$.
5. $[4]/R_5 = \{\{1\},\{2\},\{3\},\{4\}\}$.

Beispiel

Sei $\Sigma = \{a, b, c\}$ ein Alphabet und $L \subseteq \Sigma^*$ eine Sprache mit

$$L = \{\epsilon, a, b, c, ab, ac, bc, abc\}.$$

Für die Einschränkung der Wortlängenrelation $\|$ auf L gilt:

$$L/\| = \{\{\epsilon\}, \{a, b, c\}, \{ab, ac, bc\}, \{abc\}\}.$$

Quizfrage

Sei $\Sigma = \{a, b\}$ ein Alphabet und $L \subseteq \Sigma^*$ eine Sprache mit

$$L = \{\epsilon, a, b, aa, ab, bb, aaa, aab, abb, bbb\}\,.$$

Wie sieht $L/\!\|$ aus?

Für die Einschränkung der Wortlängenrelation $\|$ auf L gilt:

$$L/\| = \{\{\epsilon\}, \{a, b\}, \{aa, ab, bb\}, \{aaa, aab, abb, bbb\}\}.$$

Beispiel

Für die Einschränkung der Kongruenzrelation $\equiv_4$ modulo 4 auf $[12]$ gilt:

$$[12]/\equiv_4 = \{\{1,5,9\},\{2,6,10\},\{3,7,11\},\{4,8,12\}\}.$$

Quizfrage

Wie sieht $[9]/\equiv_3$ aus?

Für die Einschränkung der Kongruenzrelation $\equiv_3$ modulo 3 auf $[9]$ gilt:

$$[9]/\equiv_3 = \{\{1,4,7\},\{2,5,8\},\{3,6,9\}\}.$$

Sei $\sim$ eine Äquivalenzrelation über Zahlenpaare aus $\mathbb{Z} \times \mathbb{Z}$ mit

$$(a, b) \sim (c, d) \quad :\Longleftrightarrow \quad a + b = c + d$$

für alle $a, b, c, d \in \mathbb{Z}$.

1. Wieso ist $\sim$ reflexiv?
2. Wieso ist $\sim$ symmetrisch?
3. Wieso ist $\sim$ transitiv?
4. Wie sieht $([3] \times [3])/\sim$ aus?

Versuch deine Begründungen zu den ersten drei Fragen als formale Beweise zu formulieren.

1. Seien $a, b \in \mathbb{Z}$ beliebige ganze Zahlen.

   $\Longrightarrow$ Wegen $a + b = a + b$ gilt auch $(a, b) \sim (a, b)$.

□

2. Seien $a, b, c, d \in \mathbb{Z}$ beliebige ganze Zahlen mit $(a, b) \sim (c, d)$.

   $\Longrightarrow$ $a + b = c + d$.

   $\Longrightarrow$ $c + d = a + b$.

   $\Longrightarrow$ $(c, d) \sim (a, b)$.

□

3. Seien $a, b, c, d, e, f \in \mathbb{Z}$ beliebige ganze Zahlen mit $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$.

$\implies$ $a + b = c + d$ und $c + d = e + f$.

$\implies$ $a + b = e + f$.

$\implies$ $(a, b) \sim (e, f)$.

□

4. Für die Einschränkung von $\sim$ auf $[3] \times [3]$ gilt:

$$([3] \times [3])/\sim = \{\{(1,1)\}, \{(1,2),(2,1)\}, \{(1,3),(2,2),(3,1)\}, \{(2,3),(3,2)\}, \{(3,3)\}\}.$$

Info

Die Zuordnung zwischen Äquivalenzrelationen und Partitionen ist eindeutig. D.h.

- für jede Äquivalenzrelation R über A gibt es genau eine Partition P von A bzw.
- für jede Partition P von A gibt es genau eine Äquivalenzrelation R über A

mit $P = A/R$.

Somit ist beispielsweise die Anzahl der Äquivalenzrelationen über einer Menge A gleich der Anzahl der Partitionen von A.

Beispiel

Es gibt genau zwei verschiedene Äquivalenzrelationen über [2], weil die Menge [2] auf genau zwei verschiedenen Weisen partitioniert werden kann.

Partitionen	Äquivalenzrelationen
$\{\{1\},\{2\}\}$	$\{(1,1),(2,2)\}$
$\{\{1,2\}\}$	$\{(1,1),(1,2),(2,1),(2,2)\}$

Quizfrage

Wie viele verschiedene Äquivalenzrelationen gibt es über [3]?

Es gibt 5 verschiedene Partitionen der Menge [3]. Somit sind das auch genau 5 Äquivalenzrelationen:

Partitionen	Äquivalenzrelationen
$\{\{1\},\{2\},\{3\}\}$	$\{(1,1),(2,2),(3,3)\}$
$\{\{1,2\},\{3\}\}$	$\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$
$\{\{1,3\},\{2\}\}$	$\{(1,1),(2,2),(3,3),(1,3),(3,1)\}$
$\{\{1\},\{2,3\}\}$	$\{(1,1),(2,2),(3,3),(2,3),(3,2)\}$
$\{\{1,2,3\}\}$	$\{(1,1),(2,2),(3,3),(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)\}$

Themenübersicht

Partielle Ordnungen

Seien A eine Menge und R eine homogene Relation über A. Dann gilt:

$$R \text{ partielle Ordnung} \quad :\Longleftrightarrow \quad R \text{ reflexiv, antisymmetrisch und transitiv}$$

Eine totale Ordnung ist eine partielle Ordnung, die zusätzlich total ist.

Wie bei der Äquivalenzrelation, schließt diese Definition nicht aus, dass R mehr als diese drei Eigenschaften besitzen kann.

Beispiele

- Die Gleichheitsrelation $=$ (bzw. id_A) über einer beliebigen Menge A ist eine partielle Ordnung über A.
- $\leq$ ist eine totale Ordnung über $\mathbb{Z}$.
- Für jede Menge A ist $\subseteq$ eine partielle Ordnung über $\mathcal{P}(A)$.
- Die Einschränkung von $|$ auf $\mathbb{N}_0$ ist eine partielle Ordnung (s. Folie 400).
- Für jedes Alphabet Σ sind die Relationen $\sqsubseteq_p$, $\sqsubseteq_s$ und $\sqsubseteq$ partielle Ordnungen (s. Folien 281, 291 und 301).

Partielle Ordnungen und Hasse-Diagramme

Jeder partiellen Ordnung R über einer Menge A kann man ein eindeutiges Hasse-Diagramm zuordnen und umgekehrt. Man entfernt hierzu alle reflexiven und transitiven Tupel von R und definiert das Ergebnis als Relation H:

$$H = \{(a, b) \in R\}\ a \neq b \text{ und } \nexists\, x \in A : (a, x) \in R \text{ und } (x, b) \in R.$$

Das Hasse-Diagramm ist dann die graphische Darstellung von H, in der die Elemente so angeordnet sind, dass alle Pfeile von unten nach oben zeigen.

Fügt man einem Hasse-Diagramm H alle reflexive und transitive Tupel hinzu, so bekommt man die entsprechende partielle Ordnung R. Formal ist R also die reflexive transitive Hülle von H, d.h.: $R = H^*$.

Infos

- Mit Hasse-Diagrammen lassen sich Hierarchien graphisch darstellen. Jedes Element zeigt auf seinen direkten Vorgesetzten.
- Ein Hasse-Diagramm muss nicht notwendigerweise zusammenhängend sein! Es kann aus mehreren Teilen bestehen, die nicht miteinander verbunden sind.
- Weil die Richtung der Pfeile durch die Anordnung der Knoten bestimmt wird, können die Pfeilspitzen auch weggelassen werden.

Beispiel

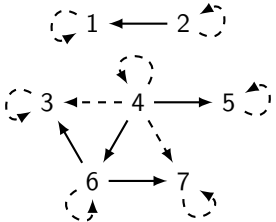
Sei R mit

$$R = \mathrm{id}_{[7]} \cup \{(2,1),(4,3),(4,5),(4,6),(4,7),(6,3),(6,7)\}$$

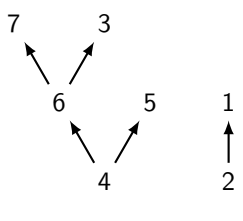
$\{(1,1),\ldots,(7,7)\}$

eine partielle Ordnung über [5].

R kann wie folgt durch das Hasse-Diagramm H graphisch dargestellt werden.



R



H

H entspricht genau R ohne transitive und reflexive Tupel (gestrichelte Pfeile).

Minimale und Maximale Elemente

Seien A eine Menge und R eine partielle Ordnung über A. Dann gilt für alle $a, b \in A$:

$$\begin{aligned} a \text{ minimal} &:\iff (\forall x \in A : (x, a) \in R \implies x = a) \\ b \text{ maximal} &:\iff (\forall y \in A : (b, y) \in R \implies y = b) \end{aligned}$$

Falls $(a, b) \in R$ für $a \neq b$ gilt, dann sagen wir „a ist kleiner als b“ bzw. „b ist größer als a“, analog zur partiellen Ordnung $\leq$.

Info

Intuitiv ist ein Element

- minimal, falls es in keinem Tupel rechts von einem anderen Element steht und
- maximal, falls es in keinem Tupel links von einem anderen Element steht.

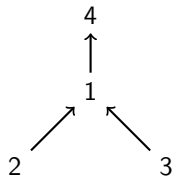
Wenn a kleiner als b ist, dann muss b im Hasse-Diagramm über a gezeichnet werden!

Gegeben seien folgende partielle Ordnungen über [4]:

1. $R_1 = \{(1,1),(1,4),(2,1),(2,2),(2,4),(3,1),(3,3),(3,4),(4,4)\}$,
2. $R_2 = \{(1,1),(2,1),(2,2),(3,3),(3,4),(4,4)\}$,
3. $R_3 = \{(1,1),(1,3),(2,1),(2,2),(2,3),(2,4),(3,3),(4,3),(4,4)\}$.

Wie sieht das Hasse-Diagramm H_i zu jeder partiellen Ordnung R_i aus? Welche Elemente sind minimal? Welche maximal?

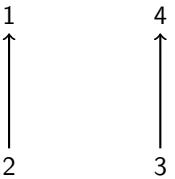
H_1 :



minimal: 2 und 3

maximal: 4

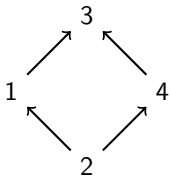
H_2 :



minimal: 2 und 3

maximal: 1 und 4

H_3 :



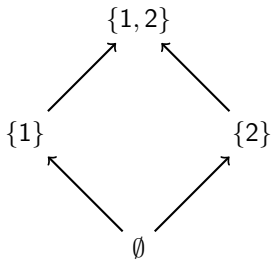
minimal: 2

maximal: 3

Beispiel

Die Einschränkung der Teilmengenrelation $\subseteq$ auf $\mathcal{P}([2])$ kann durch folgendes Hasse-Diagramm H graphisch dargestellt werden:

H :



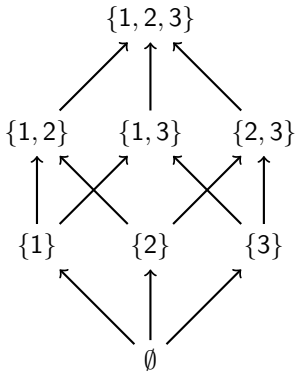
$\emptyset$ ist das einzige minimale Element und $\{1, 2\}$ das einzige maximale.

Quizfrage

Wie sieht das Hasse-Diagramm H zur Einschränkung der Teilmengenrelation $\subseteq$ auf $\mathcal{P}([3])$ aus?

Hasse-Diagramm H zu $\subseteq$:

H :

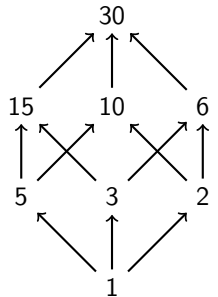


$\emptyset$ ist das einzige minimale Element und $\{1, 2, 3\}$ das einzige maximale.

Beispiel

Sei $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Die Einschränkung der Teilbarkeitsrelation $\mid$ auf A kann durch folgendes Hasse-Diagramm H graphisch dargestellt werden:

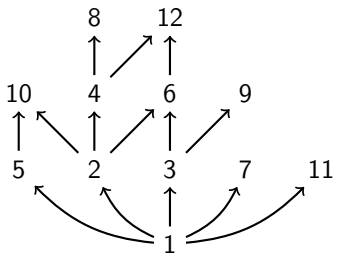
H :



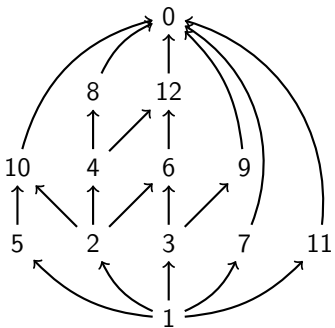
1 ist das einzige minimale Element und 30 das einzige maximale.

1. Wie sieht das Hasse-Diagramm H zur Einschränkung der Teilbarkeitsrelation $\mid$ auf $[12]$ aus?
2. Wie würde das Hasse-Diagramm aus 1. aussehen, wenn man die 0 mitberücksichtigen würde?

1.



2.



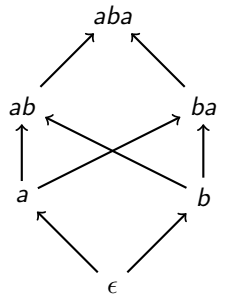
Beispiel

Sei $\Sigma = \{a, b, c\}$ ein Alphabet und $L \subseteq \Sigma^*$ mit

$$L = \{\epsilon, a, b, ab, ba, aba\}\,.$$

Die Einschränkung der Teilwortrelation $\sqsubseteq$ auf L kann durch folgendes Hasse-Diagramm H graphisch dargestellt werden:

H :



ϵ ist das einzige minimale Element und aba das einzige maximale.

Quizfrage

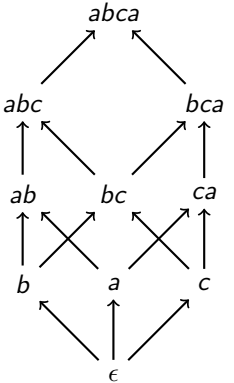
Sei $\Sigma = \{a, b, c\}$ ein Alphabet und $L \subseteq \Sigma^*$ mit

$$L = \{\epsilon, a, b, c, ab, bc, ca, abc, bca, abca\}\,.$$

Wie sieht das Hasse-Diagramm H zur Einschränkung der Teilwortrelation $\sqsubseteq$ auf L aus?

Hasse-Diagramm H:

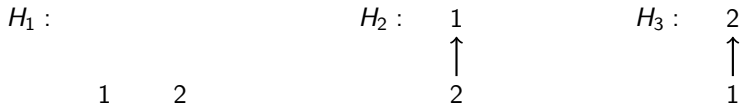
H :



ϵ ist das einzige minimale Element und *abca* das einzige maximale.

Beispiel

Es gibt genau 3 verschiedene Hasse-Diagramme H_1, H_2, H_3 über [2]:



Jedes Hasse-Diagramm H_i stellt genau eine partielle Ordnung R_i dar. Es gibt also genau 3 partielle Ordnungen über [2]:

$$R_1 = \{(1,1),(2,2)\}, \qquad R_2 = \{(1,1),(2,1),(2,2)\}, \qquad R_3 = \{(1,1),(1,2),(2,2)\}.$$

Wie viele verschiedene partielle Ordnungen gibt es über der Grundmenge $[3]$?

Hinweis: Es reicht alle möglichen Hasse-Diagramme zu finden. Zu jedem Hasse-Diagramm H ist nämlich $R = H^*$ die entsprechende partielle Ordnung.

Es gibt 19 verschiedene Hasse-Diagramme (und somit auch genau 19 partielle Ordnungen) über [3]:

- eins, in dem alle 3 Elemente minimal und maximal sind:

$$H_1: \quad 1 \qquad 2 \qquad 3$$

- sechs, in denen ein Element minimal, eins maximal und eins beides ist:

$$H_2: \begin{array}{ccc} 1 & & \\ \uparrow & & 3 \\ 2 & & \end{array} \qquad H_3: \begin{array}{ccc} 1 & & \\ \uparrow & & 2 \\ 3 & & \end{array} \qquad H_4: \begin{array}{ccc} 2 & & \\ \uparrow & & 3 \\ 1 & & \end{array}$$

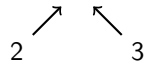
$$H_5: \begin{array}{ccc} 2 & & \\ \uparrow & & 1 \\ 3 & & \end{array} \qquad H_6: \begin{array}{ccc} 3 & & \\ \uparrow & & 2 \\ 1 & & \end{array} \qquad H_7: \begin{array}{ccc} 3 & & \\ \uparrow & & 1 \\ 2 & & \end{array}$$

- sechs, in denen ein Element minimal ist, eins maximal und eins beides:

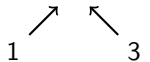
$$H_8: \begin{matrix}1\\ \uparrow\\ 2\\ \uparrow\\ 3\end{matrix} \qquad H_9: \begin{matrix}1\\ \uparrow\\ 3\\ \uparrow\\ 2\end{matrix} \qquad H_{10}: \begin{matrix}2\\ \uparrow\\ 1\\ \uparrow\\ 3\end{matrix} \qquad H_{11}: \begin{matrix}2\\ \uparrow\\ 3\\ \uparrow\\ 1\end{matrix} \qquad H_{12}: \begin{matrix}3\\ \uparrow\\ 1\\ \uparrow\\ 2\end{matrix} \qquad H_{13}: \begin{matrix}3\\ \uparrow\\ 2\\ \uparrow\\ 1\end{matrix}$$

- drei, in denen ein Element maximal ist und zwei minimal:

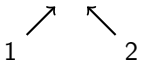
H_{14} :



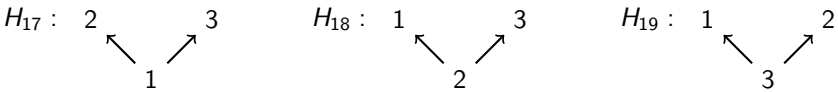
H_{15} :



H_{16} :



- drei, in denen ein Element minimal ist und zwei maximal:



Sei $\leq_2$ eine partielle Ordnung über Zahlenpaare aus $\mathbb{Z} \times \mathbb{Z}$ mit

$$(a, b) \leq_2 (c, d) \quad :\Longleftrightarrow \quad a \leq c \text{ und } b \leq d$$

für alle $a, b, c, d \in \mathbb{Z}$.

1. Wieso ist $\leq_2$ reflexiv?
2. Wieso ist $\leq_2$ antisymmetrisch?
3. Wieso ist $\leq_2$ transitiv?
4. Wie sieht das Hasse-Diagramm der Einschränkung von $\leq_2$ auf $[3] \times [3]$?

Hinweis: Bei den ersten drei Fragen sind Beweise verlangt.

1. Seien $a, b \in \mathbb{Z}$ beliebige ganze Zahlen.

   $\Longrightarrow$ Wegen $a \leq a$ und $b \leq b$ gilt auch $(a, b) \leq_2 (a, b)$.

□

2. Seien $a, b, c, d \in \mathbb{Z}$ beliebige ganze Zahlen mit $(a, b) \leq_2 (c, d)$ und $(c, d) \leq_2 (a, b)$.

   $\Longrightarrow$ $a \leq c$, $b \leq d$, $c \leq a$ und $d \leq b$.

   $\Longrightarrow$ $a = c$ und $b = d$.

   $\Longrightarrow$ $(a, b) = (c, d)$.

□

3. Seien $a, b, c, d, e, f \in \mathbb{Z}$ beliebige ganze Zahlen mit $(a, b) \leq_2 (c, d)$ und $(c, d) \leq_2 (e, f)$.

   $\Longrightarrow$ $a \leq c$, $b \leq d$, $c \leq e$ und $d \leq f$.

   $\Longrightarrow$ $a \leq c \leq e$ und $b \leq d \leq f$.

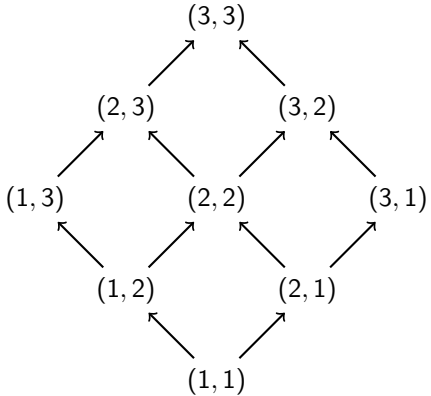
   $\Longrightarrow$ $a \leq e$ und $b \leq f$.

$\Longrightarrow \quad (a, b) \leq_2 (e, f)$.

□

4. Hasse-Diagramm H zur Einschränkung von $\leq_2$ auf $[3] \times [3]$:

H :



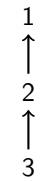
$(1, 1)$ ist das einzige minimale Element und $(3, 3)$ das einzige maximale.

Gegeben seien folgende totale Ordnungen über [3]:

1. $R_1 = \{(1,1),(2,1),(2,2),(3,1),(3,2),(3,3)\}$,
2. $R_2 = \{(1,1),(1,3),(2,1),(2,2),(2,3),(3,3)\}$,
3. $R_3 = \{(1,1),(1,2),(1,3),(2,2),(3,2),(3,3)\}$.

Wie sieht das Hasse-Diagramm H_i zu jeder totalen Ordnung R_i aus?

H_1 :



H_2 :

H_3 :

Quizfrage

Wie sieht das Hasse-Diagramm H zur Einschränkung der Kleiner-gleich-Relation $\leq$ auf $[5]$ aus?


H :
5
4
3
2
1

Quizfrage

Wie viele totale Ordnungen gibt es über $[6]$?

So viele wie die Anzahl der Möglichkeiten 6 verschiedene Objekte in eine Reihe zu ordnen:

$$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$$

Themenübersicht

Teilbarkeitsrelation |

Für beliebige ganze Zahlen $x, y \in \mathbb{Z}$ gilt $x \mid y$ genau dann, wenn es eine natürliche Zahl $k \in \mathbb{Z}$ gibt mit $y = kx$. In kompakter Schreibweise heißt das:

$$x \mid y \quad :\Longleftrightarrow \quad \exists k \in \mathbb{Z} : y = k \cdot x \ .$$

Somit ist $\mid$ eine homogene Relation über $\mathbb{Z}$.

Beispiele

Es gilt beispielsweise $3 \mid -12$, $4 \mid 12$ und $-6 \mid 12$, aber $5 \nmid 12$, $-7 \nmid 12$ und $8 \nmid 12$.

Infos

- Für $x \mid y$ sagen wir „x teilt y“, „y wird von x geteilt“ oder „y ist ein Vielfaches von x“.
- Für alle $n \in \mathbb{Z}$ gilt: $1 \mid n$ und $n \mid 0$.

Eigenschaften der Teilbarkeitsrelation

Für die Teilbarkeitsrelation $|$ über $\mathbb{Z}$ gilt:

1. $|$ ist reflexiv.
2. $|$ ist nicht symmetrisch.
3. $|$ ist nicht asymmetrisch.
4. $|$ ist nicht antisymmetrisch.
5. $|$ ist nicht total.
6. $|$ ist transitiv.

Diese Aussagen werden in den nächsten 6 Folien gezeigt.

Eigenschaften der Teilbarkeitsrelation

1. $\mid$ ist reflexiv.

   Zu zeigen ist:

   $$\forall a \in \mathbb{Z} : a \mid a.$$

   Beweis:

   Sei $a \in \mathbb{Z}$ eine beliebige ganze Zahl.

   $\Longrightarrow$ $a = 1 \cdot a$.

   $\Longrightarrow$ Es gibt also eine ganze Zahl $k \in \mathbb{Z}$ mit $a = k \cdot a$, nämlich $k = 1$.

   $\Longrightarrow$ $a \mid a$.

   $\square$.

Eigenschaften der Teilbarkeitsrelation

2. $\mid$ ist nicht symmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \mathbb{Z} : a \mid b \text{ und } b \nmid a.$$

   Beweis:

   Als Gegenbeispiel sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \mid b$ und $b \nmid a$ gelten, z.B. $a = 2$ und $b = 4$. $\square$

Eigenschaften der Teilbarkeitsrelation

3. $|$ ist nicht asymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \mathbb{Z} : a \mid b \text{ und } b \mid a.$$

   Beweis:

   Als Gegenbeispiel sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \mid b$ und $b \mid a$ gelten, z.B. $a = 4$ und $b = 4$. □

Eigenschaften der Teilbarkeitsrelation

4. $\mid$ ist nicht antisymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \mathbb{Z} : a \mid b,\ b \mid a \text{ und } a \neq b.$$

   Beweis:

   Als Gegenbeispiel sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \mid b$, $b \mid a$ und $a \neq b$ gelten, z.B. $a = 3$ und $b = -3$. □

   Info: Die Einschränkung der Teilbarkeitsrelation auf $\mathbb{N}_0$ ist schon antisymmetrisch!

Eigenschaften der Teilbarkeitsrelation

5. $|$ ist nicht total.

   Zu zeigen ist:

   $$\exists a, b \in \mathbb{Z} : a \nmid b \text{ und } b \nmid a.$$

   Beweis:

   Als Gegenbeispiel sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \nmid b$ und $b \nmid a$ gelten, z.B. $a = 3$ und $b = 4$. □

Eigenschaften der Teilbarkeitsrelation

6. $\mid$ ist transitiv.

   Zu zeigen ist:

$$\forall a, b, c \in \mathbb{Z} : (a \mid b \text{ und } b \mid c) \implies a \mid c.$$

   Beweis:

   Seien $a, b, c \in \mathbb{Z}$ beliebige ganze Zahlen mit $a \mid b$ und $b \mid c$.

   $\implies$ Es gibt ganze Zahlen $k_1, k_2 \in \mathbb{Z}$ mit $b = k_1 \cdot a$ und $c = k_2 \cdot b$.

   $\implies$ Durch Einsetzen von $b = k_1 a$ in $c = k_2 b$ erhalten wir:

$$c = k_2 \cdot k_1 \cdot a.$$

   $\implies$ Es gibt also eine ganze Zahl $k_3 \in \mathbb{Z}$ mit $c = k_3 a$, nämlich $k_3 = k_2 \cdot k_1$.

   $\implies$ $a \mid c$

□

Induktionsbeweise von Teilbarkeitsaussagen

Frage: Gegeben sei eine Zahl $x \in \mathbb{Z}$ und eine Funktion $f : \mathbb{N}_0 \to \mathbb{Z}$. Wie beweist man eine Aussage $A(n)$ der Form „$f(n)$ ist für alle $n \in \mathbb{N}_0$ durch x teilbar“?

Methode: Für beliebige $x, y \in \mathbb{Z}$ gilt:

$$x \mid y \quad :\Longleftrightarrow \quad \exists k \in \mathbb{Z} : y = k \cdot x$$

(s. Folie 397).

I.A. 0 für n einsetzen und die Aussage $x \mid f(0)$ überprüfen.

I.V. „Angenommen, es gilt $x \mid f(n)$ für ein beliebiges, aber festes $n \geq 0$, d.h. es gibt ein $k \in \mathbb{Z}$ mit $f(n) = k \cdot x$.“

I.S. Den Ausdruck $f(n+1)$ auf $f(n)$ zurückführen und die I.V. auf $f(n)$ anwenden.

Beispiel

Satz:

Für alle $n \in \mathbb{N}_0$ gilt: $3 \mid n^3 + 2n$.

Beispiel

Beweis:

I.A. Für $n = 0$: Es gilt $0^3 + 2 \cdot 0 = 0$ und $3 \mid 0$. ✓

I.V. Angenommen, es gibt für ein beliebiges aber festes $n \in \mathbb{N}_0$ ein $k \in \mathbb{Z}$ mit $n^3 + 2n = k \cdot 3$.

I.S.

$$\begin{aligned}(n+1)^3 + 2(n+1) &= n^3 + 3n^2 + 3n + 1 + 2n + 2 \\ &= n^3 + 2n + (n^2 + n + 1) \cdot 3 \\ &\overset{\text{I.V.}}{=} k \cdot 3 + (n^2 + n + 1) \cdot 3 \\ &= (k + n^2 + n + 1) \cdot 3\end{aligned}$$

Es gibt also ein $k' \in \mathbb{Z}$ mit $(n+1)^3 + 2(n+1) = k' \cdot 3$, nämlich $k' = k + n^2 + n + 1$. □

Noch ein Beispiel

Satz:

Für alle $n \in \mathbb{N}_0$ gilt: $5 \mid (-2)^n + 4 \cdot 3^n$.

Noch ein Beispiel

Beweis:

I.A. Für $n = 0$: Es gilt $(-2)^0 + 4 \cdot 3^0 = 1 + 4 \cdot 1 = 5$ und $5 \mid 5$. ✓

I.V. Angenommen, es gibt für ein beliebiges aber festes $n \in \mathbb{N}_0$ ein $k \in \mathbb{Z}$ mit $(-2)^n + 4 \cdot 3^n = k \cdot 5$.

I.S.

$$\begin{aligned}
(-2)^{n+1} + 4 \cdot 3^{n+1} &= -2 \cdot (-2)^n + 3 \cdot 4 \cdot 3^n \\
&= (-5 + 3) \cdot (-2)^n + 3 \cdot 4 \cdot 3^n \\
&= -5 \cdot (-2)^n + 3 \cdot (-2)^n + 3 \cdot 4 \cdot 3^n \\
&= -5 \cdot (-2)^n + 3 \cdot ((-2)^n + 4 \cdot 3^n) \\
&\overset{\text{I.V.}}{=} -5 \cdot (-2)^n + 3 \cdot k \cdot 5 \\
&= (-1 \cdot (-2)^n + 3 \cdot k) \cdot 5
\end{aligned}$$

Es gibt also ein $k' \in \mathbb{Z}$ mit $(-2)^{n+1} + 4 \cdot 3^{n+1} = k' \cdot 5$, nämlich $k' = -1 \cdot (-2)^n + 3 \cdot k$. □

Letztes Beispiel

Satz:

Für alle $n \in \mathbb{N}_0$ *gilt:* $19 \mid 5 \cdot 2^{3n+1} + 3^{3n+2}$.

Letztes Beispiel

Beweis:

I.A. Für $n = 0$: Es gilt $5 \cdot 2^{3 \cdot 0+1} + 3^{3 \cdot 0+2} = 5 \cdot 2 + 3^2 = 19$ und $19 \mid 19$. ✓

I.V. Angenommen, es gibt für ein beliebiges aber festes $n \in \mathbb{N}_0$ ein $k \in \mathbb{Z}$ mit
I.S. $5 \cdot 2^{3n+1} + 3^{3n+2} = k \cdot 19$.

$$\begin{aligned}
5 \cdot 2^{3(n+1)+1} + 3^{3(n+1)+2} &= 8 \cdot 5 \cdot 2^{3n+1} + 27 \cdot 3^{3n+2} \\
&= (-19 + 27) \cdot 5 \cdot 2^{3n+1} + 27 \cdot 3^{3n+2} \\
&= -19 \cdot 5 \cdot 2^{3n+1} + 27 \cdot 5 \cdot 2^{3n+1} + 27 \cdot 3^{3n+2} \\
&= -19 \cdot 5 \cdot 2^{3n+1} + 27 \cdot (5 \cdot 2^{3n+1} + 3^{3n+2}) \\
&\overset{\text{I.V}}{=} -19 \cdot 5 \cdot 2^{3n+1} + 27 \cdot k \cdot 19 \\
&= (-5 \cdot 2^{3n+1} + 27 \cdot k) \cdot 19
\end{aligned}$$

Es gibt also ein $k' \in \mathbb{Z}$ mit $5 \cdot 2^{3(n+1)+1} + 3^{3(n+1)+2} = k' \cdot 19$, nämlich $k' = -5 \cdot 2^{3n+1} + 27 \cdot k$. □

Wie kann man mit vollständiger Induktion zeigen, dass $5^n - 2^n$ für alle $n \in \mathbb{N}_0$ durch 3 teilbar ist?

Beweis:

I.A. Für $n = 0$: Es gilt $5^0 - 2^0 = 1 - 1 = 0$ und $3 \mid 0$. ✓

I.V. Angenommen, es gibt für ein beliebiges aber festes $n \in \mathbb{N}_0$ ein $k \in \mathbb{Z}$ mit $5^n - 2^n = k \cdot 3$.

I.S.

$$\begin{aligned} 5^{n+1} - 2^{n+1} &= 5 \cdot 5^n - 2 \cdot 2^n \\ &= (3+2) \cdot 5^n - 2 \cdot 2^n \\ &= 3 \cdot 5^n + 2 \cdot 5^n - 2 \cdot 2^n \\ &= 3 \cdot 5^n + 2 \cdot (5^n - 2^n) \\ &\overset{\text{I.V.}}{=} 3 \cdot 5^n + 2 \cdot k \cdot 3 \\ &= (5^n + 2 \cdot k) \cdot 3 \end{aligned}$$

Es gibt also ein $k' \in \mathbb{Z}$ mit $5^{n+1} - 2^{n+1} = k' \cdot 3$, nämlich $5^n + 2 \cdot k$. □

Kongruenzrelation $\equiv_n$ modulo n

Sei $n \in \mathbb{N}$. Für beliebige ganze Zahlen $x, y \in \mathbb{Z}$ gilt $x \equiv_n y$ genau dann, wenn es eine ganze Zahl $k \in \mathbb{Z}$ gibt mit $x = y + kn$. In kompakter Schreibweise heißt das:

$$x \equiv_n y \quad :\Longleftrightarrow \quad \exists k \in \mathbb{Z} : x = y + kn \ .$$

Somit ist $\equiv_n$ ebenfalls eine homogene Relation über $\mathbb{Z}$.

Beispiele

Für $n = 5$ gilt beispielsweise $3 \equiv_5 8$, $6 \equiv_5 -9$ und $-2 \equiv_5 -17$, aber $-3 \not\equiv_5 6$, $13 \not\equiv_5 6$ und $8 \not\equiv_5 -10$.

Infos

- Für $x \equiv_n y$ sagen wir „x und y sind kongruent modulo n“.
- Es gilt $x \equiv_n y$ genau dann, wenn die Differenz $x - y$ durch n teilbar ist:

$$x \equiv_n y \iff \exists k \in \mathbb{Z} : x = y + k \cdot n \iff \exists k \in \mathbb{Z} : x - y = k \cdot n \iff n \mid (x - y)$$

Eigenschaften der Kongruenzrelation modulo n

Für die Kongruenzrelation $\equiv_n$ modulo n gilt:

1. $\equiv_n$ ist reflexiv.
2. $\equiv_n$ ist symmetrisch.
3. $\equiv_n$ ist nicht asymmetrisch.
4. $\equiv_n$ ist nicht antisymmetrisch.
5. $\equiv_n$ ist nicht total.
6. $\equiv_n$ ist transitiv.

Diese Aussagen werden in den nächsten 6 Folien gezeigt.

Eigenschaften der Kongruenzrelation modulo n

1. $\equiv_n$ ist reflexiv.

   Zu zeigen ist:

   $$\forall a \in \mathbb{Z} : a \equiv_n a.$$

   Beweis:

   Sei $a \in \mathbb{Z}$ eine beliebige ganze Zahl.

   $\Longrightarrow$ $a = a + 0 \cdot n$.

   $\Longrightarrow$ Es gibt also eine ganze Zahl $k \in \mathbb{Z}$ mit $a = a + k \cdot n$, nämlich $k = 0$.

   $\Longrightarrow$ $a \equiv_n a$.

   $\square$.

Eigenschaften der Kongruenzrelation modulo n

2. $\equiv_n$ ist symmetrisch.

   Zu zeigen ist:

$$\forall a, b \in \mathbb{Z} : a \equiv_n b \implies b \equiv_n a.$$

   Beweis:

   Seien $a, b \in \mathbb{Z}$ beliebige ganze Zahlen mit $a \equiv_n b$.

$\implies$ Es gibt ein $k_1 \in \mathbb{Z}$ mit $a = b + k_1 \cdot n$.

$\implies$ $a - k_1 \cdot n = b$.

$\implies$ Es gibt also ein $k_2 \in \mathbb{Z}$ mit $b = a + k_2 \cdot n$, nämlich $k_2 = -k_1$.

$\implies$ $b \equiv_n a$.

$\square$.

Eigenschaften der Kongruenzrelation modulo n

3. $\equiv_n$ ist nicht asymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \mathbb{Z} : a \equiv_n b \text{ und } b \equiv_n a.$$

   Beweis:

   Als Gegenbeispiel sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \equiv_n b$ und $b \equiv_n a$ gelten, z.B. $n = 5$, $a = 1$ und $b = 6$. □

Eigenschaften der Kongruenzrelation modulo n

4. $\equiv_n$ ist nicht antisymmetrisch.

   Zu zeigen ist:

   $$\exists a, b \in \mathbb{Z} : a \equiv_n b, b \equiv_n a \text{ und } a \neq b.$$

   Beweis:

   Als Gegenbeispiel sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \equiv_n b$, $b \equiv_n a$ und $a \neq b$ gelten, z.B. wieder $n = 5$, $a = 1$ und $b = 6$. □

Eigenschaften der Kongruenzrelation modulo n

5. $\equiv_n$ ist nicht total.

   Zu zeigen ist:

   $$\exists a, b \in \mathbb{Z} : a \not\equiv_n b \text{ und } b \not\equiv_n a.$$

   Beweis:

   Als Gegenbeispiel sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ gesucht, für die $a \not\equiv_n b$ und $b \not\equiv_n a$ gelten, z.B. $n = 5$, $a = 2$ und $b = 3$. □

Eigenschaften der Kongruenzrelation modulo n

6. $\equiv_n$ ist transitiv.

   Zu zeigen ist:

$$\forall a, b, c \in \mathbb{Z} : (a \equiv_n b \text{ und } b \equiv_n c) \implies a \equiv_n c.$$

   Beweis:

   Seien $a, b, c \in \mathbb{Z}$ beliebige ganze Zahlen mit $a \equiv_n b$ und $b \equiv_n c$.

   $\implies$ Es gibt ganze Zahlen $k_1, k_2 \in \mathbb{Z}$ mit $a = b + k_1 \cdot n$ und $b = c + k_2 \cdot n$.

   $\implies$ Durch Einsetzen von $b = c + k_2 \cdot n$ in $a = b + k_1 \cdot n$ erhalten wir:

$$a = c + k_2 \cdot n + k_1 \cdot n = c + (k_2 + k_1) \cdot n.$$

   $\implies$ Es gibt also eine ganze Zahl $k_3 \in \mathbb{Z}$ mit $a = c + k_3 \cdot n$, nämlich $k_3 = k_2 + k_1$.

   $\implies$ $a \equiv_n c$

□

Die Modulo-Operation

Modulo kann auch als Operation mod : $\mathbb{Z} \times \mathbb{N} \to \mathbb{N}_0$. aufgefasst werden. Für beliebige $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt:

$$a \bmod n := a - \left\lfloor \frac{a}{n} \right\rfloor \cdot n.$$

Info

$\lfloor x \rfloor := \max \{m \in \mathbb{Z}\}\, m \leq x$ rundet den Wert von x ab.

Die Modulo-Operation (Äquivalente Definition)

Die Modulo-Operation wird auch wie folgt definiert werden. Für beliebige $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt:

$$a \bmod n = r \quad :\Longleftrightarrow \quad a \equiv_n r \text{ und } 0 \leq r < n \ .$$

Diese Definition ist äquivalent zur ersten.

Erinnerung

Aus Folie 416 wissen wir:

$$a \bmod n = r \quad \Longleftrightarrow \quad \exists k \in \mathbb{Z} : a = kn + r \quad \Longleftrightarrow \quad (a - r) \mid n$$

Beispiele

- Sind die Zahlen groß und man hat Lust zu dividieren, dann benutzt man am besten die Formel:

$$437 \bmod 7 = 437 - \left\lfloor \frac{437}{7} \right\rfloor \cdot 7 = 437 - 62 \cdot 7 = 3$$

$$-245 \bmod 9 = -245 - \left\lfloor \frac{-245}{9} \right\rfloor \cdot 9 = -245 - (-28) \cdot 9 = 7$$

- Sonst benutzt man am besten die Kongruenz modulo n:

$$29 \equiv_5 24 \equiv_5 19 \equiv_5 14 \equiv_5 9 \equiv_5 4 \quad \rightsquigarrow \quad 29 \bmod 5 = 4$$

$$-13 \equiv_3 -10 \equiv_3 -7 \equiv_3 -4 \equiv_3 -1 \equiv_3 2 \quad \rightsquigarrow \quad -13 \bmod 3 = 2$$

Quizfragen

1. Was ist 35 mod 6?
2. Was ist 3 mod 7?
3. Was ist (-5) mod 11?
4. Was ist (-17) mod 6?
5. Was ist 38 mod 2?
6. Was ist 75 mod 9?
7. Was ist (-36) mod 9?
8. Was ist 5 mod 1?
9. Was ist $(n^2 - 1)$ mod $(n + 1)$ für ein beliebiges $n \in \mathbb{N}$?
10. Was ist n^2 mod $(n + 1)$ für ein beliebiges $n \in \mathbb{N}$?

Antworten

1. $35 \bmod 6 = 5$.
2. $3 \bmod 7 = 3$.
3. $-5 \bmod 11 = 6$.
4. $-17 \bmod 6 = 1$.
5. $38 \bmod 2 = 0$.
6. $75 \bmod 9 = 3$.
7. $-36 \bmod 9 = 0$.
8. $5 \bmod 1 = 0$.
9. $n^2 - 1 \bmod (n+1) = (n+1)(n-1) \bmod (n+1) = 0$.
10. $n^2 \bmod (n+1) = ((n+1)^2 - 2(n+1) + 1) \bmod (n+1) = 1$.

Rechenregeln für Modulo

Für beliebige $a, b, c, d \in \mathbb{Z}$ und $m, n \in \mathbb{N}$ gilt:

1. $a \equiv_n b \wedge c \equiv_n d \implies a + c \equiv_n b + d$,
2. $a \equiv_n b \wedge c \equiv_n d \implies a \cdot c \equiv_n b \cdot d$,
3. $an \bmod n = 0$,
4. $a \equiv_n a \bmod n$,
5. $(a \bmod n) \bmod n = a \bmod n$,
6. $a \equiv_n b \iff a \bmod n = b \bmod n$,
7. $ma \bmod mn = m \cdot (a \bmod n)$,
8. $(a + b) \bmod n = (a + (b \bmod n)) \bmod n$,
9. $(a \cdot b) \bmod n = (a \cdot (b \bmod n)) \bmod n$.

Außerdem ist $\equiv_n$ für alle $n \in \mathbb{N}$ reflexiv, symmetrisch und transitiv, d.h. eine Äquivalenzrelation.

1. Was ist 2^{168} mod 3?
2. Was ist 2^{201} mod 3?
3. Was ist 100^{99} mod 9?
4. Was ist 2^{3600} mod 31?
5. Was ist $(10^{85} + 5^{63} + 12^{47})$ mod 3?
6. Gilt $a \equiv_n an$ für alle $a \in \mathbb{Z}, n \in \mathbb{N}$?
7. Für welche $n \in \mathbb{N}$ gilt $2a \equiv_n a$ für alle $a \in \mathbb{Z}$?

Taschenrechner sind verboten! Für die letzten zwei Fragen könnte Folie 416 helfen.

1. $2^{168} \bmod 3 = (2^2)^{84} \bmod 3 = 4^{84} \bmod 3 = 1^{84} \bmod 3 = 1$.
2. $2^{201} \bmod 3 = ((2^2)^{100} \cdot 2) \bmod 3 = (1 \cdot 2) \bmod 3 = 2$.
3. $100^{99} \bmod 9 = 1^{99} \bmod 9 = 1$.
4. $2^{500} \bmod 31 = (2^5)^{100} \bmod 31 = 32^{100} \bmod 31 = 1^{100} \bmod 31 = 1$.
5. $(10^{85} + 5^{63} + 12^{47}) \bmod 3 = (10^{85} + (5^2)^{31} \cdot 5 + 12^{47}) \bmod 3 =$
   $(10^{85} + 25^{31} \cdot 5 + 12^{47}) \bmod 3 = (1^{85} + 1^{31} \cdot 5 + 0^{47}) \bmod 3 = (1 + 5 + 0) \bmod 3 = 0$.
6. Nein! Beispielsweise gilt $1 \not\equiv_2 1 \cdot 2$.
7. Es gilt: $2a \equiv_n a \iff n \mid 2a - a \iff n \mid a$. D.h. n muss ein Teiler von a sein.

Die Ganzzahlige Division

$a \div n$ ist das ganzzahlige Ergebnis der Division von $a \in \mathbb{Z}$ durch $n \in \mathbb{N}$. Es gilt:

$$a \div n := \frac{a - (a \bmod n)}{n} = \left\lfloor \frac{a}{n} \right\rfloor .$$

Beispiele

Es gilt:

$$12 \div 5 = \frac{12 - (12 \bmod 5)}{5} = \frac{12 - 2}{5} = \frac{10}{5} = 2$$
$$-11 \div 3 = \frac{-11 - (-11 \bmod 3)}{3} = \frac{-11 - 1}{3} = \frac{-12}{3} = -4$$

bzw.

$$12 \div 5 = \left\lfloor \frac{12}{5} \right\rfloor = \lfloor 2,4 \rfloor = 2$$
$$-11 \div 3 = \left\lfloor \frac{-11}{3} \right\rfloor = \lfloor -3,666\ldots \rfloor = -4$$

Quizfragen

1. Was ist $7 \div 3$?
2. Was ist $23 \div 6$?
3. Was ist $38 \div 7$?
4. Was ist $-15 \div 4$?
5. Was ist $-8 \div 5$?
6. Was ist $-10 \div 4$?
7. Was ist $-n \div 1$ für ein beliebiges $n \in \mathbb{N}$?
8. Was ist $-2n \div 2$ für ein beliebiges $n \in \mathbb{N}$?

1. $7 \div 3 = \frac{7-(7 \bmod 3)}{3} = 2.$
2. $23 \div 6 = \frac{23-(23 \bmod 6)}{6} = 3.$
3. $38 \div 7 = \frac{38-(38 \bmod 7)}{7} = 5.$
4. $-15 \div 4 = \frac{-15-(-15 \bmod 4)}{4} = -4.$
5. $-8 \div 5 = \frac{-8-(-8 \bmod 5)}{5} = -2.$
6. $-10 \div 4 = \frac{-10-(-10 \bmod 4)}{4} = -3.$
7. $-n^2 \div 1 = \frac{-n^2-(-n^2 \bmod 1)}{1} = \frac{-n^2-0}{1} = -n.$
8. $-2n \div 2 = \frac{-2n-(-2n \bmod 2)}{2} = \frac{-2n-0}{2} = -n.$

ggT und kgV

Seien $m, n \in \mathbb{N}_0$. Der größte gemeinsame Teiler $\mathrm{ggT}(m, n)$ von m und n ist die größte natürliche Zahl, die sowohl m als auch n teilt. Das kleinste gemeinsame Vielfache $\mathrm{kgV}(m, n)$ von m und n ist die kleinste natürliche Zahl, die sowohl von m als auch von n geteilt wird.

Infos

- Wie die Teilbarkeitsrelation funktioniert kann auf Folie 397 nachgelesen werden.
- Es gilt:
$$\mathrm{kgV}(m,n) = \frac{m \cdot n}{\mathrm{ggT}(m,n)}.$$
- Falls $\mathrm{ggT}(m,n) = 1$ bzw. $\mathrm{kgV}(m,n) = m \cdot n$ gilt, dann sagt man, dass m und n teilerfremd oder koprim zueinander sind.

Beispiele

1. Für $m = 14$ und $n = 15$ gilt:

   $2 \cdot 7$ $3 \cdot 5$

   $\mathrm{ggT}(14, 15) = 1 \quad \text{und} \quad \mathrm{kgV}(14, 15) = 210.$

   $2^2 \cdot 3 \cdot 5$ $2 \cdot 3 \cdot 5 \cdot 7$

2. Für $m = 24$ und $n = 60$ gilt:

   $2^3 \cdot 3$

   $\mathrm{ggT}(24, 60) = 12 \quad \text{und} \quad \mathrm{kgV}(24, 60) = 120.$

   $2^2 \cdot 3$ $2^3 \cdot 3 \cdot 5$

3. Für $m \in \{0, 1\}$ und $n \in \mathbb{N}_0$ beliebig gilt:

   $$\mathrm{ggT}(0, n) = n, \quad \mathrm{kgV}(0, n) = 0, \quad \mathrm{ggT}(1, n) = 1 \quad \text{und} \quad \mathrm{kgV}(1, n) = n.$$

Euklidischer Algorithmus

Für zwei beliebige natürliche Zahlen $m, n \in \mathbb{N}_0$ mit $m \leq n$ berechnet der euklidische Algorithmus den größten gemeinsamen Teiler $\mathrm{ggT}(m, n)$ aus n und m. Dazu setzt er $r_0 = n$ und $r_1 = m$ und füllt systematisch mit den Formeln

$$r_{i-1} \bmod r_i = r_{i+1} \quad \text{und} \quad r_{i-1} \div r_i = s_i$$

folgende Tabelle von oben nach unten aus

r_i	s_i
n	–
m	s_1
r_2	s_2
r_3	s_3
⋮	⋮
r_{k-1}	s_{k-1}
0	–

Euklidischer Algorithmus

bis $r_k = 0$ ist. Dann gilt: $\mathrm{ggT}(m, n) = r_{k-1}$

Beispiel

Wir bestimmten $\mathrm{ggT}(21, 100)$ mit dem euklidischen Algorithmus.

r_i	s_i
100	–
21	4
16	1
5	3
1	5
0	–

Es gilt: $\mathrm{ggT}(21, 100) = 1$.

Noch ein Beispiel

Wir bestimmten $\mathrm{ggT}(28, 74)$ mit dem euklidischen Algorithmus.

r_i	s_i
74	–
28	2
18	1
10	1
8	1
2	4
0	–

Es gilt: $\mathrm{ggT}(28, 74) = 2$.

1. Was ist $\mathrm{ggT}(28, 76)$?
2. Was ist $\mathrm{ggT}(96, 129)$?
3. Was ist $\mathrm{ggT}(46, 53)$?
4. Was ist $\mathrm{ggT}(41, 94)$?

Hinweis: Benutze den euklidischen Algorithmus!

Antworten ohne Rechnungen:

1. $\mathrm{ggT}(28, 76) = 4$.
2. $\mathrm{ggT}(96, 129) = 3$.
3. $\mathrm{ggT}(46, 53) = 1$.
4. $\mathrm{ggT}(41, 94) = 1$.

Themenübersicht

Lemma von Bézout

Für zwei beliebige natürliche Zahlen $m, n \in \mathbb{N}_0$ existieren ganze Zahlen $a, b \in \mathbb{Z}$ mit:

$$a \cdot m + b \cdot n = \mathrm{ggT}(m, n).$$

Sei o.B.d.A. $m \leq n$. Um a und b zu bestimmen wird der euklidische Algorithmus ausgeführt und die Tabelle um eine Spalte t_i erweitert. Diese wird dann von unten nach oben mit den Formeln

$$t_{k-1} = 0 \quad t_{k-2} = 1 \quad \text{und} \quad t_{i-1} = t_{i+1} - t_i \cdot s_i$$

ausgefüllt. Dieser Algorithmus wird erweiterte euklidische Algorithmus genannt. Nach der Ausführung gilt $a = t_0$ und $b = t_1$.

Infos

- Die Tabelle des erweiterten euklidischen Algorithmus hat dann immer folgende Gestalt:

	r_i	s_i	t_i	
$n \longrightarrow$	r_0	—	t_0	$\longleftarrow a$
$m \longrightarrow$	r_1	s_1	t_1	$\longleftarrow b$
	⋮	⋮	⋮	
	r_{k-2}	s_{k-2}	1	
$\mathrm{ggT}(m,n) \rightarrow$	r_{k-1}	s_{k-1}	0	
	0	—	—	

- Es gibt immer unendlich viele Möglichkeiten a und b für das Lemma von Bézout zu wählen. Der erweiterte euklidische Algorithmus liefert nur eine davon.
- Wir könnten die Definition von $\mathrm{ggT}(m,n)$ und das Lemma von Bézout auf ganze Zahlen $m, n \in \mathbb{Z}$ verallgemeinern, aber das ist für uns nicht wichtig.

Beispiel

Für $n = 100$ und $m = 21$ erhalten wir

r_i	s_i	t_i
100	–	-19
21	4	4
16	1	-3
5	3	1
1	5	0
0	–	–

Es folgt $\mathrm{ggT}(100, 21) = 1$ und

$$(-19) \cdot 21 + 4 \cdot 100 = 1.$$

Beispiel

Für $n = 100$ und $m = 21$ erhalten wir

r_i	s_i	t_i
100	–	-19
21	4	4
16	1	-3
5	3	1
1	5	0
0	–	–

Es folgt $\mathrm{ggT}(100, 21) = 1$ und

$$(\text{-19}) \cdot 21 + 4 \cdot 100 = 1.$$

Info

Am besten merkt man sich die Formeln intuitiv.

- Für die linke Spalte gilt:

„ oben durch mitte gleich rechts , Rest unten .“

- Für die rechte Spalte gilt:

„ unten minus $\left(\text{mitte mal links}\right)$ gleich oben .“

$$\begin{vmatrix} \vdots & \vdots & \vdots \\ r_{i-1} & s_{i-1} & t_{i-1} \\ r_i & s_i & t_i \\ r_{i+1} & s_{i+1} & t_{i+1} \\ \vdots & \vdots & \vdots \end{vmatrix} \qquad \begin{vmatrix} \vdots & \vdots & \vdots \\ r_{i-1} & s_{i-1} & t_{i-1} \\ r_i & s_i & t_i \\ r_{i+1} & s_{i+1} & t_{i+1} \\ \vdots & \vdots & \vdots \end{vmatrix}$$

Noch ein Beispiel

Für $n = 74$ und $m = 28$ gilt:

r_i	s_i	t_i
74	–	8
28	2	−3
18	1	2
10	1	−1
8	1	1
2	4	0
0	–	–

Es folgt $\mathrm{ggT}(28, 74) = 2$ und

$$8 \cdot 28 + (-3) \cdot 74 = 2 .$$

Quizfrage

Für welche $a, b \in \mathbb{Z}$ gilt die gegebene Gleichung?

1. $a \cdot 33 + b \cdot 51 = 3$.
2. $a \cdot 53 + b \cdot 89 = 1$.
3. $a \cdot 38 + b \cdot 62 = 2$.
4. $a \cdot 14 + b \cdot 45 = 1$.
5. $a \cdot 55 + b \cdot 79 = 5$. Achtung: fiese Falle!

Antwort (ohne Rechnungen)

Die Lösung auf diese Frage ist nicht eindeutig (s. Folie 451). Folgende Werte wurden mit dem erweiterten euklidischen Algorithmus berechnet.

1. $a = -3$, $b = 2$.
2. $a = 42$, $b = -25$.
3. $a = -13$, $b = 8$.
4. $a = -16$, $b = 5$.
5. $a = 115$, $b = -80$.

Info zu 5.: Hier liefert der erweiterte euklidische Algorithmus die Gleichung $23 \cdot 55 + (-16) \cdot 79 = 1$. Multipliziert man beide Seiten mit 5, so erhält man die neue Gleichung $115 \cdot 55 + (-80) \cdot 79 = 5$.

Themenübersicht

Definition

Seien A und B zwei beliebige Mengen. Eine Abbildung oder Funktion $f : A \to B$ ist eine Zuordnung zwischen A und B, so dass jedem Element $a \in A$ genau ein Element $b \in B$ zugeordnet wird. Wir schreiben dann $f(a) = b$.

Infos

- Formal ist eine Funktion nichts anderes als eine linkstotale und rechtseindeutige Relation $f \subseteq A \times B$.
- B^A ist die Menge aller Funktionen von A nach B.
- $f : A \to B$ steht für $f \in B^A$.
- Wenn keine Verwechslungsgefahr besteht, kann man die Klammern weglassen und $f\,a$ statt $f(a)$ schreiben, z.B. in $\sin x$ und $\ln x$. Wenn das Argument a ein Tupel (x, y) ist, schreibt man beispielsweise auch oft $f(x, y)$ statt $f((x, y))$, um Klammer-Salate zu vermeiden.

Schreibweisen

1. Als Relation:

$$f \subseteq A \times B \text{ mit } f = \{(a_1, f(a_1)), (a_2, f(a_2)), (a_3, f(a_3)), \ldots\}$$

2. Als Zuordnungsvorschrift:

$$f : A \to B,\ a_1 \mapsto f(a_1),\ a_2 \mapsto f(a_2),\ a_3 \mapsto f(a_3), \ldots$$

3. Als Tabelle:

x	a_1	a_2	a_3	$\ldots$
$f(x)$	$f(a_1)$	$f(a_2)$	$f(a_3)$	$\ldots$

Wichtig!

Es ist wichtig, die Vorstellung zu verwerfen, vor allem wenn man erst kürzlich mit der Schule fertig geworden ist, dass Funktionen nur für reelle Zahlen definiert sind und mathematische Ausdrücke wie z.B. $f(x) = x^2$, $f(x) = \sin(x)$ oder $f(x) = e^x$ beinhalten müssen. Auch einfache - vor allem endliche - Funktionen spielen eine wichtige Rolle.

Ein Beispiel für eine solche Funktion wäre $f : [3] \to [2]$ mit $1 \mapsto 2$, $2 \mapsto 2$ und $3 \mapsto 1$.

Graphische Darstellung endlicher von Funktionen

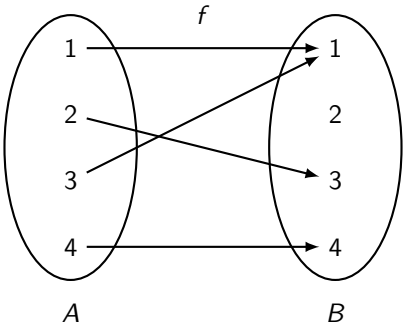
Die graphische Darstellung endlicher Funktionen funktioniert analog zu der von Relationen. Wichtig ist, dass bei einer Funktion $f : A \to B$ jedes Element aus A von genau einem Pfeil verlassen wird!

Beispiel

Die Funktion $f : [4] \to [4]$ mit

$$1 \mapsto 1, \quad 2 \mapsto 3, \quad 3 \mapsto 1, \quad 4 \mapsto 4$$

kann graphisch wie folgt dargestellt werden:



Quizfrage

Wie viele verschiedene Funktionen $f : [4] \to [3]$ gibt es?

Für jedes der 4 Elemente in [4] gibt es 3 Abbildungsmöglichkeiten in [3]. D.h. für jedes

$$(x_1, x_2, x_3, x_4) \in [3]^4$$

ist

$$1 \mapsto x_1, \quad 2 \mapsto x_2, \quad 3 \mapsto x_3, \quad 4 \mapsto x_4$$

eine mögliche Funktion. Es gibt also $|[3]^4| = 3^4 = 81$ verschiedene Funktionen.

Info

Für die Menge B^A aller Funktionen $f : A \to B$ gilt im Allgemeinen:

$$\left|B^A\right| = |B|^{|A|}.$$

Daher kommt auch die seltsame Notation B^A.

Bild und Urbild einer Funktion

Sei $f : A \to B$ eine Funktion.

- $f(a)$ ist das Bild des Elements $a \in A$
- Das Urbild $f^{-1}(b)$ eines Elements $b \in B$ ist definiert als:

$$f^{-1}(b) = \{a \in A\} f(a) = b.$$

- Das Bild $f(A')$ einer Menge $A' \subseteq A$ ist:

$$f(A') = \bigcup_{a \in A'} \{f(a)\}.$$

- Das Urbild $f^{-1}(B')$ einer Menge $B' \subseteq B$ ist:

$$f^{-1}(B') = \bigcup_{b \in B'} f^{-1}(b).$$

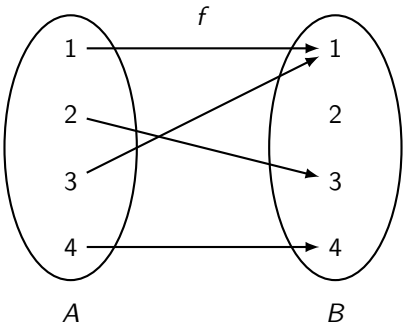
Infos

- Intuitiv wendet man bei $f(A')$ f auf jedes Element von A' an.
- Intuitiv wendet man bei $f^{-1}(B')$, analog zu $f(A')$, f^{-1} auf jedes Element von B' an.
- f^{-1} ist bei uns nicht die Umkehrfunktion, sondern die Urbildmenge!
- Es gilt immer:

$$x \in f^{-1}(B') \iff f(x) \in B' \ .$$

Beispiel

Sei $f : A \to B$ wieder folgende Funktion:

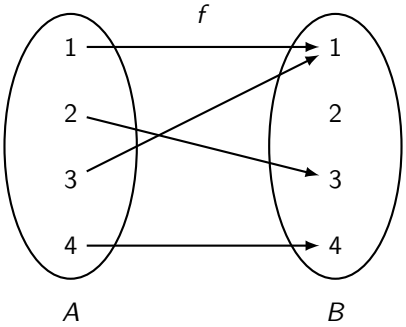


Die Bilder aller Elemente $a \in A$ sind:

$$f(1) = 1, \quad f(2) = 3, \quad f(3) = 1, \quad f(4) = 4.$$

Beispiel

Sei $f\colon A \to B$ wieder folgende Funktion:

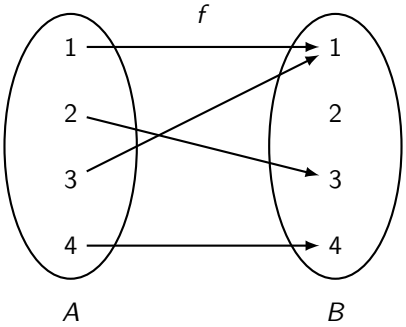


Die Urbilder aller Elemente $b \in B$ sind:

$$f^{-1}(1) = \{1, 3\}\,, \quad f^{-1}(2) = \emptyset, \quad f^{-1}(3) = \{2\}\,, \quad f^{-1}(4) = \{4\}\,.$$

Beispiel

Sei $f\colon A \to B$ wieder folgende Funktion:

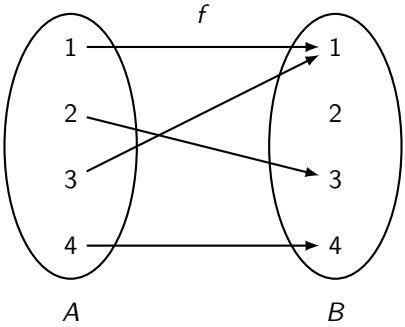


Die Bilder einiger Mengen $A' \subseteq A$ sind:

$$f(\emptyset) = \emptyset, \quad f(\{1\}) = \{1\}, \quad f(\{3,4\}) = \{1,4\}, \quad f(\{1,2,3\}) = \{1,3\}.$$

Beispiel

Sei $f\colon A \to B$ wieder folgende Funktion:



Die Urbilder einiger Mengen $B' \subseteq B$ sind:

$$f^{-1}(\emptyset) = \emptyset, \quad f^{-1}(\{1\}) = \{1,3\}, \quad f^{-1}(\{2\}) = \emptyset, \quad f^{-1}(\{1,4\}) = \{1,3,4\}.$$

Welche der folgenden Aussagen gelten für beliebige Funktionen $f : A \to B$ und alle Mengen $X \subseteq A, Y \subseteq B$?

$$|f(X)| \leq |X|, \qquad |f^{-1}(Y)| \leq |Y|,$$
$$|f(X)| = |X|, \qquad |f^{-1}(Y)| = |Y|,$$
$$|f(X)| \geq |X|, \qquad |f^{-1}(Y)| \geq |Y|.$$

Im Allgemeinen gilt nur:

$$|f(X)| \leq |X|.$$

Eigenschaften von Funktionen

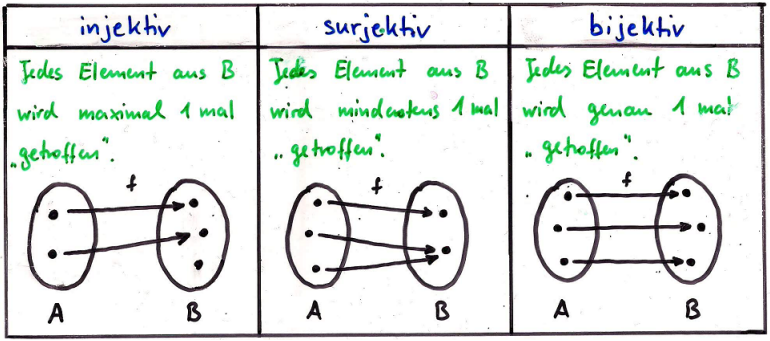
Sei $f : A \to B$. Dann gilt:

$$
\begin{aligned}
f \text{ injektiv} &\quad :\iff \quad \forall b \in B : |f^{-1}(b)| \leq 1 \\
f \text{ surjektiv} &\quad :\iff \quad \forall b \in B : |f^{-1}(b)| \geq 1 \\
f \text{ bijektiv} &\quad :\iff \quad \forall b \in B : |f^{-1}(b)| = 1
\end{aligned}
$$

Für Beweise sind folgende äquivalente Aussagen sehr nützlich:

$$
\begin{array}{lcl}
f \text{ injektiv} & \iff & (\forall a_1, a_2 \in A : f(a_1) = f(a_2) \implies a_1 = a_2) \\
f \text{ surjektiv} & \iff & \forall b \in B : \exists a \in A : f(a) = b \\
f \text{ bijektiv} & \iff & f \text{ injektiv und surjektiv}
\end{array}
$$

Graphische Bedeutung

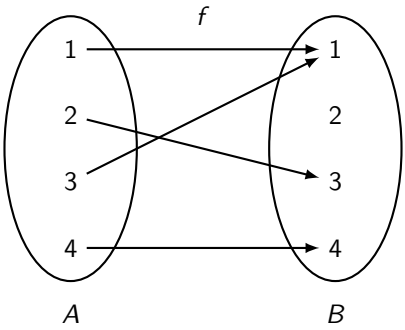


Coole Eselsbrücken:

injektiv $\rightsquigarrow$ inferior $\rightsquigarrow$ weniger $\rightsquigarrow$ 1 oder weniger
surjektiv $\rightsquigarrow$ superior $\rightsquigarrow$ mehr $\rightsquigarrow$ 1 oder mehr

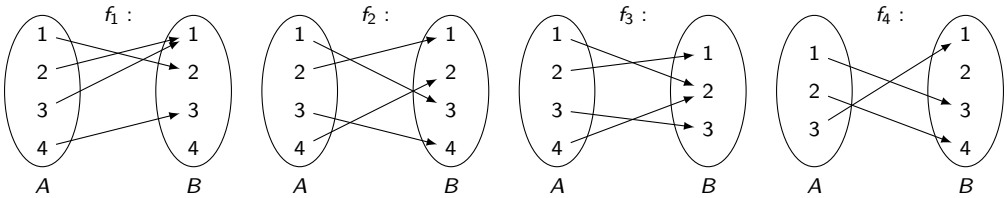
Beispiel

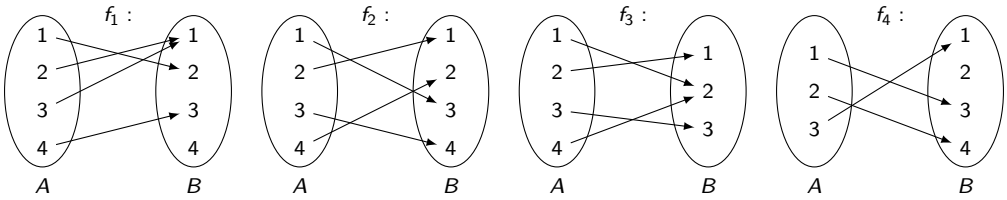
Sei $f\colon A \to B$ wieder folgende Funktion:



- f ist nicht injektiv, da $|f^{-1}(1)| = |\{1,3\}| = 2$.
- f ist nicht surjektiv, da $|f^{-1}(2)| = |\emptyset| = 0$.

Welche Eigenschaften besitzen folgende Funktionen?





- f_1 ist nicht injektiv und nicht surjektiv.
- f_2 ist injektiv und surjektiv (also bijektiv).
- f_3 ist surjektiv und nicht injektiv.
- f_4 ist injektiv und nicht surjektiv.

Welche Eigenschaften besitzen folgende Funktionen?

1. $f : \mathbb{N} \to \mathbb{N}_0$ mit $f(x) = x$,
2. $f : \mathbb{Z} \to \mathbb{N}_0$ mit $f(x) = x^2$,
3. $f : \mathbb{N}_0 \to \mathbb{N}_0$ mit $f(x) = 5$,
4. $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x - 3$,
5. $f : \mathbb{N}_0 \to \mathbb{N}_0$ mit $f(x) = 2^x$,
6. $f : \mathbb{Z} \to \mathbb{N}_0$ mit $f(x) = |x|$,
7. $f : \mathbb{N}_0 \to \mathbb{N}_0$ mit $f(x) = x + 1$,
8. $f : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ mit $f((x, y)) = x + y$,
9. $f : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ mit $f((x, y)) = x \cdot y$,
10. $f : \{0\} \to \{1\}$ mit $f(x) = e^{2\pi x}$.

1. f ist injektiv, da aus $f(a_1) = f(a_2)$ für alle $a_1, a_2 \in \mathbb{N}$ folgt: $a_1 = f(a_1) = f(a_2) = a_2$. f ist nicht surjektiv, da z.B. $|f^{-1}(0)| = 0$.
2. f ist nicht injektiv, da z.B. $|f^{-1}(1)| = 2$. f ist nicht surjektiv, da $|f^{-1}(2)| = 0$.
3. f ist nicht injektiv, da z.B. $|f^{-1}(5)| = \infty$. f ist nicht surjektiv, da z.B. $|f^{-1}(4)| = 0$.
4. f ist injektiv, da für alle $a_1, a_2 \in \mathbb{Z}$ gilt: $f(a_1) = f(a_2) \implies a_1 - 3 = a_2 - 3 \implies a_1 = a_2$. f ist surjektiv, da für jedes $b \in \mathbb{Z}$ ein $a \in \mathbb{Z}$ gibt mit $f(a) = b$, nämlich $a = b + 3$.
5. f ist injektiv, da für alle $a_1, a_2 \in \mathbb{Z}$ gilt:
   $f(a_1) = f(a_2) \implies 2^{a_1} = 2^{a_2} \implies \ln(2^{a_1}) = \ln(2^{a_2}) \implies a_1 \ln 2 = a_2 \ln 2 \implies a_1 = a_2$.
   f ist nicht surjektiv, da z.B. $|f^{-1}(0)| = 0$.

6. f ist nicht injektiv, da z.B. $|f^{-1}(1)| = 2$. f ist surjektiv, da für jedes $b \in \mathbb{N}_0$ ein a existiert mit $f(a) = |a| = b$, nämlich $a = b$ (oder $a = -b$).

7. f ist injektiv, da für alle $a_1, a_2 \in \mathbb{Z}$ gilt: $f(a_1) = f(a_2) \implies a_1 + 1 = a_2 + 1 \implies a_1 = a_2$. f ist nicht surjektiv, da z.B. $|f^{-1}(0)| = 0$.

8. f ist nicht injektiv, da z.B. $|f^{-1}(1)| = |\{(0,1),(1,0)\}| = 2$. f ist surjektiv, da es für jedes $b \in \mathbb{N}_0$ ein $(a_1, a_2) \in \mathbb{N}_0 \times \mathbb{N}_0$ gibt mit $f((a_1, a_2)) = a_1 + a_2 = b$ gibt, z.B. $(a_1, a_2) = (b, 0)$.

9. f ist nicht injektiv, da z.B. $|f^{-1}(2)| = |\{(1,2),(2,1)\}| = 2$. f ist surjektiv, da es für jedes $b \in \mathbb{N}_0$ ein $(a_1, a_2) \in \mathbb{N}_0 \times \mathbb{N}_0$ gibt mit $f((a_1, a_2)) = a_1 \cdot a_2 = b$ gibt, z.B. $(a_1, a_2) = (b, 1)$.

10. Da die Definitionsmenge von f nur die 0 enthält, die Zielmenge nur die 1 und $f(0) = e^2\pi \cdot 0 = e^0 = 1$ gilt, ist f bijektiv.

Seien A und B zwei endliche Mengen und $f : A \to B$ eine Funktion. Welche der folgenden Aussagen gelten immer?

$$
\begin{array}{lcl}
|A| \leq |B| & \Longrightarrow & f \text{ injektiv}, \\
|A| \geq |B| & \Longrightarrow & f \text{ surjektiv}, \\
|A| = |B| & \Longrightarrow & f \text{ bijektiv}, \\
f \text{ injektiv} & \Longrightarrow & |A| \leq |B|, \\
f \text{ surjektiv} & \Longrightarrow & |A| \geq |B|, \\
f \text{ bijektiv} & \Longrightarrow & |A| = |B|.
\end{array}
$$

Im Allgemeinen gelten nur:

$$\begin{array}{lcl} f \text{ injektiv} & \Longrightarrow & |A| \leq |B|, \\ f \text{ surjektiv} & \Longrightarrow & |A| \geq |B|, \\ f \text{ bijektiv} & \Longrightarrow & |A| = |B|. \end{array}$$

Quizfragen

1. Wie viele injektive Funktionen $f : [3] \to [7]$ gibt es?
2. Wie viele bijektive Funktionen $f : [5] \to [5]$ gibt es?

1. Für die 1 hat man 7 Abbildungsmöglichkeiten, für die 2 nur noch 6 und für die 3 nur noch 5. Die gesuchte Anzahl ist also
$$7 \cdot 6 \cdot 5 = 210.$$

2. Für die 1 hat man 5 Abbildungsmöglichkeiten, für die 2 nur noch 4, für die 3 nur noch 3, usw. Die gesuchte Anzahl ist also
$$5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120.$$

Umkehrfunktionen

Seien A und B beliebige Mengen und $f : A \to B$ eine Funktion.

- Ist f bijektiv, dann besitzt sie eine eindeutige Umkehrfunktion $f^{-1} : B \to A$ mit:

$$f(a) = b \iff f^{-1}(b) = a$$

  für alle $a \in A$ und alle $b \in B$.

- Gibt es eine Funktion $g : B \to A$ mit

$$\forall a \in A : g(f(a)) = a \quad \text{und} \quad \forall b \in B : f(g(b)) = b \ ,$$

  dann ist f bijektiv und g die Umkehrfunktion von f (d.h. $f^{-1} = g$).

Info

Ob mit f^{-1} eine Urbildmenge oder eine Umkehrfunktion gemeint ist, muss explizit hingeschrieben werden.

Komposition von Funktionen

Seien $f : A \to B$ und $g : B \to C$ beliebige Funktionen, dann nennt man die Funktion $g \circ f : A \to C$ mit

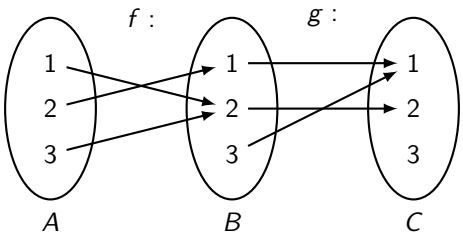
$$(g \circ f)(x) = g(f(x))$$

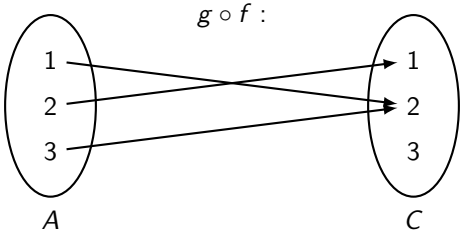
für alle $x \in A$ die Komposition oder Hintereinanderausführung von f und g.

Infos

- Wir nennen die Funktion $g \circ f$ auch „g nach f“, weil zuerst f und dann g angewendet wird.
- Eigentlich ist die Komposition von Funktionen nichts anderes als ein umgekehrtes Relationenprodukt $f \circ g$ wenn man f und g als Relationen betrachtet.

Beispiel





Welche der folgenden zwei Aussagen gilt für die Urbildmenge einer Komposition von Funktionen?

$$(g \circ f)^{-1}(y) = g^{-1}(f^{-1}(y)) \tag{1}$$

$$(g \circ f)^{-1}(y) = f^{-1}(g^{-1}(y)) \tag{2}$$

Die Aussage (2):

$$(g \circ f)^{-1}(y) = f^{-1}(g^{-1}(y))$$

Potenzen von Funktionen

Analog zu den Relationen definiert man:

$$f^n := \underbrace{f \circ f \circ \ldots \circ f}_{n \text{ mal}}$$

Beispiel

Sei $f : \mathbb{N} \to \mathbb{N},\ x \mapsto 2x^2$. Dann gilt:

$$f^3(x) = (f \circ f \circ f)(x) = f(f(f(x))) = 2(2(2x^2)^2)^2 = 128x^8$$

Also: $f^3 : \mathbb{N} \to \mathbb{N},\ x \mapsto 128x^8$

Partition der Definitionsmenge

Sei $f : A \to B$ eine Funktion. Die Relation $R \subseteq A \times A$ mit

$$R = \{(a_1, a_2) \in A \times A\} \, f(a_1) = f(a_2)$$

ist eine Äquivalenzrelation und induziert folgende Partition P der Definitionsmenge A:

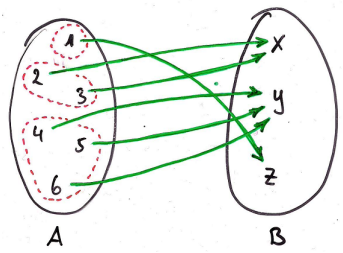
$$P = \left\{ f^{-1}(b) \right\} \, b \in B$$

Insbesondere gilt:

$$|A| = \sum_{b \in B} |f^{-1}(b)|$$

Beispiel

Sei $f : A \to B$ wie folgt:



Dann ist

$$P = \left\{ f^{-1}(x), f^{-1}(y), f^{-1}(z) \right\} = \{\{2,3\}, \{4,5,6\}, \{1\}\}$$

eine Partition von A und es gilt:

$$|A| = |f^{-1}(x)| + |f^{-1}(y)| + |f^{-1}(z)| = 2 + 3 + 1 = 6$$

Kardinalität von Mengen

Mithilfe von Funktionen können wir den Begriff der Kardinalität formalisieren. Für beliebige Mengen A und B gelten folgende Definitionen:

- A und B sind gleich mächtig ($|A| = |B|$), wenn eine bijektive Funktion $f : A \to B$ existiert.
- B ist mindestens so mächtig wie A, wenn eine injektive Funktion $f : A \to B$ existiert.
- B ist mächtiger als A, wenn eine injektive Funktion $f : A \to B$ existiert, aber keine injektive Funktion $g : B \to A$.

Aus ihnen folgt der Satz von Schröder-Bernstein:

> *Wenn A mindestens so mächtig wie B ist und B mindestens so mächtig wie A, dann sind A und B gleich mächtig.*

Abzählbarkeit von Mengen

Eine beliebige Menge A heißt abzählbar, wenn A endlich ist oder $|A| = |\mathbb{N}|$ gilt. Andernfalls ist A überabzählbar.

Info

Intuitiv ist eine Menge abzählbar, wenn ihr Elemente so durchnummeriert werden können, dass kein Element übersprungen wird.

Permutationen

Sei A eine beliebige endliche Menge. Eine bijektive Funktion $p : A \to A$ wird Permutation über A genannt.

Permutationen kann man am einfachsten als Matrix (Tabelle) darstellen. Es gilt:

$$p = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ p(a_1) & p(a_2) & p(a_3) & \dots & p(a_n) \end{pmatrix}.$$

Beispiel

Sei p eine Permutation über $[4]$ mit:

$$p(1) = 3, \quad p(2) = 1, \quad p(3) = 2, \quad p(4) = 4.$$

In Matrixschreibweise:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Noch ein Beispiel

Sei p eine Permutation über [6] mit:

$$p(1) = 5, \quad p(2) = 2, \quad p(3) = 1, \quad p(4) = 6, \quad p(5) = 3, \quad p(6) = 4.$$

In Matrixschreibweise:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$$

- die Identitätsabbildung id_A über A ist die einfachste Permutation. Es gilt:

$$\mathrm{id}_A = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$$

  Man lässt oft einfach den Index A in id_A weg.

- Weil Permutationen bijektive Abbildungen sind, besitzt jede Permutation p eine Umkehrfunktion p^{-1} mit:

$$\forall x, y \in A : p(x) = y \iff p^{-1}(y) = x$$

Gegeben seien folgende Permutationen p_1, p_2 und p_3 über $[6]$ in Matrixdarstellung:

1. $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$,
2. $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$,
3. $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}$.

Wie sehen die Umkehrfunktionen p_1^{-1}, p_2^{-1} und p_3^{-1} in Matrixdarstellung aus?

Einfach die Zeilen der Matrix vertauschen und nach der oberen Zeile sortieren!

1. $p_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$.
2. $p_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$.
3. $p_3^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$.

Was sind die Ergebnisse folgender Kompositionen in Matrixdarstellung?

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{pmatrix}$,
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$,
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 1 & 6 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 6 & 1 \end{pmatrix}$.

Antworten

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}$.
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 2 & 5 \end{pmatrix}$.
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}$.

Fixpunkte

Seien M eine Menge, $f\colon M \to M$ eine Funktion und $x \in M$ ein beliebiges Element. x ist ein Fixpunkt von f, falls $f(x) = x$ gilt. Die Menge aller Fixpunkten von f bezeichnen wir mit $\mathrm{fix}(f)$.

Beispiele

- Für $f\colon \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x^2$ gilt $\mathrm{fix}(f) = \{0, 1\}$.
- Für $g\colon \mathbb{Z} \to \mathbb{Z}$ mit $g(x) = x + 1$ gilt $\mathrm{fix}(g) = \emptyset$.
- Für $h\colon \mathbb{Z} \to \mathbb{Z}$ mit $h(x) = x$ gilt $\mathrm{fix}(h) = \mathbb{Z}$.
- Für die Permutation $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 6 & 3 & 4 & 7 \end{pmatrix}$ gilt $\mathrm{fix}(p) = \{2, 7\}$
- Für die Permutation $\mathrm{id}_{[n]} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ gilt $\mathrm{fix}(\mathrm{id}_{[n]}) = [n]$.

Themenübersicht

Themenübersicht

Syntax aussagenlogischer Formeln

Sei V eine Menge, die sog. Variablenmenge.

1. true und false sind Formeln über V.
2. Jede Variable $x \in V$ ist eine Formel über V.
3. Ist F eine Formel über V, dann auch $\neg F$.
4. Sind F und G Formeln über V, dann auch $(F \wedge G)$, $(F \vee G)$, $(F \to G)$ und $(F \leftrightarrow G)$.

Infos

- Man nennt true, false, $\neg$, $\wedge$, $\vee$, $\rightarrow$ und $\leftrightarrow$ Junktoren oder Konnektoren.
- Die Arität eines Junktors ist die Anzahl der Teilausdrücke, die er miteinander verknüpft. Junktoren mit Arität 1 nennt man monadisch oder unär. Junktoren mit Arität 2 dyadisch oder binär.
- Wir benutzen Klammern nur wenn es sein muss. Die Reihenfolge für die Bindungsstärke ist $\neg, \wedge, \vee, \rightarrow$. D.h. $\neg$ bindet am stärksten und $\rightarrow$ am schwächsten. Beispielsweise steht

$$F = \neg p \wedge q \vee r \rightarrow s \qquad \text{für} \qquad F = (((\neg p \wedge q) \vee r) \rightarrow s).$$

- Für jeden Junktor gibt es in der Literatur verschiedene Schreibweisen. Man schreibt oft 1 statt true; 0 statt false; $\overline{F}$ statt $\neg F$; FG, $F \cdot G$ oder $F \,\&\, G$ statt $F \wedge G$; $F + G$ oder $F \mid G$ statt $F \vee G$; $F \Rightarrow G$ statt $F \rightarrow G$ und $F \Leftrightarrow G$ statt $F \leftrightarrow G$.

Beispiele

Aussagenlogische Formeln sind:

$$(\neg r \to (p \wedge q)), \quad ((\neg p \leftrightarrow q) \leftrightarrow \neg r), \quad ((p \to \neg q) \vee (\neg r \wedge s)).$$

Diese dürfen wie folgt umgeschrieben werden:

$$\neg r \to p \wedge q, \quad \neg p \leftrightarrow q \leftrightarrow \neg r, \quad (p \to \neg q) \vee \neg r \wedge s.$$

Keine aussagenlogische Formeln sind:

$$p \neg q, \quad p(\neg \to) q, \quad p \to\to r, \quad \leftrightarrow q \wedge r, \quad pq \vee \neg p \neg q.$$

Quizfrage

Wie viele unterschiedliche aussagenlogische Formeln über $V = \{p\}$ gibt es?

Unendlich viele! Zum Beispiel:

$$p, \neg p, \neg\neg p, \neg\neg\neg p, \neg\neg\neg\neg p, \ldots$$

An sich ist eine aussagenlogische Formel nichts anderes als ein Wort über dem Alphabet

$$\Sigma = V \cup \{\mathsf{true}, \mathsf{false}, \neg, \wedge, \vee, \rightarrow, \leftrightarrow, (,)\}$$

und Wörter sind nur dann gleich, wenn sie auch gleich aussehen ;-)

Belegungen

- Eine Belegung $\beta\colon V \to \mathbb{B}$ ist eine Funktion die jeder Variable einer Variablenmenge V einen Wert aus $\mathbb{B} = \{0, 1\}$ zuordnet.
- Eine Belegung passt zu einer Formel F, wenn jede Variable aus F in V vorkommt, d.h. wenn $V(F) \subseteq V$ gilt.
- Eine Belegung ist minimal für F, wenn $V(F) = V$ gilt.

Infos

- Weil Belegungen Funktionen sind, bezeichnet man mit $\mathbb{B}^V$ die Menge aller Belegungen.
- Mit $V(F)$ wird hier die Menge aller Variablen in F bezeichnet.

Beispiel

Sei $V = \{p, q\}$. Dann gibt es folgende 4 Belegungen $\beta_0, \beta_1, \beta_2, \beta_3 \colon V \to \mathbb{B}$:

$$\beta_0 \colon p \mapsto 0, q \mapsto 0$$
$$\beta_1 \colon p \mapsto 0, q \mapsto 1$$
$$\beta_2 \colon p \mapsto 1, q \mapsto 0$$
$$\beta_3 \colon p \mapsto 1, q \mapsto 1$$

Sei $V = \{p, q, r, s\}$ und $\beta : V \to \mathbb{B}$ mit $p \mapsto 0, q \mapsto 1, r \mapsto 0, s \mapsto 1$. Zu welchen der folgenden Formeln $F_1, \ldots, F_5$ passt β? Für welche ist β minimal?

1. $F_1 = ((p \wedge q) \to (r \leftrightarrow s))$
2. $F_2 = (p \leftrightarrow q)$
3. $F_3 = ((r \leftrightarrow s) \vee t)$
4. $F_4 = \text{true}$
5. $F_5 = (((\neg p \wedge \neg q) \wedge \neg r) \wedge \neg s)$

Antworten

1. β passt zu F_1 und ist minimal.
2. β passt zu F_2, ist aber nicht minimal.
3. β passt nicht zu F_3 und ist also nicht minimal.
4. β passt zu F_4, ist aber nicht minimal.
5. β passt zu F_5 und ist minimal.

Quizfrage

Wie viele unterschiedliche Belegungen gibt es für Formeln über V mit $|V| = n$?

Jede Belegung ist eine Funktion von der Menge der Variablen V nach $\mathbb{B} = \{0, 1\}$. Aus dem Abschnitt für Funktionen wissen wir, dass die Menge B^A der Funktionen $f : A \to B$ genau

$$\left|B^A\right| = |B|^{|A|}$$

verschiedene Funktionen hat. Wegen $|V| = n$ und $|\mathbb{B}| = 2$ gibt es also

$$\left|\mathbb{B}^V\right| = |\mathbb{B}|^{|V|} = 2^n$$

verschiedene Belegungen.

Semantik aussagenlogischer Formeln

Die Semantik $[F]$ einer aussagenlogischer Formel F mit Variablen aus V ist eine Funktion

$$[F] : \mathbb{B}^V \to \mathbb{B},$$

wobei $\mathbb{B}^V$ wieder die Menge aller Belegungen ist.

Für alle Belegungen β gilt folgende induktive Definition:

1. $[\text{true}](\beta) = 1$ und $[\text{false}](\beta) = 0$.
2. Für jede Variable $x \in V$ gilt $[x](\beta) = \beta(x)$.

Semantik aussagenlogischer Formeln

3. Ist $[F]$ die Semantik einer Formel F, dann gilt:

$$[\neg F](\beta) = \begin{cases} 1 & \text{falls } [F](\beta) = 0 \\ 0 & \text{sonst} \end{cases}$$

4. Sind $[F]$ und $[G]$ die Semantiken zweier Formeln F und G, dann gilt:

$$[F \wedge G](\beta) = \begin{cases} 1 & \text{falls } [F](\beta) = 1 \text{ und } [G](\beta) = 1 \\ 0 & \text{sonst} \end{cases}$$

$$[F \vee G](\beta) = \begin{cases} 1 & \text{falls } [F](\beta) = 1 \text{ oder } [G](\beta) = 1 \\ 0 & \text{sonst} \end{cases}$$

Semantik aussagenlogischer Formeln

$$[F \to G](\beta) = \begin{cases} 1 & \text{falls } [F](\beta) = 0 \text{ oder } [G](\beta) = 1 \\ 0 & \text{sonst} \end{cases}$$

$$[F \leftrightarrow G](\beta) = \begin{cases} 1 & \text{falls } [F](\beta) = [G](\beta) \\ 0 & \text{sonst} \end{cases}$$

$$[F \oplus G](\beta) = \begin{cases} 1 & \text{falls } [F](\beta) \neq [G](\beta) \\ 0 & \text{sonst} \end{cases}$$

$$[F \barwedge G](\beta) = \begin{cases} 1 & \text{falls } [F](\beta) = 0 \text{ oder } [G](\beta) = 0 \\ 0 & \text{sonst} \end{cases}$$

$$[F \barvee G](\beta) = \begin{cases} 1 & \text{falls } [F](\beta) = 0 \text{ und } [G](\beta) = 0 \\ 0 & \text{sonst} \end{cases}$$

Info

Je nach Autor kann die Menge der definierten binären Junktoren variieren. Einige beschränken sich nur auf $\wedge$ und $\vee$ und andere nehmen sogar $\oplus$ (ausschließende Disjunktion), $\bar{\wedge}$ (negierte Konjunktion) und $\bar{\vee}$ (negierte Disjunktion) hinzu. Die Semantiken der letzten drei Junktoren sind wie folgt gegeben.

$$
\begin{aligned}
[F \leftrightarrow G](\beta) &= \begin{cases} 1 & \text{falls } [F](\beta) = [G](\beta) \\ 0 & \text{sonst} \end{cases} \\
[F \oplus G](\beta) &= \begin{cases} 1 & \text{falls } [F](\beta) \neq [G](\beta) \\ 0 & \text{sonst} \end{cases} \\
[F \bar{\wedge} G](\beta) &= \begin{cases} 1 & \text{falls } [F](\beta) = 0 \text{ oder } [G](\beta) = 0 \\ 0 & \text{sonst} \end{cases} \\
[F \bar{\vee} G](\beta) &= \begin{cases} 1 & \text{falls } [F](\beta) = 0 \text{ und } [G](\beta) = 0 \\ 0 & \text{sonst} \end{cases}
\end{aligned}
$$

Überblick

Die folgende Tabelle stellt einen Überblick über die Syntax aussagenlogischer Formeln dar.

Arität	Junktor	Schreibweise	Alternative Schreibweisen
0	Wahr	true	1
0	Falsch	false	0
1	Negation	$\neg F$	$\overline{F}$
2	Konjunktion	$F \wedge G$	FG, $F \cdot G$, $F \,\&\, G$
2	Disjunktion	$F \vee G$	$F + G$, $F \mid G$
2	Implikation	$F \rightarrow G$	$F \Rightarrow G$
2	Bikonditional	$F \leftrightarrow G$	$F \Leftrightarrow G$
2	Ausschließende Disjunktion	$F \oplus G$	$F \otimes G$, $F \,\mathrm{XOR}\, G$, $F \underline{\vee} G$
2	Negierte Konjunktion	$F \barwedge G$	$F \,\mathrm{NAND}\, G$
2	Negierte Disjunktion	$F \bar{\vee} G$	$F \,\mathrm{NOR}\, G$

Für den unären Junktor $\neg$ gilt:

Überblick

F	$\neg F$
0	1
1	0

Für die binären Junktoren $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\oplus$, $\barwedge$ und $\barvee$ gilt:

F	G	$F \wedge G$	$F \vee G$	$F \rightarrow G$	$F \leftrightarrow G$	$F \oplus G$	$F \barwedge G$	$F \barvee G$
0	0	0	0	1	1	0	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	0	0	1	1	0
1	1	1	1	1	1	0	0	0

Rezept

Frage: Wie findet man die Semantik einer Formel F?
Methode:

1. Fülle die Wahrheitstafel für F mit Hilfe der Tabellen aus.
2. Lese die Semantik an der entsprechenden Spalte der Wahrheitstafel ab.

Beispiel

Aufgabe: Bestimmen Sie die Semantik $[F]$ folgender Formel F über $V = \{p, q, r\}$:

$$F = \big(q \vee r\big) \rightarrow \neg\big(p \leftrightarrow \neg r\big).$$

Lösung: ,
Erstelle eine leere Wahrheitstafel für $[F]$.

p	q	r	$(q \vee r) \rightarrow \neg (p \leftrightarrow \neg r)$
0	0	0	
0	0	1	
0	1	0	
0	1	1	
1	0	0	
1	0	1	
1	1	0	
1	1	1	

Beispiel

Aufgabe: Bestimme die Semantik $[F]$ folgender Formel F über $V = \{p, q, r\}$:

$$F = (q \vee r) \rightarrow \neg(p \leftrightarrow \neg r).$$

Lösung: ,
Fülle die Spalten für $[p], [q], [r]$ und $[\neg r]$ aus.

p	q	r	$(q$	$\vee$	$r)$	$\rightarrow$	$\neg$	$(p$	$\leftrightarrow$	$\neg r)$
0	0	0	0		0			0		1
0	0	1	0		1			0		0
0	1	0	1		0			0		1
0	1	1	1		1			0		0
1	0	0	0		0			1		1
1	0	1	0		1			1		0
1	1	0	1		0			1		1
1	1	1	1		1			1		0

Beispiel

Aufgabe: Bestimme die Semantik $[F]$ folgender Formel F über $V = \{p, q, r\}$:

$$F = \big(q \vee r\big) \rightarrow \neg\big(p \leftrightarrow \neg r\big).$$

Lösung: ,
Fülle die Spalten für $[(q \vee r)]$ und $[(p \leftrightarrow \neg r)]$ aus.

p	q	r	$(q$	$\vee$	$r)$	$\rightarrow$	$\neg$	$(p$	$\leftrightarrow$	$\neg r)$
0	0	0	0	0	0			0	0	1
0	0	1	0	1	1			0	1	0
0	1	0	1	1	0			0	0	1
0	1	1	1	1	1			0	1	0
1	0	0	0	0	0			1	1	1
1	0	1	0	1	1			1	0	0
1	1	0	1	1	0			1	1	1
1	1	1	1	1	1			1	0	0

Beispiel

Aufgabe: Bestimme die Semantik $[F]$ folgender Formel F über $V = \{p, q, r\}$:

$$F = \big(q \vee r\big) \rightarrow \neg\big(p \leftrightarrow \neg r\big).$$

Lösung: ,
Fülle die Spalte für $[\neg(p \leftrightarrow \neg r)]$ aus.

p	q	r	$(q$	$\vee$	$r)$	$\rightarrow$	$\neg$	$(p$	$\leftrightarrow$	$\neg r)$
0	0	0	0	0	0		1	0	0	1
0	0	1	0	1	1		0	0	1	0
0	1	0	1	1	0		1	0	0	1
0	1	1	1	1	1		0	0	1	0
1	0	0	0	0	0		0	1	1	1
1	0	1	0	1	1		1	1	0	0
1	1	0	1	1	0		0	1	1	1
1	1	1	1	1	1		1	1	0	0

Beispiel

Aufgabe: Bestimme die Semantik $[F]$ folgender Formel F über $V = \{p, q, r\}$:

$$F = \big(q \vee r\big) \rightarrow \neg\big(p \leftrightarrow \neg r\big).$$

Lösung: ,
Fülle die Spalte für $[(q \vee r) \rightarrow \neg(p \leftrightarrow \neg r)]$ also für $[F]$ aus.

p	q	r	$(q$	$\vee$	$r)$	$\rightarrow$	$\neg$	$(p$	$\leftrightarrow$	$\neg r)$
0	0	0	0	0	0	1	1	0	0	1
0	0	1	0	1	1	0	0	0	1	0
0	1	0	1	1	0	1	1	0	0	1
0	1	1	1	1	1	0	0	0	1	0
1	0	0	0	0	0	1	0	1	1	1
1	0	1	0	1	1	1	1	1	0	0
1	1	0	1	1	0	0	0	1	1	1
1	1	1	1	1	1	1	1	1	0	0

Beispiel

Aufgabe: Bestimme die Semantik $[F]$ folgender Formel F über $V = \{p, q, r\}$:

$$F = (q \vee r) \rightarrow \neg(p \leftrightarrow \neg r).$$

Lösung: ,
Die Semantik $[F]$ von F wäre dann formal:

$$[F](p \mapsto 0, q \mapsto 0, r \mapsto 0) = 1 \qquad [F](p \mapsto 1, q \mapsto 0, r \mapsto 0) = 1$$
$$[F](p \mapsto 0, q \mapsto 0, r \mapsto 1) = 0 \qquad [F](p \mapsto 1, q \mapsto 0, r \mapsto 1) = 1$$
$$[F](p \mapsto 0, q \mapsto 1, r \mapsto 0) = 1 \qquad [F](p \mapsto 1, q \mapsto 1, r \mapsto 0) = 0$$
$$[F](p \mapsto 0, q \mapsto 1, r \mapsto 1) = 0 \qquad [F](p \mapsto 1, q \mapsto 1, r \mapsto 1) = 1$$

So formal muss sie aber selten angegeben werden. Normalerweise reicht die Wahrheitstafel aus. :-)

Sei $V = \{p, q, r\}$. Wie sehen die Wahrheitstafeln folgender aussagenlogischer Formeln über V aus?

1. $\neg q \vee \neg(p \to q)$
2. $((p \to q) \wedge (\neg q \leftarrow \neg p)) \vee (p \wedge q)$,
3. $((p \to q) \to r) \leftrightarrow (p \to (q \to r))$,
4. $((p \vee q) \leftrightarrow (p \vee r)) \leftrightarrow (\neg p \wedge (\neg q \leftrightarrow r))$,
5. $(p \vee (q \leftrightarrow r)) \leftrightarrow ((p \leftrightarrow q) \vee (p \leftrightarrow r))$.

1.

p	q	$\neg q$	$\vee$	$\neg$	$(p$	$\rightarrow$	$q)$
0	0	1	1	0	0	1	0
0	1	0	0	0	0	1	1
1	0	1	1	1	1	0	0
1	1	0	0	0	1	1	1

2.

p	q	$((p$	$\rightarrow$	$q)$	$\wedge$	$(\neg q$	$\leftarrow$	$\neg p))$	$\vee$	$(p$	$\wedge$	$q)$
0	0	0	1	0	1	1	1	1	1	0	0	0
0	1	0	1	1	0	0	0	1	0	0	0	1
1	0	1	0	0	0	1	1	0	0	1	0	0
1	1	1	1	1	1	0	1	0	1	1	1	1

3.

p	q	r	$((p$	$\rightarrow$	$q)$	$\rightarrow$	$r)$	$\leftrightarrow$	$(p$	$\rightarrow$	$(q$	$\rightarrow$	$r))$
0	0	0	0	1	0	0	0	0	0	1	0	1	0
0	0	1	0	1	0	1	1	1	0	1	0	1	1
0	1	0	0	1	1	0	0	0	0	1	1	0	0
0	1	1	0	1	1	1	1	1	0	1	1	1	1
1	0	0	1	0	0	1	0	1	1	1	0	1	0
1	0	1	1	0	0	1	1	1	1	1	0	1	1
1	1	0	1	1	1	0	0	1	1	0	1	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1

4.

p	q	r	$((p$	$\vee$	$q)$	$\leftrightarrow$	$(p$	$\vee$	$r))$	$\leftrightarrow$	$(\neg$	p	$\wedge$	$(\neg$	q	$\leftrightarrow$	$r))$
0	0	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0	0
0	0	1	0	0	0	0	0	1	1	0	1	0	1	1	0	1	1
0	1	0	0	1	1	0	0	0	0	0	1	0	1	0	1	1	0
0	1	1	0	1	1	1	0	1	1	0	1	0	0	0	1	0	1
1	0	0	1	1	0	1	1	1	0	0	0	1	0	1	0	0	0
1	0	1	1	1	0	1	1	1	1	0	0	1	0	1	0	1	1
1	1	0	1	1	1	1	1	1	0	0	0	1	0	0	1	1	0
1	1	1	1	1	1	1	1	1	1	0	0	1	0	0	1	0	1

5.

p	q	r	$(p$	$\vee$	$(q$	$\leftrightarrow$	$r))$	$\leftrightarrow$	$((p$	$\leftrightarrow$	$q)$	$\vee$	$(p$	$\leftrightarrow$	$r))$
0	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0
0	0	1	0	0	0	0	1	0	0	1	0	1	0	0	1
0	1	0	0	0	1	0	0	0	0	0	1	1	0	1	0
0	1	1	0	1	1	1	1	0	0	0	1	0	0	0	1
1	0	0	1	1	0	1	0	0	1	0	0	0	1	0	0
1	0	1	1	1	0	0	1	1	1	0	0	1	1	1	1
1	1	0	1	1	1	0	0	1	1	1	1	1	1	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Quizfrage

Wie viele unterschiedliche Semantiken gibt es für Formeln über V mit $|V| = n$?

Jede Semantik $[F]$ ist eine Funktion

$$[F] : \mathbb{B}^V \to \mathbb{B}$$

von der Menge $\mathbb{B}^V$ aller Belegungen nach $\mathbb{B} = \{0, 1\}$. Somit bezeichnet $\mathbb{B}^{\mathbb{B}^V}$ die Menge aller möglichen Semantiken für Formeln über V. (Das sieht sehr seltsam aus, ich weiß!) Also gibt es

$$\left|\mathbb{B}^{\mathbb{B}^V}\right| = |\mathbb{B}|^{|\mathbb{B}|^{|V|}} = 2^{2^n}$$

verschiedene Semantiken.

Beispiel

Für Formeln ohne Variablen gibt es folgende $2^{2^0} = 2$ mögliche Semantiken:

f_1	f_2
0	1

Noch ein Beispiel

Für Formeln mit einer Variable gibt es folgende $2^{2^1} = 4$ mögliche Semantiken:

p	f_1	f_2	f_3	f_4
0	0	0	1	1
1	0	1	0	1

Und noch ein Beispiel

Für Formeln mit zwei Variablen gibt es folgende $2^{2^2} = 16$ mögliche Semantiken:

p	q	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Ein letztes Beispiel

Für Formeln mit drei Variablen gibt es $2^{2^3} = 256$ mögliche Semantiken.

Hier hört der Spaß auf ...

Wir betrachten wieder die Menge aller 16 möglichen Semantiken für Formeln mit zwei Variablen:

p	q	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Welche Semantiken haben folgende aussagenlogische Formeln?

false	true	p	$\neg p$
q	$\neg q$	$p \wedge q$	$p \barwedge q$
$p \vee q$	$p \barvee q$	$p \leftrightarrow q$	$p \oplus q$
$p \rightarrow q$	$\neg(p \rightarrow q)$	$q \rightarrow p$	$\neg(q \rightarrow p)$

p	q	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

$[\text{false}] = f_1$ $[\text{true}] = f_{16}$ $[p] = f_4$ $[\neg p] = f_{13}$

$[q] = f_6$ $[\neg q] = f_{11}$ $[p \wedge q] = f_2$ $[p \barwedge q] = f_{15}$

$[p \vee q] = f_8$ $[p \barvee q] = f_9$ $[p \leftrightarrow q] = f_{10}$ $[p \oplus q] = f_7$

$[p \to q] = f_{14}$ $[\neg(p \to q)] = f_3$ $[q \to p] = f_{12}$ $[\neg(q \to p)] = f_5$

Eigenschaften aussagenlogischer Formeln

Sei F eine aussagenlogische Formel. Dann gilt:

$$
\begin{aligned}
F \text{ erfüllbar} &:\Longleftrightarrow \text{ es gibt eine zu } F \text{ passende Belegung } \beta \text{ mit } [F](\beta) = 1, \\
F \text{ gültig} &:\Longleftrightarrow \text{ für alle zu } F \text{ passende Belegungen } \beta \text{ gilt } [F](\beta) = 1.
\end{aligned}
$$

Infos

- Entsprechend sehen die Negationen aus:

$$
\begin{array}{lcl}
F \text{ nicht erfüllbar} & \iff & \text{für alle zu } F \text{ passende Belegungen } \beta \text{ gilt } [F](\beta) = 0, \\
F \text{ nicht gültig} & \iff & \text{es gibt eine zu } F \text{ passende Belegung } \beta \text{ mit } [F](\beta) = 0.
\end{array}
$$

- Eine nicht erfüllbare Formel wird auch unerfüllbar oder Widerspruch genannt.
- Eine gültige Formel wird auch allgemeingültig oder Tautologie genannt.
- Eine nicht gültige Formel wird auch falsifizierbar genannt.

Beispiel

Sei $V = \{p, q, r\}$ und F wieder folgende aussagenlogische Formel über V:

$$F = (q \vee r) \to \neg(p \leftrightarrow \neg r).$$

p	q	r	$(q$	$\vee$	$r)$	$\to$	$\neg$	$(p$	$\leftrightarrow$	$\neg r)$
0	0	0	0	0	0	1	1	0	0	1
0	0	1	0	1	1	0	0	0	1	0
0	1	0	1	1	0	1	1	0	0	1
0	1	1	1	1	1	0	0	0	1	0
1	0	0	0	0	0	1	0	1	1	1
1	0	1	0	1	1	1	1	1	0	0
1	1	0	1	1	0	0	0	1	1	1
1	1	1	1	1	1	1	1	1	0	0

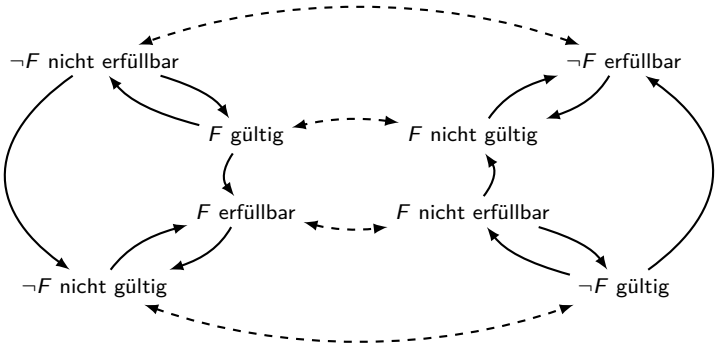
- F ist erfüllbar, da z.B. $[F](p \mapsto 0, q \mapsto 0, r \mapsto 0) = 1$.
- F ist nicht gültig, da z.B. $[F](p \mapsto 0, q \mapsto 0, r \mapsto 1) = 0$.

Quizfrage

Welche der folgenden Implikationen gelten für jede aussagenlogische Formel F?

1.	F gültig	$\Longrightarrow$	F erfüllbar
2.	F gültig	$\Longrightarrow$	$\neg F$ nicht erfüllbar
3.	F gültig	$\Longrightarrow$	$\neg F$ nicht gültig
4.	F erfüllbar	$\Longrightarrow$	F gültig
5.	F erfüllbar	$\Longrightarrow$	$\neg F$ nicht erfüllbar
6.	F erfüllbar	$\Longrightarrow$	$\neg F$ nicht gültig
7.	F nicht gültig	$\Longrightarrow$	F nicht erfüllbar
8.	F nicht gültig	$\Longrightarrow$	$\neg F$ gültig
9.	F nicht gültig	$\Longrightarrow$	$\neg F$ erfüllbar
10.	F nicht erfüllbar	$\Longrightarrow$	F nicht gültig
11.	F nicht erfüllbar	$\Longrightarrow$	$\neg F$ gültig
12.	F nicht erfüllbar	$\Longrightarrow$	$\neg F$ erfüllbar

Es gelten alle Implikationen außer die 4, die 5, die 7 und die 8. Folgendes Bild fasst das Ergebnis dieser Quizfrage zusammen.



Gestrichelte Pfeile stellen Negationen und normale Pfeile Implikationen dar.

Themenübersicht

Logische Äquivalenz $\equiv$

Sei V eine beliebige Menge. Für beliebige aussagenlogische Formeln F und G über V gilt $F \equiv G$ genau dann, wenn für jede Belegung $\beta : V \to \mathbb{B}$ gilt:

$$[F](\beta) = 1 \text{ genau dann, wenn } [G](\beta) = 1.$$

In kompakter Schreibweise heißt das:

$$F \equiv G \quad :\Longleftrightarrow \quad (\forall \beta \in \mathbb{B}^V : [F](\beta) = 1 \iff [G](\beta) = 1) \ .$$

Infos

- $\equiv$ ist nichts anderes als eine Relation über aussagenlogische Formeln.
- Für $F \equiv G$ sagen wir „F und G sind äquivalent“.
- Damit $F \equiv G$ gilt müssen F und G nicht unbedingt genau dieselben Variablen besitzen.
- Auf Folie 683 sind wichtige Aussagen zur logischen Äquivalenz aufgelistet.

Beispiel

Für $F = ((\neg p \vee q) \to (p \wedge q))$ und $G = ((r \to p) \wedge (\neg r \to p))$ gilt $F \equiv G$:

p	q	r	$((\neg p$	$\vee$	$q)$	$\to$	$(p$	$\wedge$	$q))$	$((r$	$\to$	$p)$	$\wedge$	$(\neg r$	$\to$	$p))$
0	0	0	1	1	0	0	0	0	0	0	1	0	0	1	0	0
0	0	1	1	1	0	0	0	0	0	1	0	0	0	0	1	0
0	1	0	1	1	1	0	0	0	1	0	1	0	0	1	0	0
0	1	1	1	1	1	0	0	0	1	1	0	0	0	0	1	0
1	0	0	0	0	0	1	1	0	0	0	1	1	1	1	1	1
1	0	1	0	0	0	1	1	0	0	1	1	1	1	0	1	1
1	1	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1
1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1

Die Formel $(F \leftrightarrow G)$ ist also gültig.

Nicht verwechseln!

- „$\leftrightarrow$“ ist ein logischer Junktor, d.h. er ist ein Teil von aussagenlogischen Formeln. Sind F und G Formeln, dann auch $F \leftrightarrow G$. Insbesondere besitzt diese auch eine Semantik.
- „$\equiv$“ beschreibt das Verhältnis zwischen zwei Formeln, d.h. es handelt sich um eine Relation über aussagenlogische Formeln mit Eigenschaften wie z.B. reflexiv. Damit man $F \equiv G$ schreiben darf, müssen F und G Formeln sein. $F \equiv G$ ist aber an sich, im Gegensatz zu $F \leftrightarrow G$, keine Formel!
- „ $\Longleftrightarrow$ “ ist weder ein logischer Junktor noch eine Relation. Es ist nur eine Abkürzung für „genau dann, wenn“. Dieses Symbol gehört zur logischen Metaebene. Damit man $A \Longleftrightarrow B$ schreiben darf, müssen A und B irgendwelche Aussagen sein und keine aussagenlogische Formeln.

Quizfrage

Welche Eigenschaften besitzt die homogene Relation $\equiv$ über aussagenlogische Formeln?

Antwort

$\equiv$ ist reflexiv, symmetrisch und transitiv, also eine Äquivalenzrelation.

Info: Bei n Variablen hat die durch $\equiv$ induzierte Partition genau 2^{2^n} Äquivalenzklassen, eine für jede Semantik ;-)

Äquivalenzregeln

Äquivalenzregeln

Seien F, G und H aussagenlogische Formeln. Ein paar nützliche Äquivalenzregeln sind:

$F \wedge \text{true} \equiv F$	$F \vee \text{false} \equiv F$	(Identität)
$F \vee \text{true} \equiv \text{true}$	$F \wedge \text{false} \equiv \text{false}$	(Dominanz)
$F \vee F \equiv F$	$F \wedge F \equiv F$	(Idempotenz)
$\neg\neg F \equiv F$		(Doppelte Negation)
$F \vee \neg F \equiv \text{true}$	$F \wedge \neg F \equiv \text{false}$	(Triv. Taut./Kontr.)
$F \vee G \equiv G \vee F$	$F \wedge G \equiv G \wedge F$	(Kommutativität)
$(F \vee G) \vee H \equiv F \vee (G \vee H)$	$(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$	(Assoziativität)
$F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$	$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$	(Distributivität)
$\neg(F \wedge G) \equiv \neg F \vee \neg G$	$\neg(F \vee G) \equiv \neg F \wedge \neg G$	(De Morgan)
$F \oplus G \equiv (F \vee G) \wedge \neg(F \wedge G)$	$F \oplus G \equiv (F \wedge \neg G) \vee (G \wedge \neg F)$	(Exklusives-Oder)
$F \to G \equiv \neg F \vee G$	$F \vee G \equiv \neg F \to G$	(Implikation)
$F \leftrightarrow G \equiv (F \to G) \wedge (G \to F)$	$F \leftrightarrow G \equiv \neg(F \oplus G)$	(Bikonditional)
$F \barwedge G \equiv \neg(F \wedge G)$	$F \barvee G \equiv \neg(F \vee G)$	(NAND und NOR)
$F \vee (F \wedge G) \equiv F$	$F \wedge (F \vee G) \equiv F$	(Absorption)

Man kann diese Regeln beweisen, in dem man die Teilformeln F, G und H als Variablen betrachtet, das $\equiv$-Symbol durch ein $\leftrightarrow$ ersetzt und die Gültigkeit der entstehenden Formel mit einer Wahrheitstafel beweist.

Beispielsweise gilt für die erste Regel von De Morgan:

F	G	$\neg$	$(F$	$\wedge$	$G)$	$\leftrightarrow$	$(\neg F$	$\vee$	$\neg G)$
0	0	1	0	0	0	1	1	1	1
0	1	1	0	0	1	1	1	1	0
1	0	1	1	0	0	1	0	1	1
1	1	0	1	1	1	1	0	0	0

Diese Methode kann für beliebige Formeln angewendet werden (wurde in der Vorlesung gesagt, aber nicht bewiesen).

Welche der folgenden Äquivalenzen sind richtig?

1. $(p \to q) \equiv (\neg p \to \neg q)$,
2. $(p \to q) \equiv (\neg q \to \neg p)$,
3. $\neg(p \to q) \equiv (\neg p \to \neg q)$,
4. $\neg(p \to q) \equiv (\neg q \to \neg p)$,
5. $(p \to q) \equiv (\neg p \vee q)$,
6. $(p \to q) \equiv (p \vee \neg q)$,
7. $\neg(p \to q) \equiv (\neg p \wedge q)$,
8. $\neg(p \to q) \equiv (p \wedge \neg q)$.

Antworten

1. Falsch.
2. Richtig.
3. Falsch.
4. Falsch.
5. Richtig.
6. Falsch.
7. Falsch.
8. Richtig.

Info

Um die Äquivalenz $F \equiv G$ zweier Formeln F und G zu zeigen, haben wir zwei Methoden kennengelernt:

1. Die Wahrheitstafel für $F \leftrightarrow G$ aufstellen und überprüfen, ob die Formel eine Tautologie ist.
2. Mithilfe der Äquivalenzregeln Formeln $F_1, F_2, \ldots, F_n$ finden mit:

$$F \equiv F_1 \equiv F_2 \equiv \ldots \equiv F_n \equiv G.$$

Wahrheitstafeln sind einfach und führen automatisch zum Ziel. Leider hat eine Formel mit n Variablen eine Wahrheitstafel mit 2^n Zeilen. Für $n \leq 3$ Variablen sind Wahrheitstafeln sehr angenehm. Für $n \geq 4$ Variablen sind Äquivalenzumformungen besser.

Themenübersicht

Logische Inferenz $\models$

Sei V eine beliebige Menge. Für beliebige aussagenlogische Formeln F und G über V gilt $F \models G$ genau dann, wenn für jede Belegung $\beta : V \to \mathbb{B}$ gilt:

$$\text{Wenn } [F](\beta) = 1, \text{ dann } [G](\beta) = 1.$$

In kompakter Schreibweise heißt das:

$$F \models G \quad :\Longleftrightarrow \quad (\forall \beta \in \mathbb{B}^V : [F](\beta) = 1 \implies [G](\beta) = 1) \ .$$

Infos

- $\models$ ist, wie $\equiv$, nichts anderes als eine Relation über aussagenlogische Formeln. Sie heißt Folgerungsrelation.
- Für $F \models G$ sagen wir „aus F folgt G“.
- Damit $F \models G$ gilt müssen F und G nicht unbedingt genau dieselben Variablen besitzen.
- Auf Folie 686 sind wichtige Aussagen zur logischen Äquivalenz aufgelistet.
- Für Inferenzen der Form $A_1 \wedge \ldots \wedge A_n \models G$ schreiben wir oft $A_1, \ldots, A_n \models G$ oder $\{A_1, \ldots, A_n\} \models G$. Insbesondere definieren wir:

$$\models G \quad :\Longleftrightarrow \quad G \text{ ist gültig} \ .$$

Diese Definition macht Sinn, weil die leere Konjunktion als true definiert wurde und es gilt:

$$\text{true} \models G \quad \Longleftrightarrow \quad (\text{true} \rightarrow G) \text{ ist gültig} \quad \Longleftrightarrow \quad G \text{ ist gültig.}$$

Beispiel

Für $F = ((\neg p \vee q) \to (p \wedge q))$ und $G = ((r \to p) \to (\neg r \to p))$ gilt $F \models G$.

p	q	r	$((\neg p$	$\vee$	$q)$	$\to$	$(p$	$\wedge$	$q))$	$((r$	$\to$	$p)$	$\to$	$(\neg r$	$\to$	$p))$
0	0	0	1	1	0	0	0	0	0	0	1	0	0	1	0	0
0	0	1	1	1	0	0	0	0	0	1	0	1	1	0	1	1
0	1	0	1	1	1	0	0	0	1	0	1	0	0	1	0	0
0	1	1	1	1	1	0	0	0	1	1	0	0	1	0	1	0
1	0	0	0	0	0	1	1	0	0	0	1	1	1	1	1	1
1	0	1	0	0	0	1	1	0	0	1	1	1	1	0	1	1
1	1	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1
1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1

Die Formel $(F \to G)$ ist also gültig.

Nicht verwechseln!

Analog zum Unterschied zwischen den Symbolen „$\leftrightarrow$“, „$\equiv$“ und „ $\Longleftrightarrow$ “ (s. Folie 563), unterscheiden sich „$\rightarrow$“, „$\models$“ und „ $\Longrightarrow$ “ darin, dass „$\rightarrow$“ ein logischer Junktor, „$\models$“ eine homogene Relation über aussagenlogische Formeln und „ $\Longrightarrow$ “ eine Abkürzung auf der logischen Metaebene für „dann gilt“ ist.

Als Tabelle:

Logische Ebene	Äquivalenz	Implikation
Abkürzungen in der Metaebene	$\Longleftrightarrow$	$\Longrightarrow$
Relationen über Formeln	$\equiv$	$\models$
Junktoren in der Aussagenlogik	$\leftrightarrow$	$\rightarrow$

Quizfrage

Welche Eigenschaften besitzt die homogene Relation $\models$ über aussagenlogische Formeln?

Antwort

$\models$ ist nur reflexiv und transitiv.

Themenübersicht

Literale

Ein Literal ist eine Variable oder die Negation einer Variable.

Beispiel

Die Menge aller Literale über $V = \{p, q, r\}$ ist $\{p, q, r, \neg p, \neg q, \neg r\}$.

Disjunktionen

Eine Disjunktion F von Formeln $F_1, \ldots, F_n$ ist eine Formel der Form $F = F_1 \vee \ldots \vee F_n$.

Beispiel

$F = (q \leftrightarrow (p \vee r)) \vee (r \rightarrow q) \vee p \vee (p \wedge q)$ ist eine Disjunktion.

Info

Weil $\vee$ assoziativ ist, ist es egal wie die einzelnen Formeln $F_1, \ldots, F_n$ geklammert werden. Deswegen dürfen wir auch die Klammern einfach weglassen.

Konjunktionen

Eine Konjunktion F von Formeln $F_1, \ldots, F_n$ ist eine Formel der Form $F = F_1 \wedge \ldots \wedge F_n$.

Beispiel

$F = (p \to q) \wedge q \wedge (q \leftrightarrow r) \wedge (p \vee q \vee s)$ ist eine Konjunktion.

Info

Weil $\wedge$ assoziativ ist, ist es egal wie die einzelnen Formeln $F_1, \ldots, F_n$ geklammert werden. Deswegen dürfen wir auch die Klammern einfach weglassen.

Infos

- Die Disjunktion von null Formeln (die „leere Disjunktion“) ist $F := \text{false}$.
- Die Konjunktion von null Formeln (die „leere Konjunktion“) ist $F := \text{true}$.

Disjunktive Normalform

Sei V eine beliebige Menge.

- eine Formel über V heißt DNF-Klausel, falls sie eine Konjunktion von Literalen ist.
- Eine Formel über V in disjunktiver Normalform (DNF) ist eine Disjunktion von DNF-Klauseln.

Beispiel

Folgende Formel F über $V = \{p, q, r, s\}$ ist in DNF:

$$F = \underbrace{\underbrace{(\neg p \wedge r \wedge s)}_{\text{Konjunktion}} \vee \underbrace{(\neg q \wedge \neg s)}_{\text{Konjunktion}} \vee \underbrace{(p \wedge q \wedge \neg r \wedge s)}_{\text{Konjunktion}} \vee \underbrace{(\neg r \wedge s)}_{\text{Konjunktion}}}_{\textit{Disjunktion}}$$

Konjunktive Normalform

Sei V eine beliebige Menge.

- eine Formel über V heißt KNF-Klausel, falls sie eine Disjunktion von Literalen ist.
- Eine Formel über V in konjunktiver Normalform (KNF) ist eine Konjunktion von KNF-Klauseln.

Beispiel

Folgende Formel F über $V = \{p, q, r, s\}$ ist in KNF:

$$F = \underbrace{\underbrace{(\neg p \vee r \vee s)}_{\text{Disjunktion}} \wedge \underbrace{(\neg q \vee \neg s)}_{\text{Disjunktion}} \wedge \underbrace{(p \vee q \vee \neg r \vee s)}_{\text{Disjunktion}} \wedge \underbrace{(\neg r \vee s)}_{\text{Disjunktion}}}_{\textit{Konjunktion}}$$

Vollständige Normalformen

Eine Formel ist in vollständiger DNF oder KNF, falls alle Klauseln in ihr genau dieselben Variablen besitzen.

Beispiel

Sei $V = \{p, q, r\}$.

- Die Formel $F_1 = \neg p \vee (p \wedge q \wedge r)$ über V ist in nicht vollständiger DNF.
- Die Formel $F_2 = (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r)$ über V ist in vollständiger DNF.
- Die Formel $F_1 = (\neg p \vee q) \wedge (\neg q \vee r)$ über V ist in nicht vollständiger KNF.
- Die Formel $F_2 = (p \vee \neg q \vee \neg r) \wedge (p \vee q \vee r)$ über V ist in vollständiger KNF.

Rezept

Frage: Wie findet man eine zu einer gegebenen Formel F äquivalente Formel in vollständiger DNF bzw. KNF?
Methode: Zuerst stelle die Wahrheitstafel der Formel F auf. Dann:

DNF:

1. Wähle Zeilen mit Ergebnis 1.
2. Bilde für jede Zeile eine Konjunktion aller Variablen (mit „$\wedge$“),
   in der alle mit 0 belegten Variablen negiert sind und die anderen nicht.
3. Bilde eine Disjunktion aller Konjunktionen (mit „$\vee$“).

KNF:

1. Wähle Zeilen mit Ergebnis 0.

Rezept

2. Bilde für jede Zeile eine Disjunktion aller Variablen (mit „$\vee$“),
   in der alle mit 1 belegten Variablen negiert sind und die anderen nicht.

3. Bilde eine Konjunktion aller Disjunktionen (mit „$\wedge$“).

Beispiel

Aufgabe: Sei F eine Formel über $\{p, q, r\}$ mit folgender Wahrheitstafel:

p	q	r	F
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Finde eine zu F äquivalente Formel in vollständiger DNF und eine in vollständiger KNF.

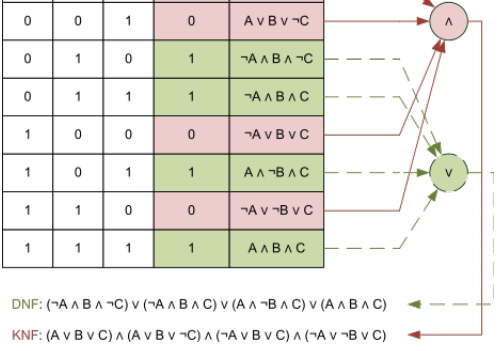
Lösung:

$$\begin{aligned} F &\equiv (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r) && \text{(DNF)} \\ &\equiv (p \vee q \vee r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) && \text{(KNF)} \end{aligned}$$

Noch ein Beispiel

Dieses Beispiel habe ich von Wikipedia geklaut:

A	B	C	Ergebnis	Klausel
0	0	0	0	$A \vee B \vee C$
0	0	1	0	$A \vee B \vee \neg C$
0	1	0	1	$\neg A \wedge B \wedge \neg C$
0	1	1	1	$\neg A \wedge B \wedge C$
1	0	0	0	$\neg A \vee B \vee C$
1	0	1	1	$A \wedge \neg B \wedge C$
1	1	0	0	$\neg A \vee \neg B \vee C$
1	1	1	1	$A \wedge B \wedge C$



Quelle: `de.wikipedia.org/wiki/Disjunktive_Normalform`

Seien F, G und H aussagenlogische Formeln über $\{p, q, r\}$ mit folgenden Wahrheitstafeln:

p	q	r	F	G	H
0	0	0	0	0	1
0	0	1	0	1	0
0	1	0	0	0	0
0	1	1	1	1	0
1	0	0	1	1	0
1	0	1	1	0	1
1	1	0	0	1	1
1	1	1	1	1	1

1. Welche Formeln in vollständiger DNF bzw. KNF sind äquivalent zu F?
2. Welche Formeln in vollständiger DNF bzw. KNF sind äquivalent zu G?
3. Welche Formeln in vollständiger DNF bzw. KNF sind äquivalent zu H?

1.

$$\begin{aligned} F &\equiv (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r) && \text{(DNF)} \\ &\equiv (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee \neg q \vee r) && \text{(KNF)} \end{aligned}$$

2.

$$\begin{aligned} G &\equiv (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r) && \text{(DNF)} \\ &\equiv (p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) && \text{(KNF)} \end{aligned}$$

3.

$$\begin{aligned} H &\equiv (\neg p \wedge \neg q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r) && \text{(DNF)} \\ &\equiv (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee r) && \text{(KNF)} \end{aligned}$$

Wie ist die Semantik (als Wahrheitstafel) folgender Formeln?

1. $F_1 = (\neg p \wedge \neg q) \vee (p \wedge \neg q) \vee (p \wedge q)$
2. $F_2 = (p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$

Hinweis: Man braucht nicht die Wahrheitstafeln komplett auszufüllen, denn F_1 und F_2 sind in vollständiger DNF bzw. KNF.

Antworten

1.

p	q	F_1
0	0	1
0	1	0
1	0	1
1	1	1

2.

p	q	F_2
0	0	0
0	1	0
1	0	1
1	1	0

Ersetzen von Variablen

Sei V eine Variablenmenge und F eine KNF-Formel mit $p \in V_F$.

- $F[p \setminus \text{true}]$ bezeichnet die Formel, die entsteht, in dem jedem Vorkommnis von p in F durch true ersetzt wird.
- $F[p \setminus \text{false}]$ bezeichnet die Formel, die entsteht, in dem jedem Vorkommnis von p in F durch false ersetzt wird.

Nachdem eine Variable mit true oder false belegt wurde, kann die entstehende Formel mit folgenden Regeln vereinfacht werden:

$$\begin{array}{lll} F \wedge \text{true} \equiv F, & F \vee \text{true} \equiv \text{true}, & \neg\,\text{true} \equiv \text{false}, \\ F \wedge \text{false} \equiv \text{false}, & F \vee \text{false} \equiv F, & \neg\,\text{false} \equiv \text{true}\,. \end{array}$$

Beispiel

Sei F folgende KNF-Formel über $V = \{p, q, r, s\}$:

$$F = (\neg p \vee q \vee s) \wedge (p \vee \neg q \vee \neg s) \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee \neg r \vee s).$$

Dann gilt

$$\begin{aligned} F[p \setminus \text{true}] &\equiv (\cancel{\neg p} \vee q \vee s) \wedge \cancel{(p \vee \neg q \vee \neg s)} \wedge \cancel{(p \vee q \vee \neg r)} \wedge (\cancel{\neg p} \vee \neg r \vee s) \\ &\equiv (q \vee s) \wedge (\neg r \vee s) \end{aligned}$$

und

$$\begin{aligned} F[p \setminus \text{false}] &\equiv \cancel{(\neg p \vee q \vee s)} \wedge (\cancel{p} \vee \neg q \vee \neg s) \wedge (\cancel{p} \vee q \vee \neg r) \wedge \cancel{(\neg p \vee \neg r \vee s)} \\ &\equiv (\neg q \vee \neg s) \wedge (q \vee \neg r). \end{aligned}$$

Infos

- $F[p \setminus \text{true}]$ entspricht also F ohne Vorkommnisse von $\neg p$ und ohne Klauseln, die p enthalten.
- $F[p \setminus \text{false}]$ entspricht also F ohne Vorkommnisse von p und ohne Klauseln, die $\neg p$ enthalten.

Themenübersicht

Rezept

Frage: Wie überprüft man mit dem DPLL-Algorithmus, ob eine gegebene KNF-Formel F erfüllbar ist?
Methode: Führe den Algorithmus aus ;-)

1. Wenn $F = \{\}$ (d.h. $F = \text{true}$), dann antworte „erfüllbar“;
2. Wenn $F = \{\{\}\}$ (d.h. $F = \text{false}$), dann antworte „unerfüllbar“;
3. Sonst:
4. Wenn F eine Klausel $\{p\}$ enthält:
5. Führe den Algorithmus für $F[p \setminus \text{true}]$ aus;
6. Wenn F eine Klausel $\{\neg p\}$ enthält:
7. Führe den Algorithmus für $F[p \setminus \text{false}]$ aus;
8. Sonst wähle eine Variable $p \in V_F$ und:

Rezept

9. Falls $F[p \setminus \text{true}]$ erfüllbar ist, antworte „erfüllbar“;

10. Falls $F[p \setminus \text{false}]$ erfüllbar ist, antworte „erfüllbar“;

Infos

- DPLL überprüft die Erfüllbarkeit einer KNF-Formel.
- KNF-Formeln werden als Mengen dargestellt. Zum Beispiel:

$$(\neg p \vee q \vee \neg r) \wedge q \wedge (r \vee \neg s) \quad \rightsquigarrow \quad \{\{\neg p, q, \neg r\}, \{q\}, \{r, \neg s\}\}$$

- Achtung mit der leeren Menge $\{\}$:

$$\begin{array}{lcll} \text{leere Klausel} & \hat{=} & \text{leere Disjunktion} & \hat{=} \quad \text{false} \\ \text{leere Formel} & \hat{=} & \text{leere Konjunktion} & \hat{=} \quad \text{true} \end{array}$$

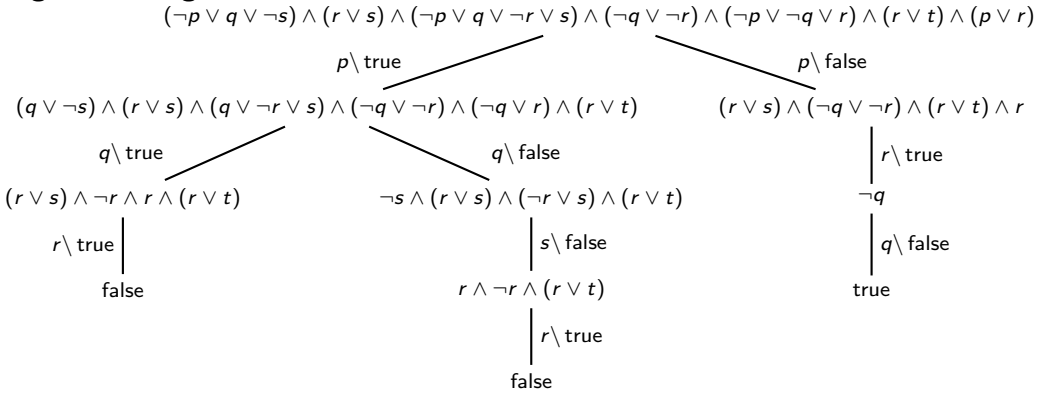
- Dieser Algorithmus wird in der Vorlesung „Algorithmus 2“ genannt. Entfernt man die one-literal rule (Zeilen 4-7), so bekommt man den „Algorithmus 1“ aus der Vorlesung.

Beispiel

Aufgabe: Überprüfe die Erfüllbarkeit folgender Formel mit dem DPLL-Algorithmus:

$$F = (\neg p \vee q \vee \neg s) \wedge (r \vee s) \wedge (\neg p \vee q \vee \neg r \vee s) \wedge (\neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee r) \wedge (r \vee t) \wedge (p \vee r).$$

Mögliche Lösung als Formeln:



Beispiel

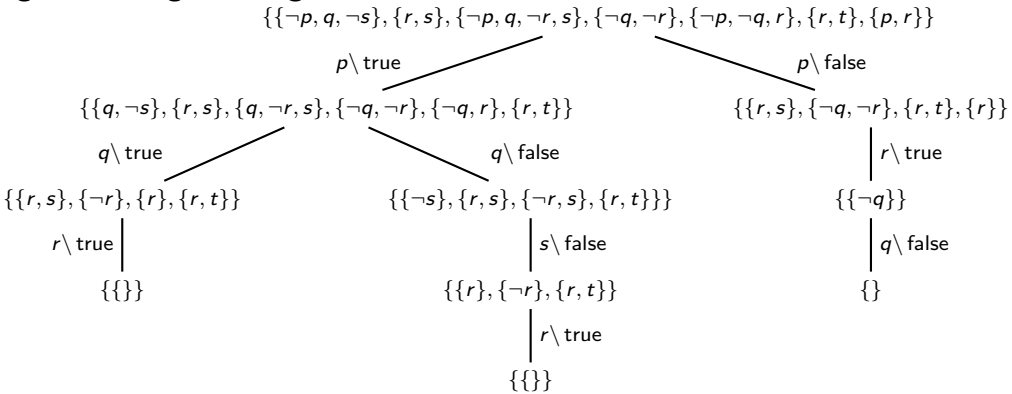
Jede Belegung β mit $p \mapsto 0$, $r \mapsto 1$ und $q \mapsto 0$ ist erfüllend.

Beispiel

Aufgabe: Überprüfe die Erfüllbarkeit folgender Formel mit dem DPLL-Algorithmus:

$$F = (\neg p \vee q \vee \neg s) \wedge (r \vee s) \wedge (\neg p \vee q \vee \neg r \vee s) \wedge (\neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee r) \wedge (r \vee t) \wedge (p \vee r).$$

Mögliche Lösung als Mengen:



Beispiel

Jede Belegung β mit $p \mapsto 0$, $r \mapsto 1$ und $q \mapsto 0$ ist erfüllend.

Infos

- Die leere Menge $\{\}$ stellt die leere Formel dar und $\{\{\}\}$ die Formel mit einer leeren Klausel, d.h.:

$$\{\} = \text{true}, \quad \text{aber} \quad \{\{\}\} = \text{false}\,.$$

- Kommt man auf eine Formel, die die leere Klausel enthält, so ist diese äquivalent zu false. Dann müssen wir zur letzten Verzweigung zurück gehen und von da aus weitermachen. Liefern alle Pfade false, so ist die Formel unerfüllbar.
- Bei DPLL ist die Lösung nicht immer eindeutig! Wir können die Reihenfolge, in der Variablen ersetzt werden, und den Wert, durch den sie ersetzt werden, selber wählen.
- Der Algorithmus hält, sobald die leere Menge zum ersten Mal gefunden wird.

Gegeben sei folgende Formel:

$$F = ((q \wedge s) \rightarrow \neg r) \wedge (q \rightarrow s) \wedge (p \rightarrow q) \wedge ((p \wedge q) \rightarrow (r \vee \neg s)) \wedge (p \vee q).$$

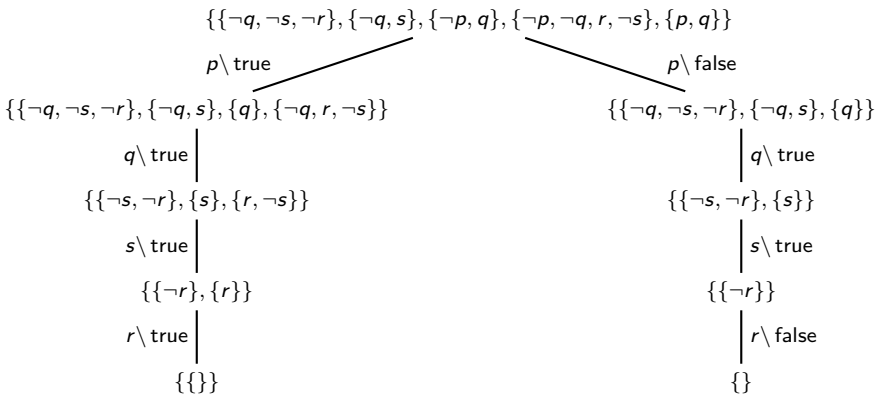
1. Welche KNF-Formel ist äquivalent zu F?
2. Ist F erfüllbar?

Hinweis: Benutze Äquivalenzregeln und DPLL.

1. Äquivalenzumformungen:

$$
\begin{aligned}
F &= ((q \wedge s) \to \neg r) \wedge (q \to s) \wedge (p \to q) \wedge ((p \wedge q) \to (r \vee \neg s)) \wedge (p \vee q) \\
&\equiv (\neg(q \wedge s) \vee \neg r) \wedge (\neg q \vee s) \wedge (\neg p \vee q) \wedge (\neg(p \wedge q) \vee (r \vee \neg s)) \wedge (p \vee q) \\
&\equiv (\neg q \vee \neg s \vee \neg r) \wedge (\neg q \vee s) \wedge (\neg p \vee q) \wedge (\neg p \vee \neg q \vee r \vee \neg s) \wedge (p \vee q).
\end{aligned}
$$

2. DPLL:


$\{\{\neg q, \neg s, \neg r\}, \{\neg q, s\}, \{\neg p, q\}, \{\neg p, \neg q, r, \neg s\}, \{p, q\}\}$
$p \setminus \text{true}$
$p \setminus \text{false}$
$\{\{\neg q, \neg s, \neg r\}, \{\neg q, s\}, \{q\}, \{\neg q, r, \neg s\}\}$
$\{\{\neg q, \neg s, \neg r\}, \{\neg q, s\}, \{q\}\}$
$q \setminus \text{true}$
$q \setminus \text{true}$
$\{\{\neg s, \neg r\}, \{s\}, \{r, \neg s\}\}$
$\{\{\neg s, \neg r\}, \{s\}\}$
$s \setminus \text{true}$
$s \setminus \text{true}$
$\{\{\neg r\}, \{r\}\}$
$\{\{\neg r\}\}$
$r \setminus \text{true}$
$r \setminus \text{false}$
$\{\{\}\}$
$\{\}$

Themenübersicht

Resolution

Sei F eine KNF-Formel und

$$(l_1 \vee \ldots \vee l_k \vee p) \quad \text{und} \quad (\neg p \vee l'_1 \vee \ldots \vee l'_m)$$

zwei Klauseln in F für irgendwelche Literale $l_1, \ldots, l_k, l'_1, \ldots, l'_m$ und eine Variable p.

Aus den Äquivalenzregeln wissen wir:

$$\begin{array}{lcl} (l_1 \vee \ldots \vee l_k \vee p) & \equiv & \neg(l_1 \vee \ldots \vee l_k) \rightarrow p \\ (\neg p \vee l'_1 \vee \ldots \vee l'_m) & \equiv & p \rightarrow (l'_1 \vee \ldots \vee l'_m) \end{array}$$

Aus diesen zwei Implikationen folgt sofort

$$\neg(l_1 \vee \ldots \vee l_k) \rightarrow (l'_1 \vee \ldots \vee l'_m),$$

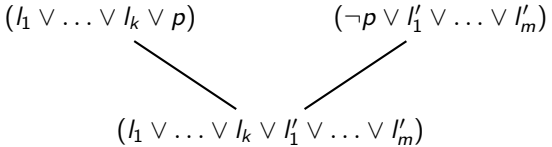
was äquivalent ist zur KNF-Klausel

$$(l_1 \vee \ldots \vee l_k \vee l'_1 \vee \ldots \vee l'_m).$$

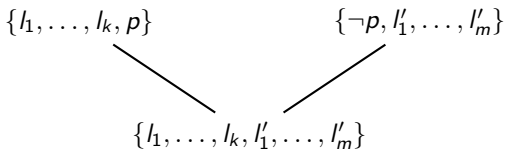
Resolution

Die Klausel $(l_1 \vee \ldots \vee l_k \vee l'_1 \vee \ldots \vee l'_m)$ wird Resolvent genannt und kann in F hinzugefügt werden ohne die Semantik von F zu ändern.

Graphisch kann das wie folgt dargestellt werden:



In Mengendarstellung:



Rezept

Frage: Wie überprüft man mit Resolution, ob eine gegebene KNF-Formel F unerfüllbar ist?
Methode: Füge durch Resolution so viele Klauseln in F hinzu, bis $\{\}$ (bzw. false) als Resolvent vorkommt oder bis keine neue Klauseln entstehen können. Im ersten Fall ist die Formel unerfüllbar, im zweiten erfüllbar.

Beispiel

Aufgabe: Überprüfe die Unerfüllbarkeit folgender Formel mit dem Resolutionsverfahren:

$$F = (\neg r \vee \neg t) \wedge (r \vee s \vee \neg t) \wedge (q \vee s \vee t) \wedge (r \vee \neg s) \wedge \neg q \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee q).$$

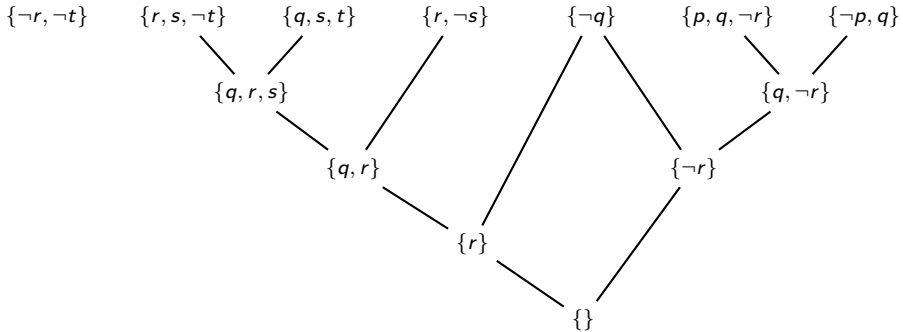
Beispiel

Beispiel

Aufgabe: Überprüfe die Unerfüllbarkeit folgender Formel mit dem Resolutionsverfahren:

$$F = (\neg r \vee \neg t) \wedge (r \vee s \vee \neg t) \wedge (q \vee s \vee t) \wedge (r \vee \neg s) \wedge \neg q \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee q).$$

Mögliche Lösung:



Infos

- Bei Resolution ist $\{\}$ (oft auch $\square$) nicht die leere Formel, sondern die leere Klausel. Bei Resolution werden die Mengenklammern ja weggelassen. D.h. hier ist, im Gegensatz zu DPLL, $\{\} = \text{false}$.
- Bei Resolution darf immer nur ein Literal als Resolvent benutzt werden. Aus $\{p, \neg q, r\}$ und $\{q, \neg r, s\}$ folgt beispielsweise nicht $\{p, s\}$!
- Klauseln dürfen mehrmals oder auch gar nicht benutzt werden. Die generierten Klauseln werden in die Formel hinzugefügt, d.h. sie ersetzen nicht die benutzten Klauseln.
- Möchte man die Gültigkeit einer DNF-Formel F überprüfen, so kann $\neg F$ mithilfe der De Morgansche Regeln ganz einfach in KNF gebracht werden. F ist dann gültig genau dann, wenn $\neg F$ unerfüllbar ist, z.B.:

$$F = (p \wedge \neg q) \vee (q \wedge \neg r) \vee \neg r \qquad \rightsquigarrow \qquad \neg F \equiv (\neg p \vee q) \wedge (\neg q \vee r) \wedge r$$

Gegeben sei folgende Formel:

$$F = (p \to r) \wedge q \wedge (q \to p) \wedge (q \to t) \wedge ((p \wedge r) \to s) \wedge (s \to t) \wedge ((s \wedge t) \to \text{false}).$$

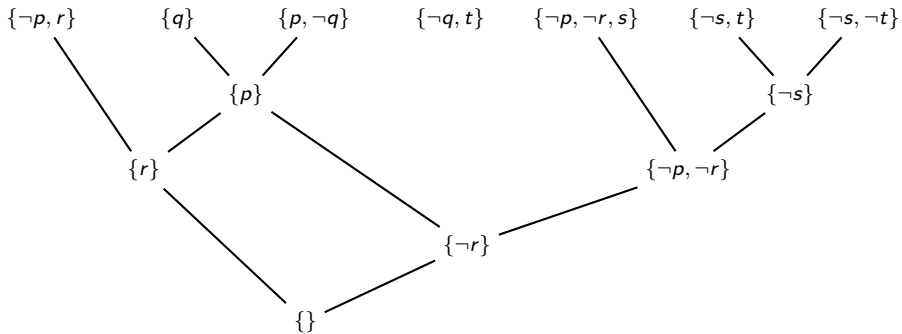
1. Welche KNF-Formel ist äquivalent zu F?
2. Ist F unerfüllbar?

Hinweis: Benutze Äquivalenzregeln und Resolution.

1. Äquivalenzumformungen:

$$
\begin{aligned}
F &= (p \to r) \land q \land (q \to p) \land (q \to t) \land ((p \land r) \to s) \land (s \to t) \land ((s \land t) \to \text{false}) \\
&\equiv (\neg p \lor r) \land q \land (\neg q \lor p) \land (\neg q \lor t) \land (\neg(p \land r) \lor s) \land (\neg s \lor t) \land (\neg(s \land t) \lor \text{false}) \\
&\equiv (\neg p \lor r) \land q \land (p \lor \neg q) \land (\neg q \lor t) \land (\neg p \lor \neg r \lor s) \land (\neg s \lor t) \land (\neg s \lor \neg t)
\end{aligned}
$$

2. Mögliche Resolution:



Info

Sowohl mit DPLL als auch mit Resolution kann man entscheiden, ob eine KNF-Formel F erfüllbar oder unerfüllbar ist.

- DPLL ist besser geeignet, um F auf Erfüllbarkeit zu testen (effizient und liefert erfüllende Belegung).
- Resolution ist besser geeignet, um F auf Unerfüllbarkeit zu testen (effizient und liefert einen Beweis).

Themenübersicht

Ein Kalkül für Inferenzen

Im Kalkül des natürlichen Schließens benutzen wir Inferenzregeln, um Aussagen der Form

$$A_1 \wedge \ldots \wedge A_n \vdash F$$

zu beweisen. Die Formeln $A_1, \ldots, A_n$ werden Annahmen genannt.

$A_1, \ldots, A_n \models F$ bedeutet:

„Wenn $A_1, \ldots, A_n$ alle wahr sind, dann auch F“.

$A_1, \ldots, A_n \vdash F$ bedeutet dagegen:

„Aus den Annahmen $A_1, \ldots, A_n$ lässt sich F mit den Inferenzregeln ableiten“.

Es wird gelten:

$$A_1, \ldots, A_n \models F \iff A_1, \ldots, A_n \vdash F$$

Infos

- $\vdash$ ist, wie $\models$ und $\equiv$, nichts anderes als eine Relation über aussagenlogische Formeln. Sie heißt Ableitungsrelation.
- Auch hier ist es üblich, dass man $A_1 \wedge \ldots \wedge A_n \vdash F$ zu

$$A_1, \ldots, A_n \vdash F \quad \text{oder} \quad \{A_1, \ldots, A_n\} \vdash F$$

umschreibt.

Graphische Darstellung der Inferenzregeln

Die Inferenzregeln haben die Form:

$$\frac{\ldots \vdash \ldots \qquad \ldots \vdash \ldots \qquad \ldots \qquad \ldots \vdash \ldots}{\ldots \vdash \ldots}$$

Dabei stehen die Prämissen oberhalb des Folgerungsstrichs und die Folgerung unterhalb.
Intuitiv heißt das:

> *„Um die Aussage unter dem Strich zu zeigen, reicht es alle Aussagen über dem Strich (getrennt voneinander) zu zeigen."*

Wichtig!

Die Regeln sind syntaktische Regeln! Man darf hier keine Äquivalenzumformungen machen.
Siehe hierzu die „Achtung!“-Blöcke bei den nächsten Beispielen.

Erstes Beispiel (Konjunktionseinführung)

Für beliebige Formeln $A_1, \ldots, A_n$, F und G gilt die Regel:

$$\frac{A_1, \ldots, A_n \vdash F \qquad A_1, \ldots, A_n \vdash G}{A_1, \ldots, A_n \vdash (F \wedge G)}$$

Intuitiv heißt das:

> *„Um zu zeigen, dass sich aus den Annahmen $A_1, \ldots, A_n$ die Formel $F \wedge G$ ableiten lässt, zeige dass sich aus denselben Annahmen $A_1, \ldots, A_n$ die Formeln F und G getrennt voneinander ableiten lassen.“*

Achtung!

Wenn die untere Formel keine Konjunktion ist (also kein „$\wedge$“ dazwischen hat), dann ist diese Regel nicht anwendbar!

Zweites Beispiel (Implikationsbeseitigung)

Für beliebige Formeln $A_1, \ldots, A_n, F, G$ gilt die Regel:

$$\frac{A_1, \ldots, A_n \vdash F \to G \qquad A_1, \ldots, A_n \vdash F}{A_1, \ldots, A_n \vdash G}$$

Intuitiv heißt das:

> *„Um zu zeigen, dass sich aus den Annahmen $A_1, \ldots, A_n$ eine Formel G ableiten lässt, zeige dass sich aus denselben Annahmen $A_1, \ldots, A_n$ sowohl die Implikation $F \to G$ als auch die Formel F ableiten lässt.“*

Infos

- Hier darf G beliebig sein! Diese Regel ist also immer anwendbar! :-)
- Der lateinische Name der Implikationsbeseitigung ist *Modus Ponens*.

Drittes Beispiel (Negationseinführung)

Für beliebige Formeln $A_1, \ldots, A_n, F$ gilt die Regel:

$$\frac{A_1, \ldots, A_n, F \vdash \text{false}}{A_1, \ldots, A_n \vdash \neg F}$$

Intuitiv heißt das:

> *„Um zu zeigen, dass sich aus den Annahmen $A_1, \ldots, A_n$ die Negation $\neg F$ ableiten lässt, zeige dass sich aus den neuen Annahmen $A_1, \ldots, A_n, F$ ein Widerspruch (*false*) ableiten lässt.“*

Achtung!

Wenn die untere Formel keine Negation ist (also kein „¬“ davor hat), dann ist diese Regel nicht anwendbar!

Viertes Beispiel (Annahmeregeln)

Für beliebige Formeln $A_1, \ldots, A_n$ gelten die Regeln:

$$\frac{}{A_1, \ldots, A_n \vdash A_1} \quad , \quad \frac{}{A_1, \ldots, A_n \vdash A_2} \quad , \quad \cdots \quad , \quad \frac{}{A_1, \ldots, A_n \vdash A_n}$$

Intuitiv heißt das:

> *„Um zu zeigen, dass sich aus den Annahmen $A_1, \ldots, A_n$ eine beliebige Annahme ableiten lässt, muss nichts gezeigt werden.“*

Achtung!

Die Annahme auf der rechten Seite von „$\vdash$“ muss syntaktisch gleich auf der linken Seite vorkommen. Semantisch äquivalent reicht nicht!

Fünftes Beispiel (Regel für false)

Für beliebige Formeln $A_1, \ldots, A_n$ und F gilt die Regel:

$$\frac{A_1, \ldots, A_n \vdash F \qquad A_1, \ldots, A_n \vdash \neg F}{A_1, \ldots, A_n \vdash \text{false}}$$

Intuitiv heißt das:

> *„Um zu zeigen, dass sich aus den Annahmen $A_1, \ldots, A_n$ ein Widerspruch* false *ableiten lässt, zeige dass sich aus denselben Annahmen $A_1, \ldots, A_n$ sowohl eine Formel F als auch ihre Negation $\neg F$ ableiten lässt.“*

Achtung!

Wenn die untere Formel nicht genau „false“ ist, sondern z.B. $F \wedge \neg F$, dann ist diese Regel nicht anwendbar!

Überblick Inferenzregeln

Für beliebige Formeln $A_1, \ldots, A_n$, F, G und H gelten folgende Regeln.

1. Annahmeregeln („AR“):

$$\frac{}{A_1, \ldots, A_n \vdash A_i} \qquad \text{für alle } i = 1, \ldots, n$$

2. Ausgeschlossener Dritte („AD“):

$$\frac{}{A_1, \ldots, A_n \vdash (F \vee \neg F)}$$

3. Regel für true („true“):

$$\frac{}{A_1, \ldots, A_n \vdash \text{true}}$$

4. Regel für false („false“):

$$\frac{A_1, \ldots, A_n \vdash F \qquad A_1, \ldots, A_n \vdash \neg F}{A_1, \ldots, A_n \vdash \text{false}}$$

Überblick Inferenzregeln

5. Konjunktionseinführung („$+\wedge$“):

$$\frac{A_1, \ldots, A_n \vdash F \qquad A_1, \ldots, A_n \vdash G}{A_1, \ldots, A_n \vdash (F \wedge G)}$$

6. Konjunktionsbeseitigung („$-\wedge$“):

$$\frac{A_1, \ldots, A_n \vdash (F \wedge G)}{A_1, \ldots, A_n \vdash F} \quad \text{und} \quad \frac{A_1, \ldots, A_n \vdash (F \wedge G)}{A_1, \ldots, A_n \vdash G}$$

7. Disjunktionseinführung („$+\vee$“):

$$\frac{A_1, \ldots, A_n \vdash F}{A_1, \ldots, A_n \vdash (F \vee G)} \quad \text{und} \quad \frac{A_1, \ldots, A_n \vdash F}{A_1, \ldots, A_n \vdash (G \vee F)}$$

8. Disjunktionsbeseitigung („$-\vee$“):

$$\frac{A_1, \ldots, A_n \vdash (F \vee G) \qquad A_1, \ldots, A_n, F \vdash H \qquad A_1, \ldots, A_n, G \vdash H}{A_1, \ldots, A_n \vdash H}$$

Überblick Inferenzregeln

9. Negationseinführung („$+\neg$“):

$$\frac{A_1, \ldots, A_n, F \vdash \text{false}}{A_1, \ldots, A_n \vdash \neg F}$$

10. Negationsbeseitigung („$-\neg$“):

$$\frac{A_1, \ldots, A_n, \neg F \vdash \text{false}}{A_1, \ldots, A_n \vdash F}$$

11. Implikationseinführung („$+ \to$“):

$$\frac{A_1, \ldots, A_n, F \vdash G}{A_1, \ldots, A_n \vdash (F \to G)}$$

12. Implikationsbeseitigung („$- \to$“) bzw. Modus Ponens („MP“):

$$\frac{A_1, \ldots, A_n \vdash (F \to G) \qquad A_1, \ldots, A_n \vdash F}{A_1, \ldots, A_n \vdash G}$$

Beispiel

Beweis, dass die Formel $(p \wedge q) \rightarrow (p \vee q)$ gültig ist:

1.	$p \wedge q$	$\vdash$	$p \wedge q$	(AR)
2.	$p \wedge q$	$\vdash$	p	$(- \wedge$ auf 1.)
3.	$p \wedge q$	$\vdash$	$p \vee q$	$(+ \vee$ auf 2.)
4.		$\vdash$	$(p \wedge q) \rightarrow (p \vee q)$	$(+ \rightarrow$ auf 3.)

Info

Man kann solche Beweise als Liste oder als Baum darstellen. Wenn man sie als Liste darstellt muss man explizit angeben auf welche Formel man die Regeln anwendet.

Wie kann man mit dem Kalkül des natürlichen Schließens beweisen, dass die Formel

$$p \to (q \to p)$$

gültig ist?

Beweis:

1.	p, q	$\vdash$	p	(AR)
2.	p	$\vdash$	$q \to p$	$(+\to$ auf 1.)
3.		$\vdash$	$p \to (q \to p)$	$(+\to$ auf 2.)

Quizfrage

Gegeben sei folgender Beweis, dass $((p \to q) \land p) \to q$ gültig ist:

1.	$(p \to q) \land p$	$\vdash$	$(p \to q) \land p$
2.	$(p \to q) \land p$	$\vdash$	$p \to q$
3.	$(p \to q) \land p$	$\vdash$	p
4.	$(p \to q) \land p$	$\vdash$	q
5.		$\vdash$	$((p \to q) \land p) \to q$

Welche Regel wurde bei jedem Schritt benutzt?

Schreibe zu jedem Schritt dazu auf welche vorangegangenen Formeln die angewandte Regel sich bezieht.

1.	$(p \to q) \land p$	$\vdash$	$(p \to q) \land p$	(AR)
2.	$(p \to q) \land p$	$\vdash$	$p \to q$	$(- \land$ auf 1.)
3.	$(p \to q) \land p$	$\vdash$	p	$(- \land$ auf 1.)
4.	$(p \to q) \land p$	$\vdash$	q	$(- \to$ auf 2. und 3.)
5.		$\vdash$	$((p \to q) \land p) \to q$	$(+ \to$ auf 4.)

Quizfrage

Gegeben sei folgender Beweis, dass $(p \to (q \to r)) \to (p \to q) \to (p \to r)$ gültig ist:

1.	$p \to (q \to r), p \to q, p$	$\vdash$	p
2.	$p \to (q \to r), p \to q, p$	$\vdash$	$p \to (q \to r)$
3.	$p \to (q \to r), p \to q, p$	$\vdash$	$p \to q$
4.	$p \to (q \to r), p \to q, p$	$\vdash$	q
5.	$p \to (q \to r), p \to q, p$	$\vdash$	$q \to r$
6.	$p \to (q \to r), p \to q, p$	$\vdash$	r
7.	$p \to (q \to r), p \to q$	$\vdash$	$p \to r$
8.	$p \to (q \to r)$	$\vdash$	$(p \to q) \to (p \to r)$
9.		$\vdash$	$(p \to (q \to r)) \to (p \to q) \to (p \to r)$

Welche Regel wurde bei jedem Schritt benutzt?

Schreibe zu jedem Schritt dazu auf welche vorangegangenen Formeln die angewandte Regel sich bezieht.

1.	$p \to (q \to r), p \to q, p$	$\vdash$	p	(AR)
2.	$p \to (q \to r), p \to q, p$	$\vdash$	$p \to (q \to r)$	(AR)
3.	$p \to (q \to r), p \to q, p$	$\vdash$	$p \to q$	(AR)
4.	$p \to (q \to r), p \to q, p$	$\vdash$	q	$(- \to$ auf 1. und 3.)
5.	$p \to (q \to r), p \to q, p$	$\vdash$	$q \to r$	$(- \to$ auf 1. und 2.)
6.	$p \to (q \to r), p \to q, p$	$\vdash$	r	$(- \to$ auf 4. 5.)
7.	$p \to (q \to r), p \to q$	$\vdash$	$p \to r$	$(+ \to$ auf 6.)
8.	$p \to (q \to r)$	$\vdash$	$(p \to q) \to (p \to r)$	$(+ \to$ auf 7.)
9.		$\vdash$	$(p \to (q \to r)) \to (p \to q) \to (p \to r)$	$(+ \to$ auf 8.)

Infos

- Ein Kalkül heißt korrekt, falls gilt:

$$A_1, \ldots, A_n \vdash F \quad \Longrightarrow \quad A_1, \ldots, A_n \models F.$$

- Ein Kalkül heißt vollständig, falls gilt:

$$A_1, \ldots, A_n \models F \quad \Longrightarrow \quad A_1, \ldots, A_n \vdash F.$$

- Der Kalkül des natürlichen Schließens ist in der Aussagenlogik sowohl korrekt als auch vollständig. Es gilt:

$$F \vdash G \quad \Longleftrightarrow \quad F \models G \quad \Longleftrightarrow \quad (F \to G) \text{ ist gültig.}$$

- Wenn die Gefahr besteht, dass man den Kalkül des natürlichen Schließens mit einem anderen verwechselt, benutzt man z.B. auch „$\vdash_{\mathsf{Nat}}$“, statt nur „$\vdash$“.
- Auf Folie 686 sind wichtige Aussagen zu $\models$ und $\vdash$ aufgelistet.

Frege-Lukasiewicz-Kalkül

Im Frege-Lukasiewicz-Kalkül (kurz FL-Kalkül) sind nur die logischen Junktoren $\to$ und $\neg$ erlaubt. Für beliebige Formeln $A_1, \ldots, A_n$, F, G und H gelten folgende fünf Inferenzregeln.

1. Annahmeregeln („AR“):

$$\frac{}{A_1, \ldots, A_n \vdash_{\mathsf{FL}} A_i} \qquad \text{für alle } i = 1, \ldots, n$$

2. Axiom 1 („Ax1“):

$$\frac{}{A_1, \ldots, A_n \vdash_{\mathsf{FL}} (F \to (G \to F))}$$

3. Axiom 2 („Ax2“):

$$\frac{}{A_1, \ldots, A_n \vdash_{\mathsf{FL}} ((F \to (G \to H)) \to ((F \to G) \to (F \to H)))}$$

4. Axiom 3 („Ax3“):

$$\frac{}{A_1, \ldots, A_n \vdash_{\mathsf{FL}} ((\neg F \to \neg G) \to (G \to F))}$$

5. Implikationsbeseitigung („$- \to$“) bzw. Modus Ponens („MP“):

$$\frac{A_1, \ldots, A_n \vdash_{\mathsf{FL}} F \to G \qquad A_1, \ldots, A_n \vdash_{\mathsf{FL}} F}{A_1, \ldots, A_n \vdash_{\mathsf{FL}} G}$$

Wichtig!

Der FL-Kalkül gehört nicht zum normalen DS-Stoff. Er ist auf diesen Folien, weil er im Wintersemester 13/14 in einer Aufgabe vorkam. Falls es dieses Semester nicht der Fall ist, kann er ignoriert werden :-)

Themenübersicht

Syntax prädikatenlogischer Formeln

1. Jede Variable und jede Konstante ist ein Term.
2. Sind $t_1, \ldots, t_n$ Terme und f ein n-äres Funktionensymbol, dann ist $f(t_1, \ldots, t_n)$ ebenfalls ein Term.
3. Sind $t_1, \ldots, t_n$ Terme und P ein n-äres Prädikatensymbol, dann ist $P(t_1, \ldots, t_n)$ eine Formel.
4. Sind t und u Terme, dann ist $t = u$ eine Formel.
5. Ist F eine Formel, dann ist auch $\neg F$ eine Formel.
6. Sind F und G Formeln, dann sind auch $(F \wedge G)$, $(F \vee G)$, $(F \rightarrow G)$, $(F \leftrightarrow G)$, $(F \oplus G)$, $(F \barwedge G)$ und $(F \barvee G)$ Formeln
7. Ist x eine Variable und F eine Formel, dann sind $\forall x F$ und $\exists x F$ ebenfalls Formeln.

Infos

- Wir gehen davon aus, dass jedes Symbol entweder als Variable, Konstante, Funktionen- oder Prädikatensymbol benutzt wird und niemals als zwei Sachen gleichzeitig.
- Für Variablen benutzen wir meistens x, y, z, für Konstanten a, b, c, als Funktionensymbole f, g, h und als Prädikatensymbole P, Q, R.
- Der Gültigkeitsbereich eines Vorkommens einer Variablen x in einer Formel F ist die kleinste Unterformel von F der Gestalt $\forall x G$ oder $\exists x G$, welche das Vorkommen enthält. In diesem Fall nennt man x gebunden.
- Wenn es diese Unterformel nicht gibt, dann ist der Gültigkeitsbereich die Formel F selbst und wir nennen x frei.
- Eine Formel ohne freie Variablen heißt geschlossen.
- Eine Formel, in der keine Variable sowohl gebunden als auch frei vorkommt, und hinter allen vorkommenden Quantoren verschiedene Variablen stehen, heißt bereinigt.
- Durch Umbenennung der Variablen kann man jede Formel bereinigen :-)

Strukturen

Eine Struktur $S = (U, I)$ besteht aus einer Menge U (das Universum) und einer partiellen Funktion I (die Interpretation), die:

- einer Variablen x ein Element aus U,
- einer Konstanten a ein Element U,
- einem k-stelligen Prädikatensymbol P eine Menge aus U^k und
- einem k-stelligen Funktionensymbol f eine Funktion $U^k \to U$

zuordnet. Wir sagen, dass $I(x)$, $I(a)$, $I(P)$ und $I(f)$ die Interpretationen von x, a, P und f unter S sind.

Eine Struktur $S = (U, I)$ passt zu einer Formel F, falls die Interpretation I für alle in F vorkommenden freien Variablen, Konstanten, Funktionen- und Prädikatensymbole definiert ist.

Infos

- Das Universum U einer Struktur S kann endlich oder unendlich sein, aber nicht leer!
- Unäre und binäre Prädikatensymbole lassen sich sehr schön modellieren:

Arität des Prädikatensymbols	graphische Darstellung	Intuition
unär (z.B. $P(x)$)	als Venn-Diagramm	„x hat die Eigenschaft“ „x ist in der Menge enthalten“
binär (z.B. $P(x, y)$)	als Graph einer Relation	„x zeigt auf y“ „x steht mit y in Relation“

- Die Interpretation von Funktionen- und Prädikatensymbolen kann man sowohl intensional als auch extensional angeben.

Semantik prädikatenlogischer Formeln

Die Semantik einer Formel F ist eine Funktion $[F]$, die jeder Struktur S, die zu F passt, einen Wert $[F](S)$ aus $\mathbb{B} = \{0, 1\}$ zuordnet.

Für alle Strukturen $S = (U, I)$ gilt folgende induktive Definition:

1. Sind $t_1, \ldots, t_n$ Terme und P ein Prädikatensymbol, dann gilt:

$$[P(t_1, \ldots, t_n)](S) \quad = \quad \begin{cases} 1, & \text{falls } (I(t_1), \ldots, I(t_n)) \in I(P) \\ 0, & \text{sonst} \end{cases}.$$

2. Sind t und u Terme, dann gilt:

$$[t = u](S) \quad = \quad \begin{cases} 1 & \text{falls } I(t) = I(u) \\ 0 & \text{sonst} \end{cases}.$$

Semantik prädikatenlogischer Formeln

3. Sind $[F]$ und $[G]$ die Semantiken zweier Formeln F und G, dann sind die Semantiken von $(F \wedge G)$, $(F \vee G)$, $(F \to G)$, $(F \leftrightarrow G)$, $(F \oplus G)$, $(F \barwedge G)$ und $(F \barvee G)$ analog zur Aussagenlogik definiert, z.B.:

$$[F \wedge G](S) \quad = \quad \begin{cases} 1 & \text{falls } [F](S) = 1 \text{ und } [G](S) = 1 \\ 0 & \text{sonst} \end{cases}.$$

4. Ist x eine Variable, G eine Formel und $S_{x:=d}$ die Struktur S mit dem einzigen Unterschied $x_{S_{x:=d}} = d$, dann gilt:

$$[\exists x G](S) \quad = \quad \begin{cases} 1 & \text{falls es ein } d \in U \text{ gibt mit: } [G](S_{x:=d}) = 1 \\ 0 & \text{sonst} \end{cases}.$$

$$[\forall x G](S) \quad = \quad \begin{cases} 1 & \text{falls für jedes } d \in U \text{ gilt: } [G](S_{x:=d}) = 1 \\ 0 & \text{sonst} \end{cases}.$$

Eigenschaften prädikatenlogischer Formeln

Die Begriffe erfüllbar, gültig, unerfüllbar, falsifizierbar, Tautologie und Widerspruch werden für prädikatenlogische Formeln analog definiert wie in der Aussagenlogik. Man muss nur auf Folie 554 das Wort „Belegung“ durch „Struktur“ ersetzen.

Infos

- Auch hier gelten die Beziehungen aus Folie 558.
- Eine Struktur S mit $[F](S) = 1$ wird Modell von F genannt.

Beispiel

In der Formel $F = \overbrace{\forall x \exists y P(x,y)}^{1.} \wedge \overbrace{\exists y \forall x \neg P(x,y)}^{2.} \wedge \overbrace{\forall x \neg P(x,x)}^{3.}$

kann P als Relation interpretiert werden, für die folgendes gelten muss:

1. Für jedes Element x gibt es ein Element y, so dass x auf y zeigt.
2. Es gibt ein Element y, so dass für alle Elemente x gilt: x zeigt nicht auf y.
3. Für alle Elemente x gilt: x zeigt nicht auf sich selbst.

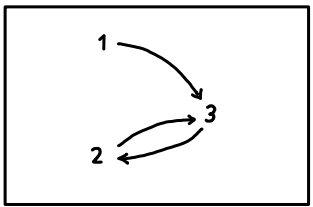
Kürzer:

1. Jedes Element x zeigt auf mindestens ein Element y.
2. Es gibt ein Element y, auf das kein Element x zeigt.
3. Kein Element x zeigt auf sich selbst.

Beispiel

Gesucht ist eine Struktur $S = (U, I)$, die F erfüllt.

Graphisch:



Formal: $U = \{1, 2, 3\}$ mit

$$I(P) = \{(1, 3), (2, 3), (3, 2)\}\,.$$

Noch ein Beispiel

Sei $S = (U, I)$ eine Struktur mit der Menge

$$U = \{\text{Asterix}, \text{Obelix}, \text{Miraculix}, \text{Troubadix}, \text{Majestix}, \ldots\}$$

aller Bewohner eines bekannten Dorfes in Gallien und

$$I(P) = \{(x, y) \mid x \text{ schlägt } y\}$$

die (in diesem Dorf) natürlichste Interpretation eines binären Prädikats P.

Noch ein Beispiel

Was sagen folgende Formeln aus?

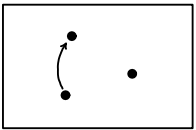
$$\exists x \exists y P(x,y), \quad \exists y \exists x P(x,y), \quad \exists x \exists y \neg P(x,y), \quad \exists y \exists x \neg P(x,y),$$
$$\exists x \forall y P(x,y), \quad \exists y \forall x P(x,y), \quad \exists x \forall y \neg P(x,y), \quad \exists y \forall x \neg P(x,y),$$
$$\forall x \exists y P(x,y), \quad \forall y \exists x P(x,y), \quad \forall x \exists y \neg P(x,y), \quad \forall y \exists x \neg P(x,y),$$
$$\forall x \forall y P(x,y), \quad \forall y \forall x P(x,y), \quad \forall x \forall y \neg P(x,y), \quad \forall y \forall x \neg P(x,y).$$

Noch ein Beispiel

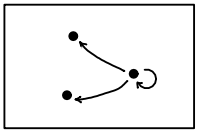
$\exists x \exists y P(x, y)$:	Jemand schlägt jemanden.
$\exists x \forall y P(x, y)$:	Jemand schlägt jeden.
$\forall x \exists y P(x, y)$:	Jeder schlägt jemanden.
$\forall x \forall y P(x, y)$:	Jeder schlägt jeden.
$\exists y \exists x P(x, y)$:	Jemand wird von jemandem geschlagen.
$\exists y \forall x P(x, y)$:	Jemand wird von jedem geschlagen.
$\forall y \exists x P(x, y)$:	Jeder wird von jemandem geschlagen.
$\forall y \forall x P(x, y)$:	Jeder wird von jedem geschlagen.
$\exists x \exists y \neg P(x, y)$:	Jemand schlägt jemanden nicht.
$\exists x \forall y \neg P(x, y)$:	Jemand schlägt niemanden.
$\forall x \exists y \neg P(x, y)$:	Jeder schlägt jemanden nicht.
$\forall x \forall y \neg P(x, y)$:	Niemand schlägt jemanden.
$\exists y \exists x \neg P(x, y)$:	Jemand wird von jemandem nicht geschlagen.
$\exists y \forall x \neg P(x, y)$:	Jemand wird von niemandem geschlagen.
$\forall y \exists x \neg P(x, y)$:	Jeder wird von jemandem nicht geschlagen.
$\forall y \forall x \neg P(x, y)$:	Niemand wird von jemandem geschlagen.

Noch ein Beispiel

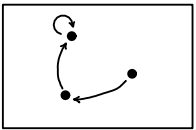
Mögliche Modelle für ein dreielementiges Universum hätten folgende Interpretationen von P.



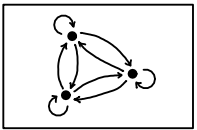
$\exists x \exists y P(x, y)$



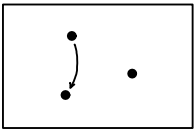
$\exists x \forall y P(x, y)$



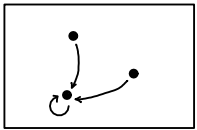
$\forall x \exists y P(x, y)$



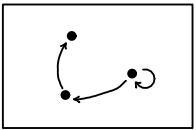
$\forall x \forall y P(x, y)$



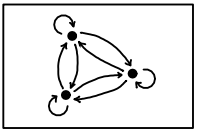
$\exists y \exists x P(x, y)$



$\exists y \forall x P(x, y)$

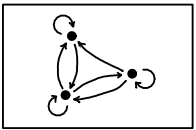


$\forall y \exists x P(x, y)$

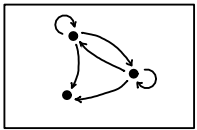


$\forall y \forall x P(x, y)$

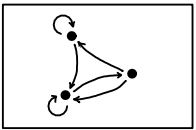
Noch ein Beispiel



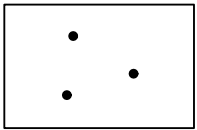
$\exists x \exists y \neg P(x, y)$



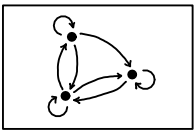
$\exists x \forall y \neg P(x, y)$



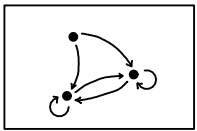
$\forall x \exists y \neg P(x, y)$



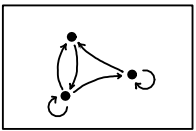
$\forall x \forall y \neg P(x, y)$



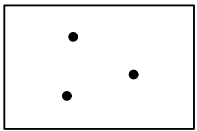
$\exists y \exists x \neg P(x, y)$



$\exists y \forall x \neg P(x, y)$



$\forall y \exists x \neg P(x, y)$



$\forall y \forall x \neg P(x, y)$

Infos

- Dass x und y unterschiedliche Variablennamen haben, heißt nicht, dass sie immer auf unterschiedliche Elemente zeigen. Wenn im Beispiel jeder jeden schlägt, dann muss sich auch jeder selber schlagen.
- Die Übersetzung von Prädikatenlogik ins Deutsche ist sehr schwierig! Bestimmt habe ich im Beispiel einiges falsch formuliert.
- Unter

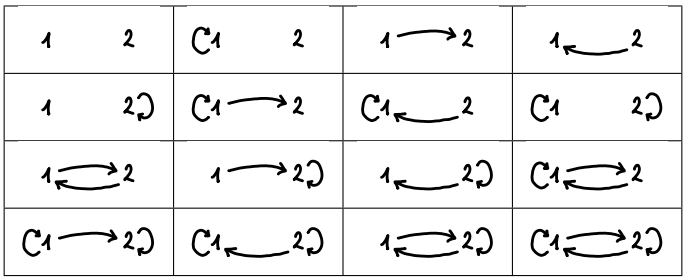
  `http://de.wikipedia.org/wiki/Quantor`

  findet ihr viele hilfreiche Beispiele, um Quantoren besser zu verstehen.

Wir betrachten die Formel

$$F = \forall x \exists y \neg P(x, y) \wedge \forall y \exists x P(x, y)$$

und eine zu F passende Struktur $S = (U, I)$ mit $U = \{1, 2\}$. Für welche der folgenden Interpretationen I von P ist S ein Modell für F?



Intuitiv besagt $\forall x \exists y \neg P(x, y)$, dass jedes Element auf mindestens ein Element nicht zeigt und $\forall y \exists x P(x, y)$, dass jedes Element von mindestens einem Element „gezeigt wird“.

Die einzigen Interpretationen von P, für die S ein Modell ist, sind:

$\{(1,1),(2,2)\}$ und $\{(1,2),(2,1)\}$

Themenübersicht

Logische Äquivalenz und Inferenz

Für beliebige Formeln F und G gilt:

$$F \equiv G \quad :\Longleftrightarrow \quad \text{(für alle passende Strukturen } S \text{ gilt: } [F](S) = 1 \iff [G](S) = 1)$$
$$F \models G \quad :\Longleftrightarrow \quad \text{(für alle passende Strukturen } S \text{ gilt: } [F](S) = 1 \implies [G](S) = 1)$$

Infos

- Auch hier sind $\equiv$ und $\models$ ist nichts anderes als Relationen über Formeln.
- Für $F \equiv G$ sagen wir „F und G sind äquivalent“.
- Für $F \models G$ sagen wir „G folgt aus F“.

Äquivalenz- und Folgerungsregeln für Quantoren

Seien F und G beliebige Formeln. Ein paar nützliche Äquivalenzregeln sind:

$\neg\forall x F \equiv \exists x \neg F$	$\neg\exists x F \equiv \forall x \neg F$	(De Morgan)
$\forall x \forall y F \equiv \forall y \forall x F$	$\exists x \exists y F \equiv \exists y \exists x F$	
$\exists x \forall y F \models \forall y \exists x F$		(Kommutativität)
$\forall x (F \wedge G) \equiv \forall x F \wedge \forall x G$	$\exists x (F \vee G) \equiv \exists x F \vee \exists x G$	
$\forall x F \vee \forall x G \models \forall x (F \vee G)$	$\exists x (F \wedge G) \models \exists x F \wedge \exists x G$	(Distributivität)
$\exists x (F \wedge G) \equiv \exists x F \wedge G$	$\exists x (F \vee G) \equiv \exists x F \vee G$	
$\forall x (F \wedge G) \equiv \forall x F \wedge G$	$\forall x (F \vee G) \equiv \forall x F \vee G$	(falls x in G nicht frei vorkommt)

Diese Regeln sind eine Erweiterung der Äquivalenzregeln für aussagenlogische Formeln (s. Folie 566).

Wichtige Aussagen zu Äquivalenzen

1. Für eine beliebige Formel F gilt:

$$\begin{array}{lcl} \text{die Formel } F \text{ ist gültig} & \iff & F \equiv \text{true} \\ \text{die Formel } F \text{ ist unerfüllbar} & \iff & F \equiv \text{false} \end{array}$$

2. Für zwei beliebige Formeln F und G gilt:

$$F \equiv G \iff \text{die Formel } (F \leftrightarrow G) \text{ ist gültig}$$

Inferenzregeln für Quantoren

Für beliebige Formeln $A_1, \ldots, A_n$, F, G und jede Konstante a gelten folgende Regeln:

13. Allquantoreinführung („$+\forall$“): Falls a nicht in $A_1, \ldots, A_n$ oder F vorkommt:

$$\frac{A_1, \ldots, A_n \vdash F[x \backslash a]}{A_1, \ldots, A_n \vdash \forall x F}$$

14. Allquantorbeseitigung („$-\forall$“):

$$\frac{A_1, \ldots, A_n \vdash \forall x F}{A_1, \ldots, A_n \vdash F[x \backslash a]}$$

15. Existenzquantoreinführung („$+\exists$“):

$$\frac{A_1, \ldots, A_n \vdash F[x \backslash a]}{A_1, \ldots, A_n \vdash \exists x F}$$

16. Existenzquantorbeseitigung („$-\exists$“): Falls a nicht in $A_1, \ldots, A_n$, F oder G vorkommt:

$$\frac{A_1, \ldots, A_n \vdash \exists x F \qquad A_1, \ldots, A_n, F[x \backslash a] \vdash G}{A_1, \ldots, A_n \vdash G}$$

Infos

- Die Inferenzregeln für Quantoren sind eine Erweiterung der Inferenzregeln von dem Kalkül des natürlichen Schließens aus Folie 645.
- Mit $F[x\backslash a]$ wird die Formel bezeichnet, die man erhält, wenn man in F alle freien Vorkommnisse von x durch a ersetzt.

Wichtige Aussagen zu Inferenzen

1. Für eine beliebige Formel F gilt:

$$\begin{array}{lcll} \text{die Formel } F \text{ ist gültig} & \iff & \text{true} \models F & \iff : \quad \models F \\ \text{die Formel } F \text{ ist unerfüllbar} & \iff & F \models \text{false} & \end{array}$$

2. Für zwei beliebige Formeln F und G gilt:

$$\begin{array}{lcl} F \models G & \iff & \text{die Formel } (F \to G) \text{ ist gültig} \\ F \equiv G & \iff & F \models G \text{ und } G \models F \end{array}$$

3. Für zwei aussagenlogische Formeln F und G gilt:

$$F \vdash G \quad \iff \quad F \models G$$

4. Für zwei prädikatenlogische Formeln F und G gilt:

$$F \vdash G \quad \Longrightarrow \quad F \models G$$

Themenübersicht

Themenübersicht

Produktregel

Die Kardinalität des kartesischen Produkts endlicher Mengen entspricht genau dem Produkt der einzelnen Kardinalitäten:

$$|A_1 \times \ldots \times A_n| = |A_1| \cdot \ldots \cdot |A_n|$$

Intuition

Sind wir an der Anzahl an Ausgängen eines mehrstufigen Experiments interessiert, dann multipliziert man die Anzahl an möglichen Ausgängen aller einzelnen Stufen.

- Zuerst: ... ($|A_1|$ Möglichkeiten)
- Dann: ... ($|A_2|$ Möglichkeiten)
- ...
- Dann: ... ($|A_n|$ Möglichkeiten)

Insgesamt hat man $|A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$ Möglichkeiten.

Wie viele verschiedene Anagramme besitzen folgende Wörter?

1. TITISEE,
2. PFEFFER,
3. KOKOMO,
4. CARACAS,
5. OUAGADOUGOU.

Info: Ein Anagramm ist ein Wort, das aus einem anderen Wort durch Umstellung der einzelnen Buchstaben gebildet wurde. Beispielsweise ist SPORT ein Anagramm von PROST.

Für jeden Buchstaben wählen wir sukzessiv die Teilmenge der freien Positionen im Wort, an dem der Buchstabe stehen soll. Mit der Produktregel erhalten wir:

1. $\binom{7}{2} \cdot \binom{5}{2} \cdot \binom{3}{2} \cdot \binom{1}{1} = \frac{7!}{2!\cdot 5!} \cdot \frac{5!}{2!\cdot 3!} \cdot \frac{3!}{2!\cdot 1!} \cdot \frac{1!}{1!\cdot 0!} = \frac{7!}{2!\cdot 2!\cdot 2!\cdot 1!} = 630.$
2. $\binom{7}{3} \cdot \binom{4}{2} \cdot \binom{2}{1} \cdot \binom{1}{1} = \frac{7!}{3!\cdot 4!} \cdot \frac{4!}{2!\cdot 2!} \cdot \frac{2!}{2!\cdot 1!} \cdot \frac{1!}{1!\cdot 0!} = \frac{7!}{3!\cdot 2!\cdot 1!\cdot 1!} = 420.$
3. $\binom{6}{3} \cdot \binom{3}{2} \cdot \binom{1}{1} = \frac{6!}{3!\cdot 3!} \cdot \frac{3!}{2!\cdot 1!} \cdot \frac{1!}{1!\cdot 0!} = \frac{6!}{3!\cdot 2!\cdot 1!} = 60.$
4. $\binom{7}{3} \cdot \binom{4}{2} \cdot \binom{2}{1} \cdot \binom{1}{1} = \frac{7!}{3!\cdot 4!} \cdot \frac{4!}{2!\cdot 2!} \cdot \frac{2!}{2!\cdot 1!} \cdot \frac{1!}{1!\cdot 0!} = \frac{7!}{3!\cdot 2!\cdot 1!\cdot 1!} = 420.$
5. $\binom{11}{3} \cdot \binom{8}{3} \cdot \binom{5}{2} \cdot \binom{3}{2} \cdot \binom{1}{1} = \frac{11!}{3!\cdot 8!} \cdot \frac{8!}{3!\cdot 5!} \cdot \frac{5!}{2!\cdot 3!} \cdot \frac{3!}{2!\cdot 1!} \cdot \frac{1!}{1!\cdot 0!} = \frac{11!}{3!\cdot 3!\cdot 2!\cdot 2!\cdot 1!} = 277200.$

Summenregel

Die Kardinalität einer disjunkten Vereinigung („$\uplus$“) endlicher Mengen entspricht genau der Summe der einzelnen Kardinalitäten:

$$|A_1 \uplus \ldots \uplus A_n| = |A_1| + \ldots + |A_n|$$

Intuition

Hat man mehrere mögliche Teilexperimente (die sich nicht überschneiden) zur Wahl, dann addiert man die Anzahl an möglichen Ausgängen aller einzelnen Teilexperimente.

- Entweder: ... ($|A_1|$ Möglichkeiten)
- oder: ... ($|A_2|$ Möglichkeiten)
- ...
- oder: ... ($|A_n|$ Möglichkeiten)

Insgesamt hat man $|A_1| + |A_2| + \ldots + |A_n|$ Möglichkeiten.

Gleichheitsregel

Existiert eine bijektive Funktion $f : A \to B$, dann haben die Mengen A und B gleich viele Elemente.

Doppeltes Abzählen

In jeder Matrix (Tabelle) ist die Summe der Zeilensummen gleich der Summe der Spaltensummen.

Beispiel

In einem Tanzkurs gibt es 24 Damen und n Herren. Nach der Tanzstunde hat jede Dame mit genau 8 Herren getanzt, jeder Herr mit genau 6 Damen.

Wie viele Herren waren anwesend?

Modellierung als Tabelle:

	d_1	d_2	$\cdots$	d_{24}
h_1	?	?	$\cdots$	?
h_2	?	?	$\cdots$	?
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
h_n	?	?	$\cdots$	?

Beispiel

Die Einträge „?“ in der Tabelle sind 1, fall das Paar miteinander getanzt hat und 0 sonst. Wir wissen:

- In jeder der n Zeilen gibt es genau 6 1en
- In jeder der 24 Spalten gibt es genau 8 1en

D.h.:

$$6 \cdot n = 24 \cdot 8 \ .$$

Daraus folgt:

$$n = \frac{24 \cdot 8}{6} = 32 \ .$$

Schubfachprinzip

Sei $f : X \to Y$ mit $0 < |Y| < |X| < \infty$. Dann gilt:

$$\exists y \in Y : |f^{-1}(y)| \geq 2$$

Intuition

X sind Objekte und Y Schubfächer für die Objekte. Hat man mehr Objekte als Schubfächer, dann existiert bei jeder Verteilung von Objekten auf Schubfächer immer mindestens ein Schubfach mit mindestens 2 Objekten.

Verallgemeinertes Schubfachprinzip

Sei $f : X \to Y$ mit $0 < |Y|, |X| < \infty$. Dann gilt:

$$\exists y \in Y : |f^{-1}(y)| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil$$

Wieder sind X Objekte und Y Schubfächer für die Objekte. Verteilt man alle Objekte auf die Schubfächer, dann hat man mindestens ein Schubfach mit mindestens $\left\lceil \frac{|X|}{|Y|} \right\rceil$ Objekten.

Zählen homogener Relationen

Sei $n \geq 1$. Wir betrachten homogene Relationen R über einer n-elementigen Menge A. Um die Anzahl an Relationen mit einer gegebenen Eigenschaften zu bestimmen, betrachtet man die Tabelle aus Folie 259:

Zählen homogener Relationen

Seien dann $l \in \{0, 1, 2\}$ die Anzahl der Häkchen (✓) in der linken Hälfte der Tabelle und $r \in \{0, 1, 2, 3, 4\}$ die Anzahl der Häkchen in der rechten Hälfte.

- Für jedes Element $a \in A$ müssen wir entscheiden, ob $(a, a) \in R$ oder $(a, a) \notin A$. Dafür gibt es genau l Möglichkeiten. Wegen $|A| = n$ gibt es hierfür nach der Produktregel insgesamt genau l^n Möglichkeiten.
- Für je zwei verschiedene Elemente $a, b \in A$ müssen wir entscheiden, ob $(a, b) \in R$ oder $(a, b) \notin A$ und ob $(b, a) \in R$ oder $(b, a) \notin A$. Dafür gibt es genau r Möglichkeiten. Weil es genau $\binom{n}{2}$ Paare unterschiedlicher Elemente aus A gibt, gibt es hierfür nach der Produktregel insgesamt genau $r^{\binom{n}{2}}$ Möglichkeiten.

Dann ist die gesuchte Anzahl an Relationen (wieder mit Produktregel) genau $l^n \cdot r^{\binom{n}{2}}$.

Erstes Beispiel

Wir wissen, dass es insgesamt 2^{n^2} Relationen gibt. Wir bestätigen das mit diesem super coolen Trick.

Erlaubt man alle Möglichkeiten, so erhält man mit $l = 2$ und $r = 4$:

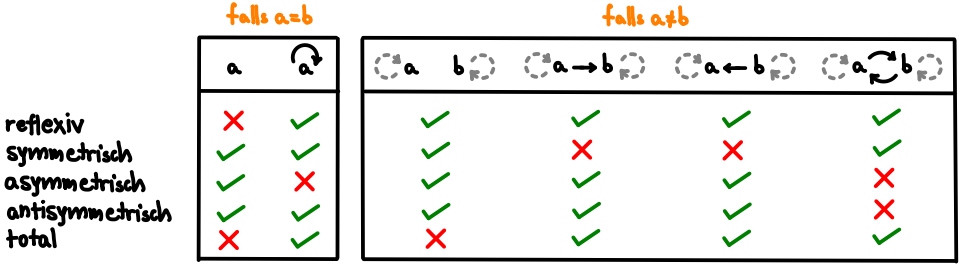
$$2^n \cdot 4^{\binom{n}{2}} = 2^n \cdot 2^{2\binom{n}{2}} = 2^n \cdot 2^{n(n-1)} = 2^n \cdot 2^{n^2-n} = 2^{n+n^2-n} = 2^{n^2}.$$

Zweites Beispiel

Die Anzahl an reflexiven Relationen ist genau

$$1^n \cdot 4^{\binom{n}{2}} = 4^{\binom{n}{2}} = 2^{2\binom{n}{2}} = 2^{2\binom{n}{2}} = 2^{n(n-1)}.$$

Erinnerung

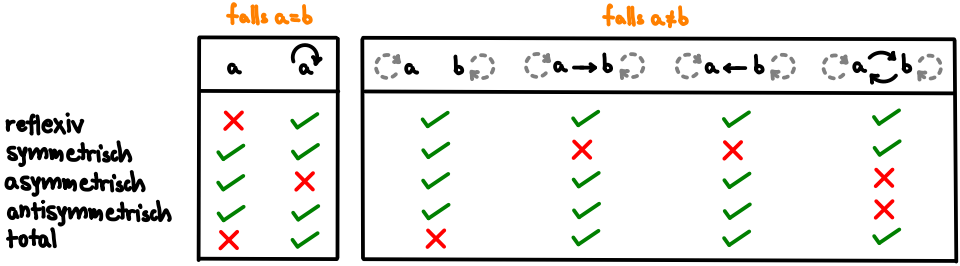

falls a=b
falls a≠b
a
a
a
b
a → b
a ← b
a
b
reflexiv
symmetrisch
asymmetrisch
antisymmetrisch
total

Drittes Beispiel

Die Anzahl an symmetrischen Relationen ist genau

$$2^n \cdot 2^{\binom{n}{2}} = 2^{n+\binom{n}{2}} = 2^{n(n+1)/2}.$$

Erinnerung

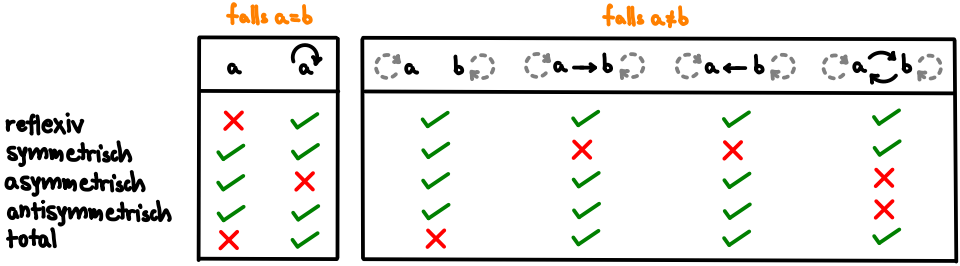

falls a=b
falls a≠b
a
a
a
b
a → b
a ← b
a
b
reflexiv
symmetrisch
asymmetrisch
antisymmetrisch
total

Viertes Beispiel

Die Anzahl an asymmetrischen Relationen ist genau

$$1^n \cdot 3^{\binom{n}{2}} = 3^{\binom{n}{2}}.$$

Erinnerung

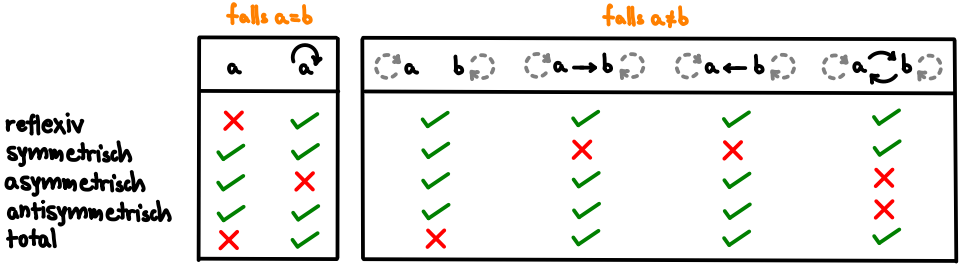

falls a=b
falls a≠b
a
a
a
b
a → b
a ← b
a
b
reflexiv
symmetrisch
asymmetrisch
antisymmetrisch
total

Fünftes Beispiel

Die Anzahl an antisymmetrischen Relationen ist genau

$$2^n \cdot 3^{\binom{n}{2}}.$$

Erinnerung

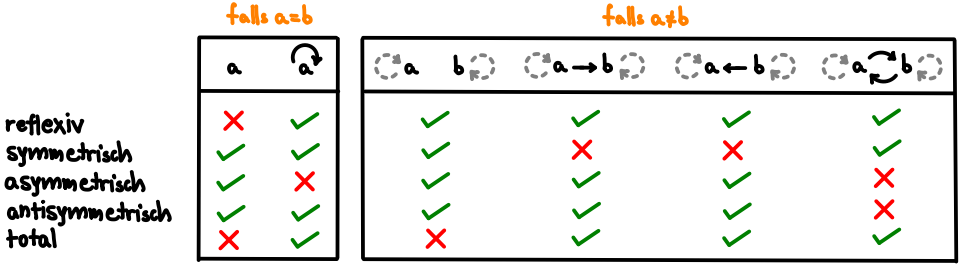

falls a=b
falls a≠b
a
a
a
b
a → b
a ← b
a
b
reflexiv
symmetrisch
asymmetrisch
antisymmetrisch
total

Sechstes Beispiel

Die Anzahl an totalen Relationen ist genau

$$1^n \cdot 3^{\binom{n}{2}} = 3^{\binom{n}{2}}.$$

Erinnerung


falls a=b
falls a≠b
a
a
a
b
a → b
a ← b
a
b
reflexiv
symmetrisch
asymmetrisch
antisymmetrisch
total

Transitive Relationen

Die schlechte Nachricht: Dieser Trick funktioniert leider nicht für transitive Relationen.

Die gute Nachricht: Das kann in der Klausur nicht abgefragt werden, weil für die Anzahl an transitiven Relationen noch keine abgeschlossene Formel bekannt ist ;-)

Sollte die Frage für ein kleines n doch vorkommen, dann kann das hier vielleicht helfen:

n:	0	1	2	3	4	$\cdots$
Anzahl:	1	2	13	171	3994	$\cdots$

Für Neugierige:

- `cs.uwaterloo.ca/journals/JIS/VOL7/Pfeiffer/pfeiffer6.pdf`
- `oeis.org/A006905`

Äquivalenzrelationen

Äquivalenzrelationen sind, wie transitive Relationen, auch schwer zu zählen. Wir wissen, dass es genau so viele Äquivalenzrelationen wie Partitionen der Grundmenge gibt, aber leider gibt es hierfür keine schöne Formel.

Sollte die Frage für ein kleines n doch vorkommen, dann kann das hier vielleicht helfen:

n:	0	1	2	3	4	5	6	7	8	$\cdots$
Anzahl:	1	1	2	5	15	52	203	877	4140	$\cdots$

Für Neugierige:

- `de.wikipedia.org/wiki/Bellsche_Zahl`
- `oeis.org/A000110`

Partielle Ordnungen

Hier ist es ähnlich wie bei Äquivalenzrelationen. Wir wissen, dass es genau so viele partielle Ordnungen wie Hasse-Diagramme gibt, aber wir haben keine Formel dafür.

Sollte die Frage für ein kleines n doch vorkommen, dann kann das hier vielleicht helfen:

n:	0	1	2	3	4	5	$\cdots$
Anzahl:	1	1	3	19	219	4231	$\cdots$

Für Neugierige:

- `oeis.org/A001035`

Totale Ordnungen

Bei totalen Ordnungen ist es wieder einfach. Wir wissen, dass es genau so viele totale Ordnungen wie Hasse-Diagramme gibt, die nur aus einem „Strang“ bestehen. Die Anzahl an totalen Ordnungen von n Elementen ist genau die Anzahl an Reihenfolgen für n Elementen, d.h.:

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1.$$

Sei M eine n-elementige Menge. Wie viele Relationen $R \subseteq M \times M$ gibt es, die antisymmetrisch und total sind?

Was ist für ein beliebiges $a \in M$ erlaubt?

- $(a, a) \in R$ ✓
- $(a, a) \notin R$ ✗

Es gilt also $I = 1$.

Was ist für beliebige aber verschiedene $a, b \in M$ erlaubt?

- $(a, b) \in R$ und $(b, a) \in R$ ✗
- $(a, b) \in R$ und $(b, a) \notin R$ ✓
- $(a, b) \notin R$ und $(b, a) \in R$ ✓
- $(a, b) \notin R$ und $(b, a) \notin R$ ✗

Es gilt also $r = 2$.

Die Anzahl solcher Relationen ist also genau

$$1^n \cdot 2^{\binom{n}{2}} = 2^{\binom{n}{2}}.$$

Noch eine Quizfrage

Sei M eine n-elementige Menge. Wie viele Relationen $R \subseteq M \times M$ gibt es, die symmetrisch und asymmetrisch sind?

Was ist für ein beliebiges $a \in M$ erlaubt?

- $(a, a) \in R$ ✗
- $(a, a) \notin R$ ✓

Es gilt also $I = 1$.

Was ist für beliebige aber verschiedene $a, b \in M$ erlaubt?

- $(a, b) \in R$ und $(b, a) \in R$ ✗
- $(a, b) \in R$ und $(b, a) \notin R$ ✗
- $(a, b) \notin R$ und $(b, a) \in R$ ✗
- $(a, b) \notin R$ und $(b, a) \notin R$ ✓

Es gilt also $r = 1$.

Die Anzahl solcher Relationen ist also genau

$$1^n \cdot 1^{\binom{n}{2}} = 1.$$

(Nur die leere Relation kann beide Eigenschaften haben)

Und noch eine Quizfrage

Sei M eine n-elementige Menge. Wie viele Relationen $R \subseteq M \times M$ gibt es, die asymmetrisch und total sind?

Was ist für ein beliebiges $a \in M$ erlaubt?

- $(a, a) \in R$ ✗
- $(a, a) \notin R$ ✗

Es gilt also $I = 0$.

Was ist für beliebige aber verschiedene $a, b \in M$ erlaubt?

- $(a, b) \in R$ und $(b, a) \in R$ ✗
- $(a, b) \in R$ und $(b, a) \notin R$ ✓
- $(a, b) \notin R$ und $(b, a) \in R$ ✓
- $(a, b) \notin R$ und $(b, a) \notin R$ ✗

Es gilt also $r = 2$.

Die Anzahl solcher Relationen ist also genau

$$0^n \cdot 2^{\binom{n}{2}} = 0.$$

(Keine Relation kann beide Eigenschaften haben)

Sei $n \in \mathbb{N}$. Wie viele Relationen $R \subseteq [n] \times [n]$ gibt es, die die Eigenschaft

$$\forall x, y \in [n] : (x, y) \in R \implies x < y \tag{4}$$

besitzen?

Hinweis: Intuitiv besagt (1), dass jedes Element nur zu einem größeren Element in Relation stehen darf (aber nicht muss).

Was ist für ein beliebiges $a \in [n]$ erlaubt?

- $(a, a) \in R$ ✗
- $(a, a) \notin R$ ✓

Es gilt also $l = 1$.

Was ist für beliebige aber verschiedene $a, b \in [n]$ erlaubt?

- $(a, b) \in R$ und $(b, a) \in R$ ✗
- $(a, b) \in R$ und $(b, a) \notin R$ ✓ (falls $a < b$) bzw. ✗ (falls $a > b$)
- $(a, b) \notin R$ und $(b, a) \in R$ ✗ (falls $a < b$) bzw. ✓ (falls $a > b$)
- $(a, b) \notin R$ und $(b, a) \notin R$ ✓

Es gilt also $r = 2$ (egal, ob $a < b$ oder $a > b$).

Die Anzahl solcher Relationen ist also genau

$$1^n \cdot 2^{\binom{n}{2}} = 2^{\binom{n}{2}}.$$

Themenübersicht

Multimengen

Multimengen sind eine Verallgemeinerung von Mengen, in denen Elemente öfter vorkommen dürfen. Die Reihenfolge der Elemente spielt dabei weiterhin keine Rolle.

Für Multimengen wird oft dieselbe Notation wie für Mengen benutzt, d.h. „$\{\ldots\}$“. Ich bevorzuge die (leider weniger verbreitete) Notation „$\{\!|\ldots|\!\}$“, da man mit ihr Multimengen von normalen Mengen sehr gut unterscheiden kann.

Beispielsweise gilt $\{\!|1,1,2,3,3,3|\!\} = \{\!|1,3,2,3,1,3|\!\}$, aber $\{\!|1,1,2,3,3,3|\!\} \neq \{\!|1,1,1,2,3,3|\!\}$.

Statt *k-elementige Multimenge über A* sagt man auch kurz *k-Multimenge über A* oder *k-Multiteilmenge von A*.

Beispiel

Es gibt 15 verschiedene 4-elementige Multimengen über [3]:

$$\{\!|1,1,1,1|\!\}, \{\!|1,1,1,2|\!\}, \{\!|1,1,1,3|\!\}, \{\!|1,1,2,2|\!\}, \{\!|1,1,2,3|\!\},$$
$$\{\!|1,1,3,3|\!\}, \{\!|1,2,2,2|\!\}, \{\!|1,2,2,3|\!\}, \{\!|1,2,3,3|\!\}, \{\!|1,3,3,3|\!\},$$
$$\{\!|2,2,2,2|\!\}, \{\!|2,2,2,3|\!\}, \{\!|2,2,3,3|\!\}, \{\!|2,3,3,3|\!\}, \{\!|3,3,3,3|\!\}.$$

Infos

- Formal ist eine Multimenge M über einer Menge A eine Abbildung $M\colon A \to \mathbb{N}_0$. $M(x)$ gibt für ein $x \in A$ an, wie oft x in M vorkommt.
- Eine k-elementige Multimenge über A ist eine Multimenge über A mit insgesamt k Elementen, d.h. mit $\sum_{x \in A} M(x) = k$.
- Die Multimengenklammern „$\{\!|\ldots|\!\}$“ sind nur eine intuitive und einfache Schreibweise! Für $A = [5]$ ist beispielsweise $M = \{\!|1, 1, 1, 2, 4, 5, 5|\!\}$ eine Schreibweise für die 7-elementige Multimenge $M = \{(1, 3), (2, 1), (3, 0), (4, 1), (5, 2)\}$.

Zählen von Multimengen

Man kann jede k-elementige Multimenge über einer n-elementigen Menge A (z.B. $A = [n]$) als Wort über dem Alphabet $\Sigma = \{\bullet, \circ\}$ mit genau k schwarzen und $n-1$ weißen Kugeln darstellen. Die weißen Kugeln teilen das Wort in n Bereichen auf. Die Anzahl an schwarzen Kugeln in jedem Bereich gibt die Anzahl an Vorkommnisse des entsprechenden Elements in der Multimenge an.

Jedem dieser Wörter kann genau eine der k-elementigen Teilmengen der Menge $[k+n-1]$ zugeordnet werden. Intuitiv gibt die jeweilige Teilmenge an, welche der $k+n-1$ Kugeln schwarz sind.

Man kann also jeder k-elementigen Multimenge über $A = [n]$ genau einer der k-elementigen Teilmengen der Menge $[k+n-1]$ zuordnen. Es folgt, dass es genau $\binom{k+n-1}{k}$ k-elementige Multimengen einer n-elementigen Menge gibt.

Beispiel

Wir betrachten folgende Multimenge mit $k = 7$ Elementen über $A = [n]$ mit $n = 4$:

$$\{\!|1, 1, 2, 3, 3, 3, 4|\!\} \ .$$

Diese Multimenge wird durch folgendes Wort der Länge $k + n - 1 = 10$ kodiert:

$$\bullet\bullet\circ\bullet\circ\bullet\bullet\bullet\circ\bullet \, .$$

Diesem Wort kann folgende 7-elementige Teilmenge von $[10]$ eindeutig zugeordnet werden:

$$\{1, 2, 4, 6, 7, 8, 10\} \, .$$

Noch ein Beispiel

Es gibt $\binom{2+3-1}{2} = \binom{4}{2} = 6$ verschiedene 2-elementige Multimengen über [3]:

Multimenge über A	Kodierung	Teilmenge von [4]
$\{\!\{1,1\}\!\}$	$\bullet\bullet\circ\circ$	$\{1,2\}$
$\{\!\{1,2\}\!\}$	$\bullet\circ\bullet\circ$	$\{1,3\}$
$\{\!\{1,3\}\!\}$	$\bullet\circ\circ\bullet$	$\{1,4\}$
$\{\!\{2,2\}\!\}$	$\circ\bullet\bullet\circ$	$\{2,3\}$
$\{\!\{2,3\}\!\}$	$\circ\bullet\circ\bullet$	$\{2,4\}$
$\{\!\{3,3\}\!\}$	$\circ\circ\bullet\bullet$	$\{3,4\}$

Ein letztes Beispiel

Es gibt $\binom{3+3-1}{3} = \binom{5}{3} = 10$ verschiedene 3-elementige Multimengen über $[3]$:

Multimenge über A	Kodierung	Teilmenge von $[5]$
$\{\!\{1,1,1\}\!\}$	● ● ● ○ ○	$\{1,2,3\}$
$\{\!\{1,1,2\}\!\}$	● ● ○ ● ○	$\{1,2,4\}$
$\{\!\{1,1,3\}\!\}$	● ● ○ ○ ●	$\{1,2,5\}$
$\{\!\{1,2,2\}\!\}$	● ○ ● ● ○	$\{1,3,4\}$
$\{\!\{1,2,3\}\!\}$	● ○ ● ○ ●	$\{1,3,5\}$
$\{\!\{1,3,3\}\!\}$	● ○ ○ ● ●	$\{1,4,5\}$
$\{\!\{2,2,2\}\!\}$	○ ● ● ● ○	$\{2,3,4\}$
$\{\!\{2,2,3\}\!\}$	○ ● ● ○ ●	$\{2,3,5\}$
$\{\!\{2,3,3\}\!\}$	○ ● ○ ● ●	$\{2,4,5\}$
$\{\!\{3,3,3\}\!\}$	○ ○ ● ● ●	$\{3,4,5\}$

Info

Für die Anzahl der k-elementigen Multimengen über einer n-elementigen Menge wird manchmal auch die Notation

$$\left(\!\binom{n}{k}\!\right) := \binom{k+n-1}{k}$$

verwendet.

Sei $\Sigma = \{a, b, c, \ldots, z\}$ ein Alphabet mit $|\Sigma| = 26$. Wie viele Wörter $w \in \Sigma^*$ mit Länge $|w| = 3$ gibt es, so dass die Zeichen in w von links nach rechts gelesen in alphabetischer Reihenfolge vorkommen, d.h. zuerst alle as, dann alle bs, etc. ?

Jedes dieser Wörter kann eindeutig durch eine 3-elementige Multimenge über Σ dargestellt werden. Da die Reihenfolge sich automatisch aus den Elementen selber ergibt muss man sie nicht berücksichtigen. Beispielsweise stellt die Multimenge $\{\!|a, c, a|\!\}$ eindeutig das Wort *aac* dar.

Demnach ist die Anzahl solcher Wörter genau die Anzahl der 3-elementigen Multimengen über Σ, d.h.:

$$\left(\!\binom{26}{3}\!\right) = \binom{3+26-1}{3} = \binom{28}{3} = \frac{28 \cdot 27 \cdot 26}{3 \cdot 2 \cdot 1} = 3276.$$

Themenübersicht

Binomialkoeffizient

Seien $k, n \in \mathbb{N}_0$ beliebig. $\binom{n}{k}$ gibt die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge an.

Intuitiv gibt $\binom{n}{k}$ die Anzahl der Möglichkeiten an, k Objekte aus einer Menge von n verschiedenen Objekten ohne Zurücklegen und ohne Beachtung der Reihenfolge auszuwählen.

Wie beim Lotto!

Beispiel

Es gibt genau 6 2-elementige Teilmengen von [4]:

$$\{1,2\} \ , \ \{1,3\} \ , \ \{1,4\} \ , \ \{2,3\} \ , \ \{2,4\} \ , \ \{3,4\} \ .$$

Es gilt: $\binom{4}{2} = 6$.

Noch ein Beispiel

Es gibt genau 10 3-elementige Teilmengen von $[5]$:

$$\{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \{1,3,4\}, \{1,3,5\},$$
$$\{1,4,5\}, \{2,3,4\}, \{2,3,5\}, \{2,4,5\}, \{3,4,5\}.$$

Also ist $\binom{5}{3} = 10$.

Ein letztes Beispiel (für Lotto-Spieler)

Es gibt genau 13 983 816 6-elementige Teilmengen von [49].

Also ist $\binom{49}{6} = 13\,983\,816$.

Direkte Berechnung

Für $k, n \in \mathbb{N}_0$ gilt:

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!}.$$

Gilt außerdem $k \leq n$, dann kann man $n^{\underline{k}} = \frac{n!}{(n-k)!}$ setzen und man erhält:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Intuition

Für die erste Ziehung gibt es n Möglichkeiten, für die zweite nur noch $n-1$, für die dritte $n-2$, etc. Weil die Reihenfolge der k gezogenen Elemente nicht relevant ist muss man durch die Anzahl der Permutationen aller k Elemente dividieren, also durch $k!$.

Beispiele (nochmal)

$$\binom{4}{2} = \frac{4^{\underline{2}}}{2!} = \frac{4 \cdot 3}{2 \cdot 1} = 6,$$

$$\binom{5}{3} = \frac{5^{\underline{3}}}{3!} = \frac{5 \cdot 4 \cdot 3}{3 \cdot 2 \cdot 1} = 10,$$

$$\binom{49}{6} = \frac{49^{\underline{6}}}{6!} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 13\,983\,816.$$

Quizfragen

1. Was ist $\binom{6}{2}$?
2. Was ist $\binom{7}{3}$?
3. Was ist $\binom{6}{3}$?
4. Was ist $\binom{8}{4}$?

Antworten

1. $\binom{6}{2} = \frac{6 \cdot 5}{2 \cdot 1} = 15$.
2. $\binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1} = 35$.
3. $\binom{6}{3} = \frac{6 \cdot 5 \cdot 4}{3 \cdot 2 \cdot 1} = 20$.
4. $\binom{8}{4} = \frac{8 \cdot 7 \cdot 6 \cdot 5}{4 \cdot 3 \cdot 2 \cdot 1} = 70$.

Rekursive Berechnung

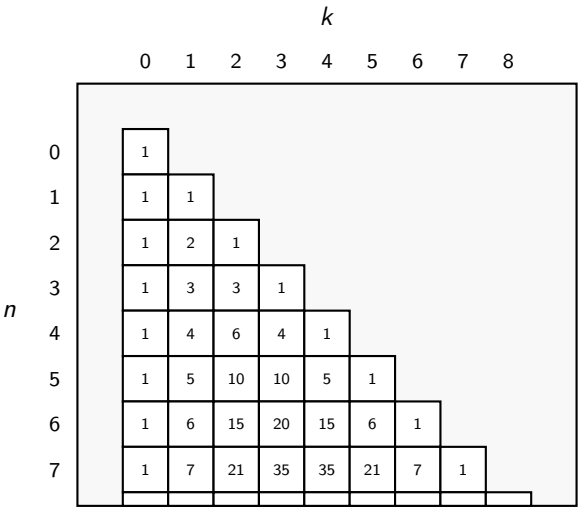
Der Binomialkoeffizient $\binom{n}{k}$ genügt für alle $k, n \in \mathbb{N}$ mit $k \leq n$ die Rekursion

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

mit $\binom{0}{0} = 1$, $\binom{n}{0} = 1$ und $\binom{n}{n} = 1$ für alle $n \in \mathbb{N}$.

Diese Formel heißt auch Pascal'sche Identität und ist die Grundlage für die Konstruktions des Pascal'schen Dreiecks. In ihm können die Werte von $\binom{n}{k}$ abgelesen werden.

Pascal'sches Dreieck



Intuition

Wenn man k Zahlen aus $[n]$ zieht, wird die Zahl n entweder gezogen oder nicht gezogen (deswegen „+“).

- Falls n gezogen wird, so muss man aus den restlichen $n-1$ Zahlen nur noch $k-1$ ziehen. Dafür gibt es $\binom{n-1}{k-1}$ Möglichkeiten.
- Falls n nicht gezogen wird, so muss man aus den restlichen $n-1$ Zahlen alle k ziehen. Dafür gibt es $\binom{n-1}{k}$ Möglichkeiten.

Binomische Formel

Für $n \in \mathbb{N}_0$ beliebige a und b gilt:

$$\sum_{i=0}^{n} \binom{n}{i} \cdot a^i \cdot b^{n-i} = (a+b)^n$$

Beispiele

Für die ersten Werte von n gilt:

$$
\begin{aligned}
1 &= (a+b)^0 \\
b+a &= (a+b)^1 \\
b^2+2ab+a^2 &= (a+b)^2 \\
b^3+3ab^2+3a^2b+a^3 &= (a+b)^3 \\
b^4+4ab^3+6a^2b^2+4a^3b+a^4 &= (a+b)^4 \\
b^5+5ab^4+10a^2b^3+10a^3b^2+5a^4b+a^5 &= (a+b)^5 \\
b^6+6ab^5+15a^2b^4+20a^3b^3+15a^4b^2+6a^5b+a^6 &= (a+b)^6
\end{aligned}
$$

Beispiel

Multipliziert man $(x+y+z)^6$ aus, so erhält man:

$$x^6+6x^5y+6x^5z+15x^4y^2+30x^4yz+15x^4z^2+20x^3y^3+60x^3y^2z+60x^3yz^2+20x^3z^3+15x^2y^4+60x^2y^3z+90x^2y^2z^2+60x^2yz^3+15x^2z^4+6xy^5+30xy^4z+60xy^3z^2+60xy^2z^3+30xyz^4+6xz^5+y^6+6y^5z+15y^4z^2+20y^3z^3+15y^2z^4+6yz^5+z^6.$$

Wir erkennen beispielsweise, dass 60 der Koeffizient von x^2yz^3 in $(x+y+z)^6$ ist.

Beispiel

Den Koeffizient von x^2yz^3 in $(x+y+z)^6$ kann man mit der Binomischen Formel sehr leicht berechnen:

- Für $a = x$, $b = y + z$ und $n = 6$ erhalten wir:

$$(x+y+z)^6 = (x+(y+z))^6 = \sum_{k=0}^{6} \binom{6}{k} x^k (y+z)^{6-k} = \ldots + \binom{6}{2} x^2 (y+z)^4 + \ldots$$

- Für $a = y$, $b = z$ und $n = 4$ erhalten wir:

$$(y+z)^4 = \sum_{k=0}^{4} \binom{4}{k} y^k z^{4-k} = \ldots + \binom{4}{1} yz^3 + \ldots$$

Somit erhält $(x+y+z)^6$ den Summanden $\binom{6}{2} x^2 \binom{4}{1} yz^3 = \binom{6}{2}\binom{4}{1} x^2 yz^3$ und der gesuchte Koeffizient ist $\binom{6}{2}\binom{4}{1} = 60$.

Quizfragen

1. Was ist der Koeffizient von $x^2y^2z^2$ in $(x+y+z)^6$?
2. Was ist der Koeffizient von xyz^4 in $(x+y+z)^6$?
3. Was ist der Koeffizient von xy^3z^2 in $(x+2y+z)^6$?
4. Was ist der Koeffizient von x^3yz^2 in $(3x+y+2z)^6$?
5. Was ist der Koeffizient von $x^2y^4z^2$ in $(xy+y+z)^6$?
6. Was ist der Koeffizient von $x^3y^5z^4$ in $(xyz+y+z)^6$?
7. Was ist der Koeffizient von $w^2x^3yz^2$ in $(w+x+y+z)^8$?

1. $(x+y+z)^6 = (x+(y+z))^6 = \sum_{k=0}^{6} \binom{6}{k} x^k (y+z)^{6-k} = \ldots + \binom{6}{2} x^2 (y+z)^4 + \ldots$
   $\rightsquigarrow (y+z)^4 = \sum_{k=0}^{4} \binom{4}{k} y^k z^{4-k} = \ldots + \binom{4}{2} y^2 z^2 + \ldots$
   $\rightsquigarrow$ Der Koeffizient ist $\binom{6}{2}\binom{4}{2} = 90$.

2. $(x+y+z)^6 = (x+(y+z))^6 = \sum_{k=0}^{6} \binom{6}{k} x^k (y+z)^{6-k} = \ldots + \binom{6}{1} x (y+z)^5 + \ldots$
   $\rightsquigarrow (y+z)^5 = \sum_{k=0}^{5} \binom{5}{k} y^k z^{5-k} = \ldots + \binom{5}{1} yz^4 + \ldots$
   $\rightsquigarrow$ Der Koeffizient ist $\binom{6}{1}\binom{5}{1} = 30$.

3. $(x+2y+z)^6 = (x+(2y+z))^6 = \sum_{k=0}^{6} \binom{6}{k} x^k (2y+z)^{6-k} = \ldots + \binom{6}{1} x (2y+z)^5 + \ldots$
   $\rightsquigarrow (2y+z)^5 = \sum_{k=0}^{5} \binom{5}{k} (2y)^k z^{4-k} = \ldots + \binom{5}{3} (2y)^3 z^2 + \ldots = \ldots + \binom{5}{3} 2^3 y^3 z^2 + \ldots$
   $\rightsquigarrow$ Der Koeffizient ist $\binom{6}{1}\binom{5}{3} 2^3 = 480$.

4. $(3x+y+2z)^6 = (3x+(y+2z))^6 = \sum_{k=0}^{6} \binom{6}{k} 3x^k (y+2z)^{6-k} =$
   $\ldots + \binom{6}{3} (3x)^3 (y+2z)^3 + \ldots = \ldots + \binom{6}{3} 3^3 x^3 (y+2z)^3 + \ldots$
   $\rightsquigarrow (y+2z)^3 = \sum_{k=0}^{3} \binom{3}{k} y^k (2z)^{3-k} = \ldots + \binom{3}{1} y (2z)^2 + \ldots = \ldots + \binom{3}{1} 2^2 yz^2 + \ldots$
   $\rightsquigarrow$ Der Koeffizient ist $\binom{6}{3} 3^3 \binom{3}{1} 2^2 = 6480$.

5. $(xy+y+z)^6 = (xy+(y+z))^6 = \sum_{k=0}^{6} \binom{6}{k}(xy)^k(y+z)^{6-k} =$
   $\ldots + \binom{6}{2}(xy)^2(y+z)^4 + \ldots = \ldots + \binom{6}{2}x^2y^2(y+z)^4 + \ldots$
   $\rightsquigarrow (y+z)^4 = \sum_{k=0}^{4} \binom{4}{k}y^k z^{4-k} = \ldots + \binom{4}{2}y^2z^2 + \ldots$
   $\rightsquigarrow$ Der Koeffizient ist $\binom{6}{2}\binom{4}{2} = 90$.

6. $(xyz+y+z)^6 = (xyz+(y+z))^6 = \sum_{k=0}^{6} \binom{6}{k}(xyz)^k(y+z)^{6-k} =$
   $\ldots + \binom{6}{3}(xyz)^3(y+z)^3 + \ldots = \ldots + \binom{6}{3}x^3y^3z^3(y+z)^3 + \ldots$
   $\rightsquigarrow (y+z)^3 = \sum_{k=0}^{3} \binom{3}{k}y^k z^{3-k} = \ldots + \binom{3}{2}y^2z + \ldots$
   $\rightsquigarrow$ Der Koeffizient ist $\binom{6}{3}\binom{3}{2} = 60$.

7. $(w+x+y+z)^8 = (w+(x+y+z))^8 = \sum_{k=0}^{8} \binom{8}{k}w^k(x+y+z)^{8-k} =$
   $\ldots + \binom{8}{2}w^2(x+y+z)^6 + \ldots$
   $\rightsquigarrow (x+y+z)^6 = (3x+(y+z))^6 = \sum_{k=0}^{6} \binom{6}{k}x^k(y+z)^{6-k} = \ldots + \binom{6}{3}x^3(y+z)^3 + \ldots$
   $\rightsquigarrow (y+z)^3 = \sum_{k=0}^{3} \binom{3}{k}y^k z^{3-k} = \ldots + \binom{3}{1}yz^2 + \ldots$
   $\rightsquigarrow$ Der Koeffizient ist $\binom{8}{2}\binom{6}{3}\binom{3}{1} = 1680$.

Rechenregeln für Binomialkoeffizienten

Folgende Rechenregeln sind sehr wichtig. Es gilt für $n, m, k \in \mathbb{N}_0$:

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!}\,, \qquad \text{(Erste direkte Berechnung)}$$

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}\,, \qquad k \leq n \qquad \text{(Zweite direkte Berechnung)}$$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}\,, \qquad 1 \leq k, n \qquad \text{(Pascalsche Identität)}$$

$$\binom{n}{k} = \sum_{i=0}^{k} \binom{m}{i} \cdot \binom{n-m}{k-i}\,, \qquad m \leq n \qquad \text{(Vandermondsche Identität)}$$

$$\binom{n}{k} = \binom{n}{n-k}\,, \qquad k \leq n \qquad \text{(Symmetrie-Eigenschaft)}$$

Rechenregeln für Binomialkoeffizienten

$$\sum_{i=0}^{n} \binom{n}{i} \cdot a^i \cdot b^{n-i} = (a+b)^n \,, \qquad a, b \in \mathbb{R} \qquad \text{(Binomische Formel)}$$

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n \qquad \text{(Zeilensumme)}$$

$$\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1} \,, \qquad k \leq n \qquad \text{(Spaltensumme)}$$

$$\sum_{i=0}^{k} \binom{n+i}{i} = \binom{n+k+1}{k} \qquad \text{(Diagonalsumme)}$$

Diese Rechenregeln kann man sehr schön am Pascalschen Dreieck erkennen!

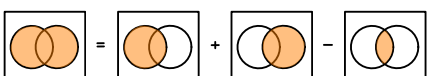
Themenübersicht

Inklusion und Exklusion bzw. Siebformel (für $n = 2$)

Für beliebige endliche Mengen A und B gilt:

$$|A \cup B| = |A| + |B| - |A \cap B| \ .$$

Graphisch:

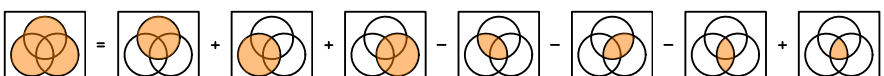


Inklusion und Exklusion bzw. Siebformel (für $n = 3$)

Für beliebige endliche Mengen A, B und C gilt:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \ .$$

Graphisch:



Inklusion und Exklusion bzw. Siebformel (für ein allgemeines n)

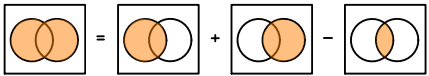
Für beliebige endliche Mengen $A_1, \ldots, A_n$ gilt:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{S\subseteq[n], S\neq\emptyset} (-1)^{|S|-1} \cdot \left|\bigcap_{i\in S} A_i\right|.$$

- Das Summenzeichen $\sum_{S\subseteq[n], S\neq\emptyset}$ summiert über alle möglichen nichtleeren Teilmengen von $[n]$.
- Der Ausdruck $(-1)^{|S|-1}$ ist für den Vorzeichenwechsel zuständig. Ist $|S|$ gerade, so hat $\left|\bigcap_{i\in S} A_i\right|$ Minus als Vorzeichen. Ist $|S|$ ungerade, so hat $\left|\bigcap_{i\in S} A_i\right|$ Plus als Vorzeichen.

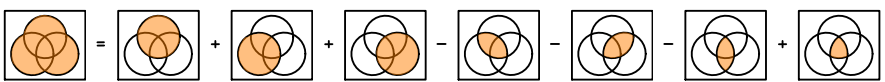
Beispiel ($n = 2$)

$$
\begin{aligned}
|A_1 \cup A_2| &= \sum_{S \subseteq [2], S \neq \emptyset} (-1)^{|S|-1} \cdot \left| \bigcap_{i \in S} A_i \right| \\
&= \left| \bigcap_{i \in \{1\}} A_i \right| + \left| \bigcap_{i \in \{2\}} A_i \right| - \left| \bigcap_{i \in \{1,2\}} A_i \right| \\
&= |A_1| + |A_2| - |A_1 \cap A_2|.
\end{aligned}
$$



Noch ein Beispiel ($n = 3$)

$$
\begin{aligned}
|A_1 \cup A_2 \cup A_3| &= \sum_{S \subseteq [3], S \neq \emptyset} (-1)^{|S|-1} \cdot \left| \bigcap_{i \in S} A_i \right| \\
&= \left| \bigcap_{i \in \{1\}} A_i \right| + \left| \bigcap_{i \in \{2\}} A_i \right| + \left| \bigcap_{i \in \{3\}} A_i \right| - \left| \bigcap_{i \in \{1,2\}} A_i \right| - \left| \bigcap_{i \in \{1,3\}} A_i \right| - \left| \bigcap_{i \in \{2,3\}} A_i \right| + \left| \bigcap_{i \in \{1,2,3\}} A_i \right| \\
&= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.
\end{aligned}
$$



Beweis (für Interessierte)

Mit vollständiger Induktion nach der Anzahl n der vorhandenen Mengen.

- Induktionsanfang ($n = 2$):
  Da A_1 und $A_2 \setminus (A_1 \cap A_2)$ disjunkt sind, gilt:

$$|A_1 \cup (A_2 \setminus (A_1 \cap A_2))| = |A_1| + |A_2 \setminus (A_1 \cap A_2)|.$$

  Da $A_1 \cap A_2$ und $A_2 \setminus (A_1 \cap A_2)$ ebenfalls disjunkt sind, gilt:

$$|A_2| = |(A_1 \cap A_2) \cup (A_2 \setminus (A_1 \cap A_2))| = |A_1 \cap A_2| + |A_2 \setminus (A_1 \cap A_2)|,$$

  d.h.

$$|A_2 \setminus (A_1 \cap A_2)| = |A_2| - |A_1 \cap A_2|.$$

  Aus $A_1 \cup A_2 = A_1 \cup (A_2 \setminus (A_1 \cap A_2))$ folgt:

$$|A_1 \cup A_2| = |A_1 \cup (A_2 \setminus (A_1 \cap A_2))| = |A_1| + |A_2 \setminus (A_1 \cap A_2)| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Beweis (für Interessierte)

- Induktionsschritt: Sei $n \in \mathbb{N}$ beliebig mit

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{S \subseteq [n], S \neq \emptyset} (-1)^{|S|-1} \cdot \left| \bigcap_{i \in S} A_i \right|$$

für beliebige endliche Mengen $A_1, \ldots, A_n$.

Seien nun $A_1, \ldots, A_{n+1}$ beliebige endliche Mengen. Dann gilt:

Beweis (für Interessierte)

$$\begin{aligned}
\left|\bigcup_{i=1}^{n+1} A_i\right| &= \left|\left(\bigcup_{i=1}^{n} A_i\right) \cup A_{n+1}\right| = \left|\bigcup_{i=1}^{n} A_i\right| + |A_{n+1}| - \left|\left(\bigcup_{i=1}^{n} A_i\right) \cap A_{n+1}\right| \\
&= \left|\bigcup_{i=1}^{n} A_i\right| + |A_{n+1}| - \left|\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\right| \\
&= \sum_{S\subseteq[n],S\neq\emptyset} (-1)^{|S|-1} \cdot \left|\bigcap_{i\in S} A_i\right| + |A_{n+1}| - \sum_{S\subseteq[n],S\neq\emptyset} (-1)^{|S|-1} \cdot \left|\bigcap_{i\in S} (A_i \cap A_{n+1})\right| \\
&= \sum_{\substack{S\subseteq[n+1],S\neq\emptyset \\ n+1\notin S}} (-1)^{|S|-1} \cdot \left|\bigcap_{i\in S} A_i\right| + \sum_{\substack{S\subseteq[n+1],S\neq\emptyset \\ n+1\in S}} (-1)^{|S|-1} \cdot \left|\bigcap_{i\in S} A_i\right| \\
&= \sum_{\substack{S\subseteq[n+1], \\ S\neq\emptyset}} (-1)^{|S|-1} \cdot \left|\bigcap_{i\in S} A_i\right|. \qquad \square
\end{aligned}$$

Spezialfall

Falls die Kardinalität einer Schnittmenge von k Mengen nur von der Anzahl k an beteiligten Mengen und nicht von den Mengen selbst abhängig ist, dann gilt:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{S\subseteq[n],S\neq\emptyset} (-1)^{|S|-1} \cdot \left|\bigcap_{i\in S} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \cdot \binom{n}{k} \cdot \left|\bigcap_{i=1}^{k} A_i\right|$$

Es gibt genau $\binom{n}{k}$ k-elementige Teilmengen von $[n]$. Sind alle Summanden $\left|\bigcap_{i\in S} A_i\right|$ für $|S| = k$ gleich, dann kann man $\binom{n}{k}$ mal einen beliebigen nehmen, z.B. $\left|\bigcap_{i=1}^{k} A_i\right|$.

Beispiel

4 verschiedene Gäste bestellen beim selben Kellner 4 verschiedene Gerichte. Dummerweise vergisst der Kellner sofort, wer was bestellt hat, und beschließt, die Verteilung der Gerichte dem Zufall zu überlassen. Bei wie vielen der insgesamt $4! = 24$ Verteilungsmöglichkeiten (Permutationen) bekommt keiner der 4 Gäste sein bestelltes Essen?

Wir definieren A_i für $i = 1, 2, 3, 4$ als diejenige Menge, die alle Verteilungsmöglichkeiten enthält, bei denen Gast i sein bestelltes Essen bekommt. $A_1 \cup A_2 \cup A_3 \cup A_4$ enthält somit alle Verteilungen bei denen mindestens ein Gast sein bestelltes Essen bekommt.

Mit

$$\begin{aligned} |A_1| &= 3!, \\ |A_1 \cap A_2| &= 2!, \\ |A_1 \cap A_2 \cap A_3| &= 1!, \\ |A_1 \cap A_2 \cap A_3 \cap A_4| &= 0! \end{aligned}$$

Beispiel

folgt:

$$\begin{aligned}|A_1 \cup A_2 \cup A_3 \cup A_4| &= \binom{4}{1} \cdot 3! - \binom{4}{2} \cdot 2! + \binom{4}{3} \cdot 1! - \binom{4}{4} \cdot 0! \\ &= 4 \cdot 6 - 6 \cdot 2 + 4 \cdot 1 - 1 \cdot 1 = 15.\end{aligned}$$

D.h. er kriegt bei $24 - 15 = 9$ Verteilungsmöglichkeiten von allen 4 Gästen Ärger.

Info: Hier durfte man den Spezialfall der Siebformel verwenden, weil die Kardinalität jeder Schnittmenge nur von der Anzahl der beteiligten Mengen und nicht von den Mengen selbst abhängig ist, d.h.:

$$\begin{aligned}&|A_1| = |A_2| = |A_3| = |A_4| = 3!, \\ &|A_1 \cap A_2| = |A_1 \cap A_3| = |A_1 \cap A_4| = |A_2 \cap A_3| = |A_2 \cap A_4| = |A_3 \cap A_4| = 2!, \\ &|A_1 \cap A_2 \cap A_3| = |A_1 \cap A_2 \cap A_4| = |A_1 \cap A_3 \cap A_4| = |A_2 \cap A_3 \cap A_4| = 1!, \\ &|A_1 \cap A_2 \cap A_3 \cap A_4| = 0!.\end{aligned}$$

Übungsaufgabe

Seien $\Sigma = \{a, b, c\}$ ein Alphabet und $\Omega = \Sigma^6$ die Menge aller Wörter über Σ der Länge 6.

1. Bestimme die Anzahl der Wörter $w \in \Omega$, die jedes der Zeichen aus Σ mindestens einmal enthalten. Benutze hierfür die Mengen

$$A = \{w \in \Omega \mid \text{in } w \text{ kommt kein } a \text{ vor}\},$$
$$B = \{w \in \Omega \mid \text{in } w \text{ kommt kein } b \text{ vor}\},$$
$$C = \{w \in \Omega \mid \text{in } w \text{ kommt kein } c \text{ vor}\}.$$

2. Wie viele solche Wörter gibt es in Abhängigkeit von m und n, falls $\Sigma = \{a_1, \ldots, a_n\}$ und $\Omega = \Sigma^m$?

1. Für die Kardinalität von $A \cup B \cup C$ gilt nach dem Spezialfall der Siebformel für $n = 3$:

$$\begin{aligned} |A \cup B \cup C| &= \binom{3}{1}|A| - \binom{3}{2}|A \cap B| + \binom{3}{3}|A \cap B \cap C| \\ &= 3|A| - 3|A \cap B| + |A \cap B \cap C| \\ &= 3 \cdot 2^6 - 3 \cdot 1^6 + 0^6 \\ &= 189 \end{aligned}$$

Die gesuchte Anzahl an Wörtern beträgt dann:

$$|\Omega| - |A \cup B \cup C| = 3^6 - 189 = 729 - 189 = 540.$$

2. Für $m < n$ ist die Anzahl offensichtlich Null. Für $m \geq n$ definieren wir

$$A_i = \{w \in \Omega \mid \text{in } w \text{ kommt kein } a_i \text{ vor}\}$$

für alle $i \in [n]$ und erhalten:

$$|\Omega| - \left|\bigcup_{i=1}^{n} A_i\right| = n^m - \sum_{k=1}^{n} (-1)^{k-1} \cdot \binom{n}{k} \cdot (n-k)^m = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot (n-k)^m.$$

Themenübersicht

Ziehen von Elementen

Wir ziehen k Elemente aus einer n-elementigen Menge. Dabei kann die Reihenfolge der Ziehungen eine Rolle spielen („geordnet“) oder nicht („ungeordnet“) und die gezogenen Elemente können wieder zurückgelegt werden oder nicht.

	mit Zurücklegen	ohne Zurücklegen
geordnet	n^k	$n^{\underline{k}}$
ungeordnet	$\binom{k+n-1}{k}$	$\binom{n}{k}$

Beispiel

Wir ziehen 2 Elemente aus der Menge $M = [3]$, d.h. es gilt $k = 2$ und $n = 3$. Für die Anzahl an Möglichkeiten gilt:

	mit Zurücklegen	ohne Zurücklegen
geordnet	$3^2 = 9$	$3^{\underline{2}} = 3 \cdot 2 = 6$
ungeordnet	$\binom{2+3-1}{2} = \frac{4 \cdot 3}{2 \cdot 1} = 6$	$\binom{3}{2} = \frac{3 \cdot 2}{2 \cdot 1} = 3$

Dies entspricht folgenden Ergebnissen:

	mit Zurücklegen	ohne Zurücklegen
geordnet	$(1,2),(1,3),(2,1),$ $(2,3),(3,1),(3,2),$ $(1,1),(2,2),(3,3).$	$(1,2),(1,3),(2,1),$ $(2,3),(3,1),(3,2).$
ungeordnet	$\{\!\{1,2\}\!\},\{\!\{1,3\}\!\},\{\!\{2,3\}\!\},$ $\{\!\{1,1\}\!\},\{\!\{2,2\}\!\},\{\!\{3,3\}\!\}.$	$\{1,2\},\{1,3\},\{2,3\}.$

Themenübersicht

Zyklenschreibweise für Permutationen

Eine Permutation p ist eine bijektive Funktion $p\colon A \to A$ über eine endliche Menge A (s. Folie 503).

Permutationen kann man auch als eine Komposition von Zyklen darstellen. Es gilt:

$$p = \underbrace{(c_{1,1}, \ldots, c_{l_1,1})}_{\substack{\text{Zyklus 1}\\ \text{mit Länge } l_1}} \underbrace{(c_{1,2}, \ldots, c_{l_2,2})}_{\substack{\text{Zyklus 2}\\ \text{mit Länge } l_2}} \ldots \underbrace{(c_{1,k}, \ldots, c_{l_k,k})}_{\substack{\text{Zyklus } k\\ \text{mit Länge } l_k}},$$

wobei $A = \{c_{1,1}, \ldots, c_{l_1,1}, c_{1,2}, \ldots, c_{l_2,2}, \ldots, c_{1,k}, \ldots, c_{l_k,k}\}$ und für alle $c_{i,j}$ gilt:

$$p(c_{i,j}) = \begin{cases} c_{i+1,j}, & \text{falls } i < l_j \\ c_{1,j}, & \text{falls } i = l_j \end{cases}.$$

Man versteht das aber viel viel besser mit einem Beispiel :-)

Beispiel

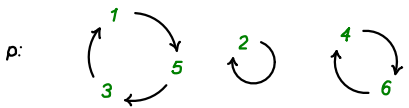
Sei p eine Permutation über $[6]$ mit:

$$p(1) = 5,\ p(2) = 2,\ p(3) = 1,\ p(4) = 6,\ p(5) = 3,\ p(6) = 4.$$

Matrixschreibweise:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$$

Graphisch:



Zyklenschreibweise:

$$p = (1, 5, 3)(2)(4, 6)$$

Noch ein Beispiel

Sei p eine Permutation über [8] mit:

$$p(1) = 5,\ p(2) = 6,\ p(3) = 7,\ p(4) = 8,\ p(5) = 1,\ p(6) = 2,\ p(7) = 3,\ p(8) = 4.$$

Matrixschreibweise:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Graphisch:

Zyklenschreibweise:

$$p = (1, 5)(2, 6)(3, 7)(4, 8)$$

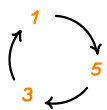
Infos

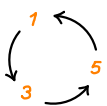
- Es gibt in der Regel mehrere Möglichkeiten einen Zyklus aufzuschreiben. Zum Beispiel:

$$(1,8,2,5) = (8,2,5,1) = (2,5,1,8) = (5,1,8,2).$$

- Achtung: Man darf die Komponenten eines Zyklus beliebig „shiften“, aber man darf die Reihenfolge nicht beliebig ändern! Zum Beispiel:

$$\underbrace{(1,5,3) = (5,3,1) = (3,1,5)}_{}\neq\underbrace{(1,3,5) = (3,5,1) = (5,1,3)}_{}.$$





- Die Reihenfolge der Zyklen ist irrelevant. Zum Beispiel:

$$(1,6)(2)(4)(3,5) = (3,5)(4)(1,6)(2).$$

Quizfragen

1. Gilt $(3,1,4,5,2,6) = (4,5,2,6,3,1)$?
2. Gilt $(3,1,4,5,2,6) = (6,2,5,4,1,3)$?
3. Gilt $(3,4)(5,1,2,6) = (3,4)(1,2,6,5)$?
4. Gilt $(3,4)(5,1,2,6) = (1,2,6,5)(3,4)$?
5. Gilt $(2,4,3)(5,1,6) = (4,2,3)(1,5,6)$?
6. Gilt $(2,4)(1,5)(3,6) = (4,2)(1,5)(6,3)$?
7. Gilt $(2,4)(1,5)(3,6) = (5,1)(4,2)(6,3)$?
8. Gilt $(1)(4,2)(3,6,5) = (1)(2,4)(5,3,6)$?
9. Gilt $(1)(4,2)(3,6,5) = (6,5,3)(1)(4,2)$?

Antworten

1. Ja.
2. Nein.
3. Ja.
4. Ja.
5. Nein.
6. Ja.
7. Ja.
8. Ja.
9. Ja.

Gegeben seien folgende Permutationen p_1, p_2 und p_3 über $[6]$ in Matrixdarstellung:

1. $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$,
2. $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}$,
3. $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 6 & 4 \end{pmatrix}$.

Wie sehen p_1, p_2 und p_3 in Zyklendarstellung aus?

Antworten

1. $p_1 = (1, 2, 6, 3)(4, 5)$.
2. $p_2 = (1, 3)(2)(4, 5, 6)$.
3. $p_3 = (1, 2, 3, 5, 6, 4)$.

Gegeben seien folgende Permutationen p_1, p_2 und p_3 über $[6]$ in Zyklendarstellung:

1. $p_1 = (2,3)(4)(1,5,6)$,
2. $p_2 = (1,3,2)(6,4,5)$,
3. $p_3 = (5,3,6,2)(4,1)$.

Wie sehen p_1, p_2 und p_3 in Matrixdarstellung aus?

1. $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 4 & 6 & 1 \end{pmatrix}$.
2. $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix}$.
3. $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 3 & 2 \end{pmatrix}$.

Stirling-Zahlen erster Art

$\begin{bmatrix} n \\ k \end{bmatrix}$ gibt die Anzahl der Permutationen in Zyklenschreibweise (s. Folie 503) von n Elementen mit genau k (nichtleeren) Zyklen an. Man schreibt oft auch $\begin{bmatrix} n \\ k \end{bmatrix}$ statt $\begin{bmatrix} n \\ k \end{bmatrix}$.

Beispiel

Es gibt genau 11 Permutationen über [4] mit genau 2 Zyklen:

$(1)(2,3,4), (1)(2,4,3), (2)(1,3,4), (2)(1,4,3), \quad (3)(1,2,4), (3)(1,4,2), (4)(1,2,3), (4)(1,3,2), (1,2)(3$

Also ist $\begin{bmatrix} 4 \\ 2 \end{bmatrix} = 11$.

Man kann die Elemente innerhalb eines Zykels beliebig „shiften“, z.B.:

$$(1,2,3) = (2,3,1) = (3,1,2) \neq (1,3,2) = (2,1,3) = (3,2,1)$$

Quizfragen

1. Was ist $\begin{bmatrix} 3 \\ 1 \end{bmatrix}$?
2. Was ist $\begin{bmatrix} 3 \\ 2 \end{bmatrix}$?
3. Was ist $\begin{bmatrix} 4 \\ 1 \end{bmatrix}$?
4. Was ist $\begin{bmatrix} 4 \\ 3 \end{bmatrix}$?
5. Was ist $\begin{bmatrix} n \\ 0 \end{bmatrix}$ für $n \in \mathbb{N}$?
6. Was ist $\begin{bmatrix} n \\ 1 \end{bmatrix}$ für $n \in \mathbb{N}$?
7. Was ist $\begin{bmatrix} n \\ n-1 \end{bmatrix}$ für $n \in \mathbb{N}$?
8. Was ist $\begin{bmatrix} n \\ n \end{bmatrix}$ für $n \in \mathbb{N}_0$?

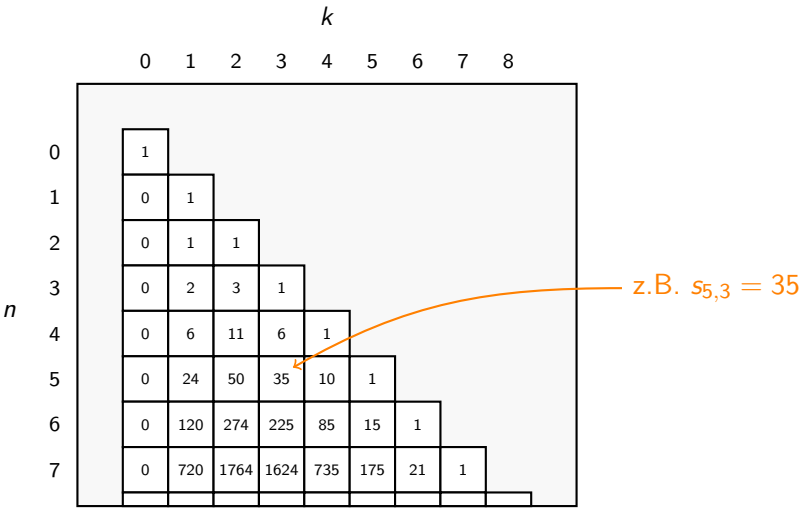
Antworten

1. $\begin{bmatrix} 3 \\ 1 \end{bmatrix} = 2$.
2. $\begin{bmatrix} 3 \\ 2 \end{bmatrix} = 3$.
3. $\begin{bmatrix} 4 \\ 1 \end{bmatrix} = 6$.
4. $\begin{bmatrix} 4 \\ 3 \end{bmatrix} = 6$.
5. $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$.
6. $\begin{bmatrix} n \\ 1 \end{bmatrix} = \frac{n!}{n} = (n-1)!$.
7. $\begin{bmatrix} n \\ n-1 \end{bmatrix} = \binom{n}{2}$.
8. $\begin{bmatrix} n \\ n \end{bmatrix} = 1$.

Info

Die Werte von $\begin{bmatrix} n \\ k \end{bmatrix}$ können in folgendem Dreieck abgelesen werden.

Info


k
0 1 2 3 4 5 6 7 8
n
0 1
1 0 1
2 0 1 1
3 0 2 3 1
4 0 6 11 6 1
5 0 24 50 35 10 1
6 0 120 274 225 85 15 1
7 0 720 1764 1624 735 175 21 1
z.B. $s_{5,3} = 35$

Rekursive Berechnung

Die Stirling-Zahl erster Art $\begin{bmatrix} n \\ k \end{bmatrix}$ genügt für alle $n, k \in \mathbb{N}$ mit $k \leq n$ die Rekursion

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}$$

mit $\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1$, $\begin{bmatrix} n \\ 0 \end{bmatrix} = 0$ und $\begin{bmatrix} n \\ n \end{bmatrix} = 1$ für alle $n \in \mathbb{N}$.

Intuition

Wenn man k Zyklen mit Zahlen aus $[n]$ füllen möchte, dann kann das Element n entweder alleine in einem Zyklus sein oder nicht (deswegen „+“).

- Falls n alleine in einem Zyklus ist, so hat man für die restlichen $n-1$ Elemente nur noch $k-1$ Zyklen. Daher gibt es hierfür $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ Möglichkeiten.
- Falls n nicht alleine in einem Zyklus ist, so muss man die restlichen $n-1$ Elemente in allen k Zyklen verteilen ($\begin{bmatrix} n-1 \\ k \end{bmatrix}$ Möglichkeiten) und dann (deswegen jetzt „$\cdot$“) das Element n rechts von einem der $n-1$ restlichen Elemente in dem entsprechenden Zyklus hinzufügen ($n-1$ Möglichkeiten). Insgesamt gibt es hierfür $(n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}$ Möglichkeiten.

Rechenregeln für Stirlingzahlen erster Art

Folgende Rechenregeln sind für Stirlingzahlen erster Art wichtig. Es gilt für $n, k \in \mathbb{N}_0$:

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}, \qquad 1 \leq n, k \qquad \text{(Rekursive Berechnung)}$$

$$\sum_{i=0}^{n} \begin{bmatrix} n \\ i \end{bmatrix} = n! \qquad \text{(Zeilensumme)}$$

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = 0, \qquad 1 \leq n$$

$$\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!, \qquad 1 \leq n$$

$$\begin{bmatrix} n \\ n-1 \end{bmatrix} = \binom{n}{2} = \frac{n \cdot (n-1)}{2}, \qquad 1 \leq n$$

$$\begin{bmatrix} n \\ n \end{bmatrix} = 1$$

Rechenregeln für Stirlingzahlen erster Art

Diese Rechenregeln kann man sehr schön am Dreieck für Stirlingzahlen erster Art erkennen!

Themenübersicht

Stirling-Zahlen zweiter Art

$\left\{ {n \atop k} \right\}$ gibt die Anzahl der Partitionen (s. Folie 45) einer n-elementigen Menge in k nichtleere Klassen an. Man schreibt oft auch $\left\{ {n \atop k} \right\}$ statt $\left\{ {n \atop k} \right\}$.

Beispiel

Es gibt genau 7 2-Partitionen der Menge [4]:

$$\{\{1\},\{2,3,4\}\},\{\{2\},\{1,3,4\}\},\{\{3\},\{1,2,4\}\},\{\{4\},\{1,2,3\}\},$$
$$\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\ .$$

Bzw. kurz:

$$1 \mid 2,3,4 \qquad 2 \mid 1,3,4 \qquad 3 \mid 1,2,4 \qquad 4 \mid 1,2,3 \qquad 1,2 \mid 3,4 \qquad 1,3 \mid 2,4 \qquad 1,4 \mid 2,3$$

Also ist $\left\{ {4 \atop 2} \right\} = 7$.

Quizfragen

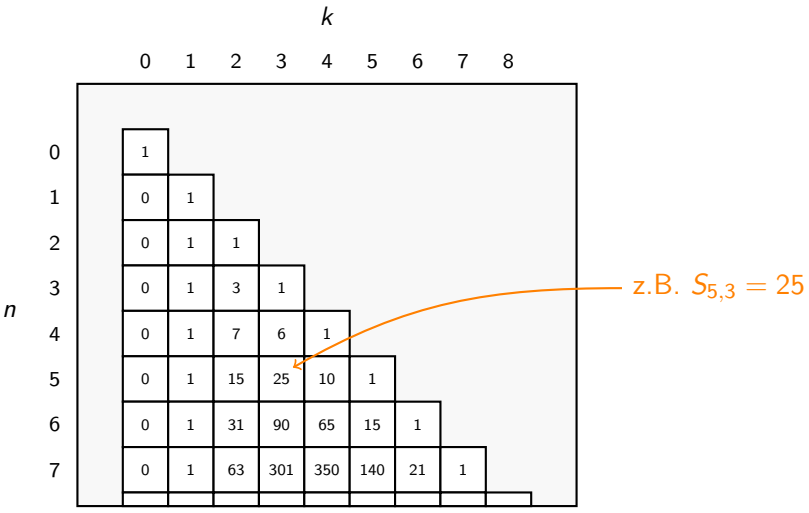
1. Was ist $\left\{ {3 \atop 1} \right\}$?
2. Was ist $\left\{ {3 \atop 2} \right\}$?
3. Was ist $\left\{ {4 \atop 1} \right\}$?
4. Was ist $\left\{ {4 \atop 3} \right\}$?
5. Was ist $\left\{ {n \atop 0} \right\}$ für $n \in \mathbb{N}$?
6. Was ist $\left\{ {n \atop 1} \right\}$ für $n \in \mathbb{N}$?
7. Was ist $\left\{ {n \atop n-1} \right\}$ für $n \in \mathbb{N}$?
8. Was ist $\left\{ {n \atop n} \right\}$ für $n \in \mathbb{N}_0$?

1. $\left\{ {3 \atop 1} \right\} = 1$.
2. $\left\{ {3 \atop 2} \right\} = 3$.
3. $\left\{ {4 \atop 1} \right\} = 1$.
4. $\left\{ {4 \atop 3} \right\} = 6$.
5. $\left\{ {n \atop 0} \right\} = 0$.
6. $\left\{ {n \atop 1} \right\} = 1$.
7. $\left\{ {n \atop n-1} \right\} = \binom{n}{2}$.
8. $\left\{ {n \atop n} \right\} = 1$.

Info

Die Werte von $\left\{ {n \atop k} \right\}$ können in folgendem Dreieck abgelesen werden.

Info


k
0 1 2 3 4 5 6 7 8
n
0 1
1 0 1
2 0 1 1
3 0 1 3 1
4 0 1 7 6 1
5 0 1 15 25 10 1
6 0 1 31 90 65 15 1
7 0 1 63 301 350 140 21 1
z.B. $S_{5,3} = 25$

Rekursive Berechnung

Die Stirling-Zahl zweiter Art $\left\{ {n \atop k} \right\}$ genügt für alle $n, k \in \mathbb{N}$ mit $k \leq n$ die Rekursion

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \cdot \left\{ {n-1 \atop k} \right\}$$

mit $\left\{ {0 \atop 0} \right\} = 1$, $\left\{ {n \atop 0} \right\} = 0$ und $\left\{ {n \atop n} \right\} = 1$ für alle $n \in \mathbb{N}$.

Intuition

Wenn man k Klassen mit Zahlen aus $[n]$ füllen möchte, dann kann das Element n entweder alleine in einer Klasse sein oder nicht (deswegen „$+$“).

- Falls n alleine in einer Klasse ist, so hat man für die restlichen $n-1$ Elemente nur noch $k-1$ Klassen. Daher gibt es hierfür $\left\{ {n-1 \atop k-1} \right\}$ Möglichkeiten.
- Falls n nicht alleine in einer Klasse ist, so muss man die restlichen $n-1$ Elemente in allen k Klassen verteilen ($\left\{ {n-1 \atop k} \right\}$ Möglichkeiten) und dann (deswegen jetzt „$\cdot$“) das Element n in eine der k Klassen hinzufügen (k Möglichkeiten). Insgesamt gibt es hierfür $k \cdot \left\{ {n-1 \atop k} \right\}$ Möglichkeiten.

Rechenregeln für Stirlingzahlen zweiter Art

Folgende Rechenregeln sind für Stirlingzahlen zweiter Art wichtig. Es gilt für $n, k \in \mathbb{N}_0$:

$$\left\{ n \atop k \right\} = \left\{ n-1 \atop k-1 \right\} + k \cdot \left\{ n-1 \atop k \right\}, \qquad 1 \leq n, k \qquad \text{(Rekursive Berechnung)}$$

$$\left\{ n \atop 0 \right\} = 0, \qquad 1 \leq n$$

$$\left\{ n \atop 1 \right\} = 1, \qquad 1 \leq n$$

$$\left\{ n \atop 2 \right\} = 2^{n-1} - 1, \qquad 1 \leq n$$

$$\left\{ n \atop n-1 \right\} = \binom{n}{2} = \frac{n \cdot (n-1)}{2}, \qquad 1 \leq n$$

$$\left\{ n \atop n \right\} = 1$$

Diese Rechenregeln kann man sehr schön am Dreieck für Stirlingzahlen zweiter Art erkennen!

Themenübersicht

Zahlpartitionen

$P_{n,k}$ gibt die Anzahl der Partitionen der n-elementigen Multimenge $\{\!|1, 1, \ldots, 1|\!\}$ (s. Folie 733) in k nichtleere Klassen an. Intuitiv gibt $P_{n,k}$ die Anzahl der Möglichkeiten, n als Summe von k Summanden aus $\mathbb{N}$ darzustellen.

Beispiel

Es gibt genau 4 3-Partitionen über $\{\!|1,1,1,1,1,1,1|\!\}$:

$$\{\!|\{\!|1|\!\},\{\!|1|\!\},\{\!|1,1,1,1,1|\!\}|\!\},$$
$$\{\!|\{\!|1|\!\},\{\!|1,1|\!\},\{\!|1,1,1,1|\!\}|\!\},$$
$$\{\!|\{\!|1|\!\},\{\!|1,1,1|\!\},\{\!|1,1,1|\!\}|\!\},$$
$$\{\!|\{\!|1,1|\!\},\{\!|1,1|\!\},\{\!|1,1,1|\!\}|\!\}.$$

Bzw. kurz:

$$7 \quad = \quad 1+1+5 \quad = \quad 1+2+4 \quad = \quad 1+3+3 \quad = \quad 2+2+3.$$

Also ist $P_{7,3} = 4$.

Quizfragen

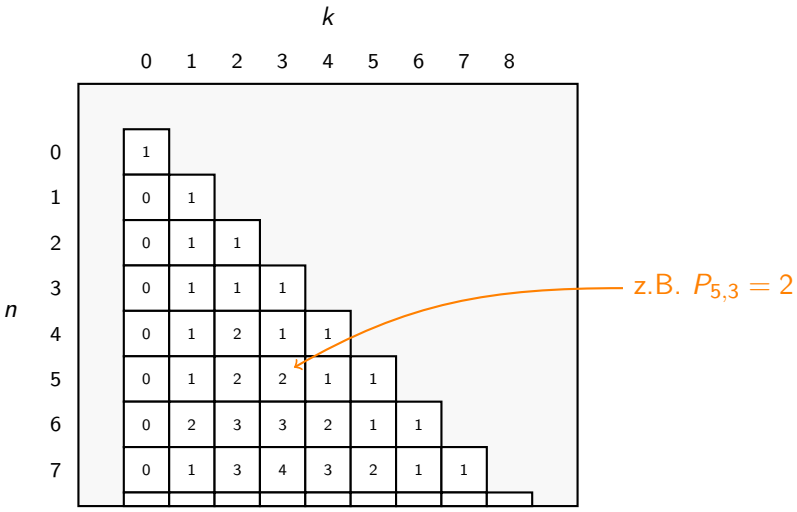
1. Was ist $P_{6,4}$?
2. Was ist $P_{6,5}$?
3. Was ist $P_{7,2}$?
4. Was ist $P_{8,3}$?
5. Was ist $P_{n,0}$ für $n \in \mathbb{N}$?
6. Was ist $P_{n,1}$ für $n \in \mathbb{N}$?
7. Was ist $P_{n,2}$ für $n \in \mathbb{N}$?
8. Was ist $P_{n,n-1}$ für $n \in \mathbb{N}$?
9. Was ist $P_{n,n}$ für $n \in \mathbb{N}_0$?

1. $P_{6,4} = 2$.
2. $P_{6,5} = 1$.
3. $P_{7,2} = 3$.
4. $P_{8,3} = 5$.
5. $P_{n,0} = 0$.
6. $P_{n,1} = 1$.
7. $P_{n,2} = \left\lfloor \frac{n}{2} \right\rfloor$.
8. $P_{n,n-1} = 1$.
9. $P_{n,n} = 1$.

Info

Die Werte von $P_{n,k}$ können in folgendem Dreieck abgelesen werden.

Info


k
0 1 2 3 4 5 6 7 8
n
0 1
1 0 1
2 0 1 1
3 0 1 1 1
4 0 1 2 1 1
5 0 1 2 2 1 1
6 0 2 3 3 2 1 1
7 0 1 3 4 3 2 1 1
z.B. $P_{5,3} = 2$

Erste Rekursive Berechnung

Die Zahlpartition $P_{n,k}$ genügt für alle $n, k \in \mathbb{N}$ mit $k \leq n$ die Rekursion

$$P_{n,k} = \sum_{i=0}^{k} P_{n-k,i} = P_{n-k,0} + P_{n-k,1} + P_{n-k,2} + \ldots + P_{n-k,k}$$

mit $P_{0,0} = 1$, $P_{n,0} = 0$ und $P_{n,n} = 1$ für alle $n \in \mathbb{N}$.

Intuition

Man möchte n 1en in k Klassen so verteilen, dass keine Klasse leer bleibt. Man kann als erstes in jede Klasse zuerst genau eine 1 hinzufügen, so dass wir nur noch $n - k$ übrig haben. Dann gilt:

- entweder wir fügen alle restlichen $n - k$ 1en in keine Klasse hinzu ($P_{n-k,0} = 0$ Möglichkeiten, falls $n - k \neq 0$ bzw. $P_{n-k,0} = 1$ Möglichkeit, falls $n - k = 0$)
- oder wir fügen alle restlichen $n - k$ 1en in eine Klasse hinzu ($P_{n-k,1}$ Möglichkeiten)
- oder wir verteilen sie auf zwei Klassen ($P_{n-k,2}$ Möglichkeiten)
- oder wir verteilen sie auf drei Klassen ($P_{n-k,3}$ Möglichkeiten)
- ...
- oder wir verteilen sie auf alle k Klassen ($P_{n-k,k}$ Möglichkeiten)

Zweite rekursive Berechnung

Aus der ersten Formel folgt: $P_{n-1,k-1} = \sum_{i=0}^{k-1} P_{n-k,i}$. Ersetzt man nun die ersten $k-1$ Summanden der Summe $\sum_{i=0}^{k} P_{n-k,i}$ durch $P_{n-1,k-1}$ erhält man folgende äquivalente Aussage für alle $n, k \in \mathbb{N}$:

$$P_{n,k} = P_{n-1,k-1} + P_{n-k,k}$$

wieder mit $P_{0,0} = 1$, $P_{n,0} = 0$ und $P_{n,n} = 1$ für alle $n \in \mathbb{N}$.

Intuition

Entweder es gibt mindestens eine Klasse mit nur einer 1 oder nicht.

- Falls eine Klasse nur eine 1 hat, dann muss man lediglich die restlichen $n-1$ 1en auf die restlichen $k-1$ Klassen verteilen ($P_{n-1,k-1}$ Möglichkeiten)
- Falls alle Klassen mindestens zwei 1en haben so kann man sich von jeder Klasse eine 1 „wegdenken“ und nur $n-k$ 1en auf die k Klassen verteilen.

Rechenregeln für Zahlpartitionen

Folgende Rechenregeln sind für Zahlpartitionen wichtig. Es gilt für $n, k \in \mathbb{N}_0$:

$$P_{n,k} = \sum_{i=0}^{k} P_{n-k,i} \ , \qquad 1 \leq n, k \qquad \text{(Erste rekursive Berechnung)}$$

$$P_{n,k} = P_{n-1,k-1} + P_{n-k,k} \ , \qquad 1 \leq n, k \qquad \text{(Zweite rekursive Berechnung)}$$

$$P_{n,0} = 0 \ , \qquad 1 \leq n$$

$$P_{n,1} = 1 \ , \qquad 1 \leq n$$

$$P_{n,2} = \left\lfloor \frac{n}{2} \right\rfloor \ , \qquad 1 \leq n$$

$$P_{n,n-1} = 1 \ , \qquad 1 \leq n$$

$$P_{n,n} = 1$$

Diese Rechenregeln kann man sehr schön am Dreieck für Zahlpartitionen erkennen!

Vergleich: $s_{n,k}$ vs. $S_{n,k}$ vs. $P_{n,k}$

Mit $s_{n,k}$, $S_{n,k}$ und $P_{n,k}$ zählen wir die Möglichkeiten irgendwelche Elemente in nicht unterscheidbaren Zyklen bzw. Klassen zu verteilen.

- Bei $s_{n,k}$ sind die Elemente alle verschieden und die Reihenfolge der Elemente innerhalb eines Zykels spielt eine Rolle.
- Bei $S_{n,k}$ sind die Elemente, wie bei $s_{n,k}$, alle verschieden, aber die Reihenfolge der Elemente innerhalb einer Klasse ist irrelevant.
- Bei $P_{n,k}$ sind die Elemente alle gleich (das heißt es spielt keine Rolle welches wo landet) und die Reihenfolge der Elemente innerhalb einer Klasse ist ebenfalls irrelevant.

Vergleich: $s_{n,k}$ vs. $S_{n,k}$ vs. $P_{n,k}$

Übersichtlicher als Tabelle:

Zählkoeffizient	Elemente	Reihenfolge der Elemente	Reihenfolge der Klassen
$s_{n,k}$	verschieden	Zyklus	irrelevant
$S_{n,k}$	verschieden	irrelevant	irrelevant
$P_{n,k}$	gleich	irrelevant	irrelevant

Deswegen gilt für alle $n, k \in \mathbb{N}_0$:

$$P_{n,k} \leq S_{n,k} \leq s_{n,k} \ .$$

Beispiel

$s_{4,2} = 11$	$S_{4,2} = 7$	$P_{4,2} = 2$
$(1)(2,3,4)$	$\{\{1\},\{2,3,4\}\}$	$\{\{\{1\}\},\{\{1,1,1\}\}\}$
$(1)(2,4,3)$		
$(2)(1,3,4)$	$\{\{2\},\{1,3,4\}\}$	
$(2)(1,4,3)$		
$(3)(1,2,4)$	$\{\{3\},\{1,2,4\}\}$	
$(3)(1,4,2)$		
$(4)(1,2,3)$	$\{\{4\},\{1,2,3\}\}$	
$(4)(1,3,2)$		
$(1,2)(3,4)$	$\{\{1,2\},\{3,4\}\}$	$\{\{\{1,1\}\},\{\{1,1\}\}\}$
$(1,3)(2,4)$	$\{\{1,3\},\{2,4\}\}$	
$(1,4)(2,3)$	$\{\{1,4\},\{2,3\}\}$	

Themenübersicht

Goldene Tabelle

Wir zählen die Anzahl aller möglichen Verteilungen von k Bällen auf n Urnen.

k Bälle $\to$ n Urnen		**1** beliebig viele Bälle pro Urne („beliebig“)	**2** höchstens ein Ball pro Urne („injektiv“)	**3** mindestens ein Ball pro Urne („surjektiv“)	**4** genau ein Ball pro Urne („bijektiv“)
A	Bälle unterscheidbar Urnen unterscheidbar	n^k	$n^{\underline{k}}$	$n! \cdot S_{k,n}$	$k!$
B	Bälle gleich Urnen unterscheidbar	$\binom{k+n-1}{k}$	$\binom{n}{k}$	$\binom{k-1}{n-1}$	1
C	Bälle unterscheidbar Urnen gleich	$\sum_{i=0}^{n} S_{k,i}$	1	$S_{k,n}$	1
D	Bälle gleich Urnen gleich	$\sum_{i=0}^{n} P_{k,i}$	1	$P_{k,n}$	1

Infos

- Damit die Verteilungen injektiv, surjektiv oder bijektiv sein können, muss entsprechend $k \leq n$, $k \geq n$ oder $k = n$ gelten, sonst ist die Anzahl solcher Verteilungen natürlich Null ;-)
- Falls $k = n$ gilt, dann liefern die Formeln für injektiv, surjektiv und bijektiv dieselben Ergebnisse.
- Oft steht in den Musterlösungen $\frac{\overline{n^k}}{k!}$ statt $\binom{k+n-1}{k}$.
- Falls Bälle und Urnen unterscheidbar sind, dann ist die Verteilung automatisch eine Funktion.
- Dieses Modell ist eine Erweiterung des Modells auf Folie 781:

	mit Zurücklegen	ohne Zurücklegen
Reihenfolge relevant	n^k	$n^{\underline{k}}$
Reihenfolge irrelevant	$\binom{k+n-1}{k}$	$\binom{n}{k}$

Rezept

Frage: Wie benutzt man die goldene Tabelle richtig?
Methode: Man stellt sich für jede der gegebenen Mengen folgende zwei Fragen:

Darf ein beliebiges Element aus dieser Menge mit

1. mehreren
2. Null

Elementen aus der anderen Menge in Verbindung stehen?

Hat eine der beiden Mengen auf beide Fragen *nein* als Antwort, dann sind das die Bälle! Für die andere Menge gilt dann:

1. Frage	*ja*	*nein*	*ja*	*nein*
2. Frage	*ja*	*ja*	*nein*	*nein*
Verteilung	beliebig	injektiv	surjektiv	bijektiv

Bei bijektiven Funktionen ist es dann egal was Bälle und was Urnen sind! ;-)

Beispiele

1. Wir würfeln mit mehreren Würfeln gleichzeitig. Jeder Würfel zeigt eine von 6 verschiedenen Zahlen.
   - Es kann nicht passieren, dass ein Würfel mehr als eine oder keine Zahl zeigt.
   - Eine Zahl kann mehr als einmal oder auch Null mal vorkommen.

   Es gilt also:

   $$f : \text{Würfeln} \to \text{Zahlen} \qquad \text{(beliebig)}.$$

2. Wir bilden Wörter einer bestimmten Länge über ein bestimmtes Alphabet.
   - Ein Zeichen kann an mehreren Positionen im Wort oder auch an keiner vorkommen.
   - Es kann nicht passieren, dass eine Position im Wort mit mehr oder weniger als ein Zeichen belegt wird.

   Es gilt also:

   $$f : \text{Positionen im Wort} \to \text{Zeichen im Alphabet} \qquad \text{(beliebig)}.$$

Beispiele

3. Wir verteilen ganze Schokoladen auf Studenten.
   - Es gibt gierige Studenten, die mehr als eine Schokolade essen und auch andere die auf Diät sind und gar keine essen.
   - Schokoladen werden nicht geteilt und auch nicht weggeschmissen.

   Es gilt also:
   $$f : \text{Schokoladen} \to \text{Studenten} \qquad \text{(beliebig)}.$$

4. Hühner legen bekanntlich Eier.
   - Ein Huhn kann mehrere oder auch gar keine Eier legen.
   - Ein Ei wird nicht von mehreren Hühnern gelegt und entsteht auch nicht von alleine.

   Es gilt also:
   $$f : \text{Eier} \to \text{Hühner} \qquad \text{(beliebig)}.$$

5. Wir spielen Lotto. Es werden Zahlen ohne zurücklegen gezogen.
   - Eine Zahl kann nicht mehrmals gezogen werden, aber es kann schon passieren, dass sie nicht gezogen wird.

Beispiele

- In einer Ziehung kann man nicht mehr und auch nicht weniger als eine Zahl ziehen.

Es gilt also:

$$f : \text{Ziehungen} \to \text{Zahlen} \qquad \text{(injektiv)}.$$

6. Informatikstudenten organisieren sich, um zusammen in Autos nach Garching zu fahren.
   - Ein Student kann nicht in zwei Autos sein und bleibt auch nicht ohne Mitfahrgelegenheit.
   - In einem Auto passen mehrere Studenten rein, aber das Auto kann nicht leer sein (noch fahren Autos nicht von alleine).

   Es gilt also:

$$f : \text{Informatikstudenten} \to \text{Autos} \qquad \text{(surjektiv)}.$$

7. Jeder von 11 Fußballspielern zieht vor einem Spiel eins von 11 Trikots an.
   - Kein Spieler trägt mehr oder weniger als ein Trikot.
   - Kein Trikot wird von mehr oder weniger als ein Spieler getragen.

Beispiele

Es gilt also:

$$f : \text{Fußballspieler} \to \text{Trikots} \qquad \text{(bijektiv)}.$$

Oder auch:

$$f : \text{Trikots} \to \text{Fußballspieler} \qquad \text{(bijektiv)}.$$

Eine Banane, ein Apfel, eine Orange und eine Pflaume werden auf 2 Körbe verteilt. Wie viele Verteilungsmöglichkeiten gibt es in jedem der folgenden Fälle?

1. Die Körbe sind unterscheidbar,
2. Die Körbe sind unterscheidbar und kein Korb darf leer bleiben,
3. Die Körbe sind unterscheidbar und jeder Korb soll genau 2 Obststücke bekommen,
4. Die Körbe sind nicht unterscheidbar,
5. Die Körbe sind nicht unterscheidbar und kein Korb darf leer bleiben,
6. Die Körbe sind nicht unterscheidbar und jeder Korb soll genau 2 Obststücke bekommen.

Gib dein Ergebnis als Zahl und nicht als unausgewertetem mathematischen Ausdruck an.

1. Verteile 4 unterscheidbare Bälle auf 2 unterscheidbare Urnen beliebig: $2^4 = 16$.
2. Verteile 4 unterscheidbare Bälle auf 2 unterscheidbare Urnen surjektiv: $2! \cdot S_{4,2} = 2 \cdot 7 = 14$.
3. Für den ersten Korb wähle 2 Obststücke aus 4 und für den zweiten 2 aus 2: $\binom{4}{2} \cdot \binom{2}{2} = 6$.
4. Verteile 4 unterscheidbare Bälle auf 2 gleiche Urnen beliebig: $S_{4,1} + S_{4,2} = 1 + 7 = 8$.
5. Verteile 4 unterscheidbare Bälle auf 2 gleiche Urnen surjektiv: $S_{4,2} = 7$.
6. Für den ersten Korb wähle 2 Obststücke aus 4 und für den zweiten 2 aus 2. Da die Körbe gleich sind, sind je zwei Verteilungen identisch und wir müssen durch 2 dividieren: $\frac{\binom{4}{2} \cdot \binom{2}{2}}{2} = 3$.

Der Weihnachtsmann hat dieses Jahr von 12 Informatikstudenten der TUM keinen Wunschzettel bekommen. (Es gibt tatsächlich Leute, die nicht an den Weihnachtsmann glauben!) Zu Hause am Nordpol hat er noch von Weihnachten 24 identische Socken übrig, die er jetzt großzügigerweise den Studenten nachträglich schenken möchte. Wie viele Verteilungsmöglichkeiten gibt es in jedem der folgenden Fälle?

1. Er verteilt alle 24 Socken irgendwie auf die 12 Studenten.
2. Er hält das für zu unpersönlich und entscheidet jede Socke mit einer unterschiedlichen Farbe zu färben und verteilt sie dann alle irgendwie.
3. Er möchte sparsamer mit seinen Socken umgehen und beschließt 12 der 24 gefärbten Socken irgendwie zu verteilen und 12 für sich zu behalten (für nächstes Jahr).
4. Er hält diese Idee für zu unfair und beschließt 12 der 24 gefärbten Socken fair zu verteilen (also eine Socke pro Student) und 12 für sich zu behalten.

5. Er merkt, dass man mit nur einer Socke nicht viel anfangen kann und beschließt aus den 24 gefärbten Socken 12 Paare zu bilden und diese fair zu verteilen.

Antworten

1. Verteile 24 gleiche Bälle auf 12 unterscheidbare Urnen beliebig: $\binom{24+12-1}{24} = \binom{35}{24}$.
2. Verteile 24 unterscheidbare Bälle auf 12 unterscheidbare Urnen beliebig: 12^{24}.
3. Wähle zuerst 12 aus 24 und verteile dann die restlichen 12 beliebig. $\binom{24}{12} \cdot 12^{12}$.
4. Wie 4., aber bijektiv: $\binom{24}{12} \cdot 12! = \frac{24^{\underline{12}}}{12!} \cdot 12! = 24^{\underline{12}}$. Alternativ: verteile die Studenten injektiv auf die Socken.
5. Wähle für Student 2 aus 24 Socken für Student 1, dann 2 aus 22 für Student 2, dann 2 aus 20 für Student 3, usw.: $\binom{24}{2} \cdot \binom{22}{2} \cdot \binom{20}{2} \cdot \ldots \cdot \binom{2}{2} = \frac{24!}{(2!)^{12}}$.

Wir betrachten jetzt Aufgaben die etwa so aussehen:

> *m verschiedene Urnen stehen nebeneinander. Nun werden n Bälle so auf die Urnen geworfen, dass in jeder Urne höchstens ein Ball landet und jede Urne, in der ein Ball landet, benachbarte Urnen beeinflusst.*

Die Anzahl an Verteilungsmöglichkeiten ermittelt man nicht, indem man Bälle auf Urnen verteilt, sondern leere Urnen auf Zwischenräume. Das Rezept dazu steht auf der nächsten Folie.

Rezept

Frage: Wie verteilt man leere Urnen auf Zwischenräume?
Methode: Zähle die Anzahl der Möglichkeiten für folgende Schritte und multipliziere sie zusammen.

1. Stelle die Bälle in eine Reihe (eindeutig, falls alle Bälle gleich sind bzw. $n!$ Möglichkeiten, falls alle unterschiedlich sind).
2. Von den m Urnen sind n belegt und $m-n$ leer. Verteile einige der leeren Urnen so auf die $n+1$ Zwischenräume neben den Bällen, dass alle notwendigen Bedingungen erfüllt werden.
3. Verteile schließlich die restlichen leeren Urnen auf die Zwischenräume.

Die Urnen werden dabei als gleich betrachtet. Ihre Nummerierung ergibt sich dann aus der Verteilung.

Beispiel

Aufgabe: Wir betrachten ein Parkhaus mit 12 nebeneinander stehenden Parkplätzen

und drei gleiche Monstertrucks, die dort parken wollen. Aufgrund ihrer absurden Größe, belegen die Mostertrucks jeweils zwei benachbarte Parkplätze. Außerdem soll links und rechts von jedem Monstertruck mindestens ein Parkplatz zum Rangieren freigehalten werden.

Eine Parkmöglichkeit wäre beispielsweise:

Wie viele solche Parkmöglichkeiten gibt es?

Lösung: Wir modellieren belegte Parkplätze mit • und freie Parkplätze mit ○ und verteilen dann freie Parkplätze auf Zwischenräume wie folgt.

1. Weil die Monstertrucks alle gleich sind, gibt es nur eine Möglichkeit sie in eine Reihe anzuordnen:

$$\underset{1}{\cup}\bullet\bullet\underset{2}{\cup}\bullet\bullet\underset{3}{\cup}\bullet\bullet\underset{4}{\cup}$$

2. Weil links und rechts von jedem Monstertruck ein freier Platz sein muss, werden von den 6 freien Parkplätzen 4 auf die Zwischenräume verteilt (jeweils 1). Hierfür gibt es auch nur eine Möglichkeit:

$$\overset{\circ}{\underset{1}{\cup}}\bullet\bullet\overset{\circ}{\underset{2}{\cup}}\bullet\bullet\overset{\circ}{\underset{3}{\cup}}\bullet\bullet\overset{\circ}{\underset{4}{\cup}}$$

3. Die übrigen 2 freien Parkplätze werden beliebig auf die 4 unterscheidbaren Zwischenräume verteilt. Hierfür gibt es genau $\binom{2+4-1}{2} = \binom{5}{2} = 10$ Möglichkeiten.

Das sind die 10 Parkmöglichkeiten:

1) ○●●○●●○●●○○○
2) ○●●○●●○○●●○○
3) ○●●○●●○○○●●○
4) ○●●○○●●○●●○○
5) ○●●○○●●○○●●○
6) ○●●○○○●●○●●○
7) ○○●●○●●○●●○○
8) ○○●●○●●○○●●○
9) ○○●●○○●●○●●○
10) ○○○●●○●●○●●○

Wir betrachten wieder ein Parkhaus mit 40 nebeneinander stehenden Parkplätzen. Wieder wollen Monstertrucks parken, die jeweils zwei Parkplätze belegen. Wie viele Parkmöglichkeiten gibt es in den folgenden Szenarien?

1. Es sind 12 gleiche Monstertrucks.
2. Es sind 9 verschiedene Monstertrucks und zwischen je zwei Monstertrucks muss mindestens ein Parkplatz frei bleiben.
3. Es sind 3 *Snakebites*, 2 *Ghostriders* und ein *Bigfoot*. Außerdem müssen zwischen je zwei Monstertrucks mindestens drei Parkplätze frei bleiben.

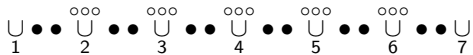
1. Bei 12 gleichen Monstertrucks ist die Reihenfolge eindeutig. Weil zwischen ihnen keine Parkplätze frei bleiben müssen, werden keine freien Parkplätze im Voraus verteilt:

   Schließlich werden die übrigen 16 freien Parkplätze beliebig auf 13 Zwischenräume verteilt. Hierfür gibt es $\binom{16+13-1}{16} = \binom{28}{16}$ Möglichkeiten. Das ist auch die Gesamtanzahl an Parkmöglichkeiten.

2. Bei 9 verschiedenen Monstertrucks gibt es 9! verschiedene Reihenfolgen. Von den 22 freien Parkplätzen werden 8 zwischen den Monstertrucks verteilt (1 pro Zwischenraum).

Schließlich werden die übrigen 14 freien Parkplätze beliebig auf 10 Zwischenräume verteilt. Hierfür gibt es $\binom{14+10-1}{14} = \binom{23}{14}$ Möglichkeiten. Insgesamt gibt es also $9! \cdot \binom{23}{14}$ Parkmöglichkeiten.

3. Bei 3 *Snakebites*, 2 *Ghostriders* und einem *Bigfoot* gibt es $\frac{6!}{3!\cdot 2!\cdot 1!} = 60$ verschiedene Reihenfolgen. Von den 28 freien Parkplätzen werden 15 zwischen den Monstertrucks verteilt (3 pro Zwischenraum).



Schließlich werden die übrigen 13 freien Parkplätze beliebig auf 7 Zwischenräume verteilt. Hierfür gibt es $\binom{13+7-1}{13} = \binom{19}{13}$ Möglichkeiten. Insgesamt gibt es also $60 \cdot \binom{19}{13}$ verschiedene Parkmöglichkeiten.

7 Studenten bekommen am Tag der DS Klausur Sitzplätze in der ersten Reihe des Hörsaales zugewiesen. Diese besitzt 24 Sitzplätze. Wie viele mögliche Verteilungen gibt es in den folgenden Szenarien?

1. Damit sie nicht voneinander abschreiben können, sollen zwischen je zwei Studenten mindestens zwei Sitzplätze frei bleiben.
2. 3 der 7 Studenten kommen zu früh in die Klausur und legen sich auf den Sitzplätzen zum Schlafen hin. Dabei belegt jeder genau 5 Sitzplätze.
3. Nun erscheinen für die Klausur doppelt so viele Studenten wie angemeldet waren. Das heißt, dass 14 Studenten sich nun die erste Reihe teilen müssen. Dabei dürfen die äußeren zwei Sitzplätze nicht frei bleiben. Weil die Studenten alle voneinander abschreiben wollen, soll es zwischen je zwei Studenten höchstens einen freien Platz geben.

Hinweis: Natürlich sind Studenten unterscheidbar! ;-)

Wir modellieren freie Sitzplätze mit $\circ$ und belegte Sitzplätze mit $\bullet$.

1. Bei 7 Studenten gibt es 7! Reihenfolgen. Von den 17 freien Sitzplätzen werden 12 zwischen den Studenten verteilt:

$$\underset{1}{\cup}\bullet\underset{2}{\overset{\circ\circ}{\cup}}\bullet\underset{3}{\overset{\circ\circ}{\cup}}\bullet\underset{4}{\overset{\circ\circ}{\cup}}\bullet\underset{5}{\overset{\circ\circ}{\cup}}\bullet\underset{6}{\overset{\circ\circ}{\cup}}\bullet\underset{7}{\overset{\circ\circ}{\cup}}\bullet\underset{8}{\cup}$$

   Schließlich werden die übrigen 5 freien Sitzplätze beliebig auf 8 Zwischenräume verteilt. Hierfür gibt es $\binom{5+8-1}{5} = \binom{12}{5}$ Möglichkeiten. Insgesamt gibt es also $7! \cdot \binom{12}{5}$ Verteilungsmöglichkeiten.

2. Bei 3 Studenten gibt es 3! Reihenfolgen. Weil jeder von ihnen 5 Sitzplätze belegt, gibt es 9 frei Sitzplätze. Weil zwischen den Studenten keine Sitzplätze frei bleiben müssen, werden keine freien Sitzplätze im Voraus verteilt:

Schließlich werden die 9 freien Sitzplätze beliebig auf 4 Zwischenräume verteilt. Hierfür gibt es $\binom{9+4-1}{9} = \binom{12}{9}$ Möglichkeiten. Insgesamt gibt es also $3! \cdot \binom{12}{9}$ Verteilungsmöglichkeiten.

3. Bei 14 Studenten gibt es 14! Reihenfolgen. Weil zwischen den Studenten keine Sitzplätze frei bleiben müssen, werden keine freien Sitzplätze im Voraus verteilt:

Weil die äußeren Sitzplätze nicht frei sein dürfen, gibt es nur die 13 inneren Zwischenräume. Die übrigen 10 freien Sitzplätze werden also so auf 13 Zwischenräume, dass jeder Zwischenraum höchstens einen freien Platz bekommt (injektiv). Hierfür gibt es $\binom{13}{10}$ Möglichkeiten. Insgesamt gibt es also $14! \cdot \binom{13}{10}$ Verteilungsmöglichkeiten.

Themenübersicht

Rencontres-Zahlen

$D_{n,k}$ gibt die Anzahl der Permutationen einer n-elementigen Menge an, die genau k Fixpunkte besitzen.

Beispiel

Es gibt genau 6 Permutationen über [4] mit genau 2 Fixpunkten:

$$(1,2)(3)(4), \quad (1,3)(2)(4), \quad (1,4)(2)(3), \quad (1)(2,3)(4), \quad (1)(2,4)(3), \quad (1)(2)(3,4).$$

Also ist $D_{4,2} = 6$.

Noch ein Beispiel

Es gibt genau $3! = 6$ Permutationen über $[3]$. Für diese gilt:

p	$\mathrm{fix}(p)$	$\lvert\mathrm{fix}(p)\rvert$
(1)(2)(3)	$\{1,2,3\}$	3
(1,2)(3)	$\{3\}$	1
(1,3)(2)	$\{2\}$	1
(1)(2,3)	$\{1\}$	1
(1,2,3)	$\emptyset$	0
(1,3,2)	$\emptyset$	0

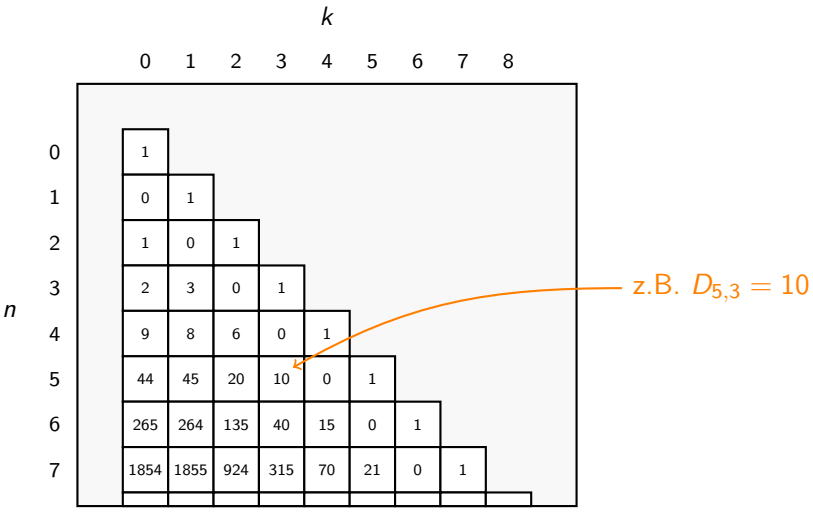
Also gilt:

$$D_{3,0} = 2, \quad D_{3,1} = 3, \quad D_{3,2} = 0 \quad \text{und} \quad D_{3,3} = 1.$$

Info

Die Werte von $D_{n,k}$ können in folgendem Dreieck abgelesen werden.

Info


k
0 1 2 3 4 5 6 7 8
n
0 1
1 0 1
2 1 0 1
3 2 3 0 1
4 9 8 6 0 1
5 44 45 20 10 0 1
6 265 264 135 40 15 0 1
7 1854 1855 924 315 70 21 0 1
z.B. $D_{5,3} = 10$

Themenübersicht

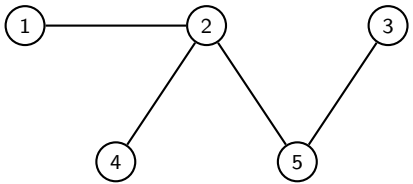
Themenübersicht

Graphen

Sei $\binom{V}{2} = \{M \subseteq V\} |M| = 2$ die Menge aller 2-elementigen Teilmengen von V. Ein Graph $G = (V, E)$ besteht aus einer Menge V von Knoten und einer Menge $E \subseteq \binom{V}{2}$ von Kanten.

Beispiel

$G = (V, E)$ mit $V = [5]$ und $E = \{\{1,2\}, \{2,4\}, \{2,5\}, \{3,5\}\}$:



Erinnerung: $[n] = \{1, \ldots, n\}$.

Infos

- Nicht irritieren lassen! $\binom{V}{2}$ ist nur eine Schreibweise und kein Binomialkoeffizient! Es gilt beispielsweise:

$$\binom{\{a,b,c\}}{2} = \{\{a,b\},\{a,c\},\{b,c\}\}.$$

  Erinnerung: Analog dazu kann man 2^A für die Potenzmenge von A oder B^A für die Menge aller Funktionen $f : A \to B$ schreiben. Dann gilt nämlich:

$$\left|2^A\right| = 2^{|A|}, \quad \left|B^A\right| = |B|^{|A|}, \quad \left|\binom{V}{2}\right| = \binom{|V|}{2}.$$

  Aber wie gesagt: Das sind nur Schreibweisen! Es heißt nicht, dass man einfach so Mengen in Potenzen oder Binomialkoeffizienten einsetzen darf, als wären sie normale Zahlen.

- Graphen sind ungerichtet, d.h. die Kanten zeigen in keine der beiden Richtungen. Deswegen zeichnet man sie als Striche und nicht als Pfeile. Die Begriffe Graph, ungerichteter Graph und einfacher Graph sind bei uns Synonyme.

Quizfragen

1. Kann ein Graph Schlingen haben?
2. Kann ein Graph Mehrfachkanten haben?
3. Wie viele Graphen mit Knotenmenge $V = [5]$ gibt es?

Hinweise:

- Eine Schlinge ist eine Kante von einem Knoten zu sich selbst.
- Eine Mehrfachkante ist eine Kante, die mehrmals vorkommt.
- Erinnerung: $[n] = \{1, \ldots, n\}$.

1. Nein! Kanten sind 2-elementige Mengen, d.h. es können keine Duplikate geben.
2. Auch nicht! Die Kanten sind in einer Menge E enthalten, d.h. wieder sind keine Duplikate erlaubt.
3. $\binom{V}{2}$ ist die Menge aller „potentiellen“ Kanten. Davon gibt es insgesamt $\binom{5}{2} = \frac{5 \cdot 4}{2 \cdot 1} = 10$ Stück. Da jede Teilmenge von $\binom{V}{2}$ eine mögliche Kantenmenge ist, entspricht die Anzahl an Graphen genau der Anzahl an Teilmengen von $\binom{V}{2}$, d.h.:

$$2^{|\binom{V}{2}|} = 2^{\binom{5}{2}} = 2^{10} = 1024.$$

Nachbarschaften, Grade, Gradfolge und k-Regularität

Sei $G = (V, E)$ ein Graph.

- Die Nachbarschaft $\Gamma(v)$ („Gamma“) von einem Knoten v ist die Menge aller Knoten die mit v durch eine Kante verbunden sind, also:

$$\Gamma(v) := \{w \in V \mid \{v, w\} \in E\}.$$

  Die Knoten in $\Gamma(v)$ werden Nachbarn von v genannt.

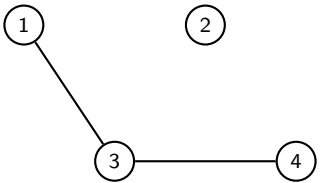
- Der Grad $\deg(v)$ eines Knotens v ist die Anzahl der Knoten, die mit v durch eine Kante verbunden sind, also:

$$\deg(v) := |\Gamma(v)|.$$

- Sei $V = \{v_1, \ldots, v_n\}$. Dann heißt $(\deg(v_1), \ldots, \deg(v_n))$ eine Gradfolge von G.
- $\Delta(G) := \max\{\deg(v) \mid v \in V\}$ ist der Maximalgrad von G.
- $\delta(G) := \min\{\deg(v) \mid v \in V\}$ ist der Minimalgrad von G.
- Besitzt G die Gradfolge $(k, k, \ldots, k)$, so heißt G k-regulär.

Beispiel

Sei $G = (V, E)$ folgender Graph:



Es gilt:

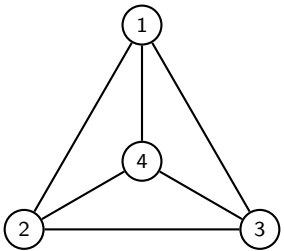
- $\Gamma(1) = \{3\}$, $\Gamma(2) = \{\}$, $\Gamma(3) = \{1, 4\}$ und $\Gamma(4) = \{3\}$.
- $\deg(1) = 1$, $\deg(2) = 0$, $\deg(3) = 2$ und $\deg(4) = 1$.
- Eine Gradfolge von G ist $(0, 1, 1, 2)$.
- Der Maximalgrad von G ist $\Delta(G) = 2$.

Beispiel

- Der Minimalgrad von G ist $\delta(G) = 0$.
- G ist nicht k-regulär.

Noch ein Beispiel

Sei $G = (V, E)$ folgender Graph:



Es gilt:

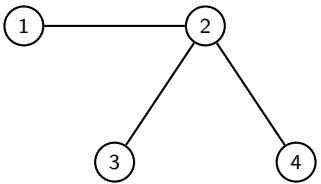
- $\Gamma(1) = \{2, 3, 4\}$, $\Gamma(2) = \{1, 3, 4\}$, $\Gamma(3) = \{1, 2, 4\}$ und $\Gamma(4) = \{1, 2, 3\}$.
- $\deg(1) = 3$, $\deg(2) = 3$, $\deg(3) = 3$ und $\deg(4) = 3$.
- Die einzige Gradfolge von G ist $(3, 3, 3, 3)$.
- Der Maximalgrad von G ist $\Delta(G) = 3$.

Noch ein Beispiel

- Der Minimalgrad von G ist $\delta(G) = 3$.
- G ist 3-regulär.

Info

Manchmal wird gefordert, dass eine Gradfolge auf- oder absteigend sortiert sein soll. Dies ist bei uns nicht der Fall. Insbesondere kann ein Graph also verschiedene Gradfolgen haben. Beispielsweise besitzt der Graph



vier verschiedene Gradfolgen: $(1, 1, 1, 3)$, $(1, 1, 3, 1)$, $(1, 3, 1, 1)$ und $(3, 1, 1, 1)$.

Wege, Pfade und Kreise

Sei $G = (V, E)$ ein Graph.

- Ein Weg der Länge k ist eine nichtleere Folge $(v_0, v_1, v_2, \ldots, v_k)$ von $k+1$ Knoten mit

$$\underbrace{\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{k-1}, v_k\}}_{k \text{ paarweise benachbarte Kanten}} \in E.$$

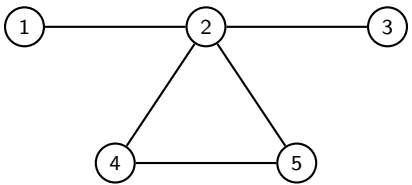
- Ein Pfad der Länge k ist ein Weg $(v_0, \ldots, v_k)$, in dem alle Knoten $v_0, \ldots, v_k$ paarweise verschieden sind.
- Ein Kreis der Länge k ($k \geq 3$) ist ein Weg $(v_0, \ldots, v_k)$, in dem alle Knoten $v_0, \ldots, v_{k-1}$ paarweise verschieden sind und $v_0 = v_k$ gilt.

Info

Graphen, die keine Kreise besitzen, nennt man kreisfrei oder azyklisch.

Beispiel

Sei $G = (V, E)$ folgender Graph:



- $(1, 2, 4, 5, 2, 3)$ ist ein Weg der Länge 5, der weder Pfad noch Kreis ist.
- $(1, 2, 3)$ ist ein Pfad der Länge 2.
- $(2, 4, 5, 2)$ ist ein Kreis der Länge 3.

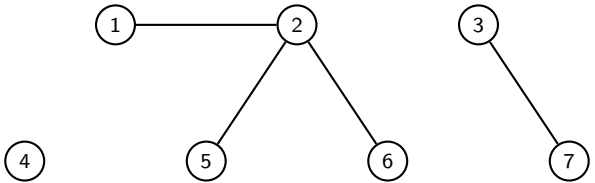
Erreichbarkeit und Zusammenhangskomponenten

Sei $G = (V, E)$ ein Graph.

- Der Knoten w ist vom Knoten v aus erreichbar, falls ein Pfad $(v, \ldots, w)$ in G existiert.
- Die Erreichbarkeit ist eine reflexive, symmetrische und transitive Relation auf Knoten, d.h. eine Äquivalenzrelation.
- Die Menge aller Knoten, die sich untereinander erreichen können, bilden eine Äquivalenzklasse und werden eine Zusammenhangskomponente von G gennant.
- Besitzt G genau eine Zusammenhangskomponente, dann nennt man G zusammenhängend.

Beispiel

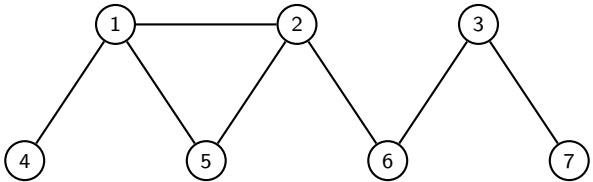
Sei $G = (V, E)$ folgender Graph:



- G hat genau 3 Zusammenhangskomponenten: $\{4\}$, $\{1, 2, 5, 6\}$ und $\{3, 7\}$.
- G ist nicht zusammenhängend.

Noch ein Beispiel

Sei $G = (V, E)$ folgender Graph:



- G hat nur eine Zusammenhangskomponente: $\{1, 2, 3, 4, 5, 6, 7\}$. D.h. jeder Knoten ist von jedem anderen aus erreichbar.
- G ist also zusammenhängend.

k-partite Graphen

Sei $G = (V, E)$ ein Graph und $k \in \mathbb{N}_0$. G heißt k-partit, falls es eine k-Partition P der Knotenmenge V gibt, so dass keine Kante vollständig in eine der Klassen enthalten ist. D.h.:

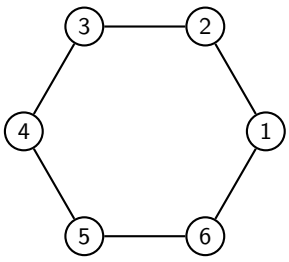
$$\forall u, v \in V, A \in P : (\{u, v\} \in E \implies \{u, v\} \not\subseteq A).$$

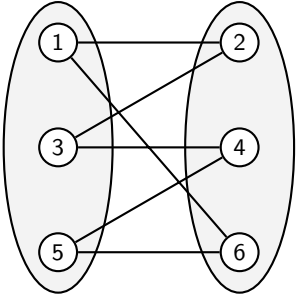
Infos

- Was eine k-Partition war kann auf Folie 45 aufgefrischt werden.
- 2-partite Graphen heißen bipartit und 3-partite tripartit.
- Dass ein Graph mehrere solcher k-Partitionen besitzt heißt nicht, dass es mehrere verschiedene k-partite Graphen sind.

Beispiel

Der folgende Graph ist bipartit.

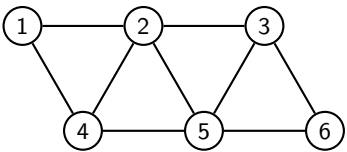


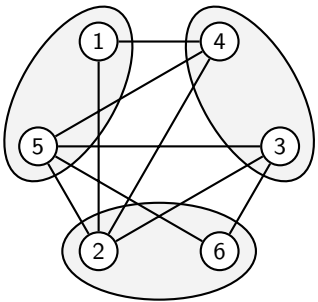


In der rechten Zeichnung wurden die Knoten umgeordnet und die zugrundeliegende Bipartition $P = \{\{1, 3, 5\}, \{2, 4, 6\}\}$ eingezeichnet.

Noch ein Beispiel

Der folgende Graph ist tripartit.

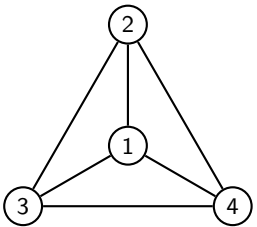


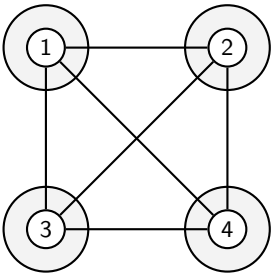


In der rechten Zeichnung wurden die Knoten umgeordnet und die zugrundeliegende Tripartition $P = \{\{1,5\},\{2,6\},\{3,4\}\}$ eingezeichnet.

Ein letztes Beispiel

Der folgende Graph ist 4-partit.





In der rechten Zeichnung wurden die Knoten umgeordnet und die zugrundeliegende 4-Partition $P = \{\{1\}, \{2\}, \{3\}, \{4\}\}$ eingezeichnet.

Quizfragen

1. Ist jeder k-partite Graph $G = (V, E)$ mit $|V| > k$ auch $(k+1)$-partit?
2. Ist jeder k-partite Graph $G = (V, E)$ mit $k > 1$ auch $(k-1)$-partit?
3. Wann ist ein Graph $G = (V, E)$ 1-partit?

1. Ja! Wenn keine Kante innerhalb einer Knotenteilmenge V_i verläuft, dann kann man V_i beliebig in zwei weitere Mengen aufteilen und innerhalb von diesen wird ebenfalls keine Kante verlaufen. Somit ist jeder Graph $G = (V, E)$ automatisch $|V|$-partit.
2. Nein! Die Graphen aus den letzten drei Beispielen können als Gegenbeispiel benutzt werden. Der Graph auf Folie 883 ist bipartit, aber nicht 1-partit, der auf Folie 884 ist tripartit, aber nicht bipartit und der auf Folie 885 ist 4-partit, aber nicht tripartit. Wäre diese Aussage auch wahr, dann wäre jeder Graph $G = (V, E)$ automatisch 1-, 2-, 3-, ... und $|V|$-partit, was echt seltsam wäre.
3. Wenn $V \neq \emptyset$ und $E = \emptyset$. Gäbe es eine Kante $\{u, v\}$ in E, dann könnten u und v nicht in derselben Klasse sein und G wäre nicht 1-partit. Andererseits, falls $V = \emptyset$, dann ist nach Folie 45 $P = \{\}$ die einzige mögliche Partition der Knotenmenge V und G wäre dann 0-partit.

Teilgraphen und induzierte Teilgraphen

Sei $G = (V, E)$ ein Graph.

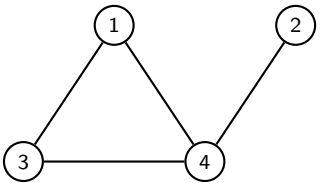
- $H = (V', E')$ heißt Teilgraph von G, falls $V' \subseteq V$ und $E' \subseteq E \cap \binom{V'}{2}$ gilt.
- $H = (V', E')$ heißt induzierter Teilgraph von G, falls $V' \subseteq V$ und $E' = E \cap \binom{V'}{2}$ gilt.

Erinnerung

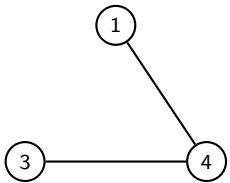
$\binom{V'}{2}$ enthält alle möglichen Kanten über der neuen Knotenmenge V'.

Beispiel

Seien $G = (V, E)$ und $H = (V', E')$ folgende Graphen:



G



H

H ist ein Teilgraph von G, aber kein induzierter Teilgraph, da $\{1, 3\} \notin E'$

Was ist an folgender Überlegung falsch?

> *Möchte man zu $G = (V, E)$ einen Teilgraph $H = (V', E')$ konstruieren, so hat man $|\mathcal{P}(V)| = 2^{|V|}$ verschiedene Möglichkeiten für V' und $|\mathcal{P}(E)| = 2^{|E|}$ für E'. G hat also*
>
> $$2^{|V|} \cdot 2^{|E|} = 2^{|V|+|E|}$$
>
> *verschiedene Teilgraphen.*

Das ist nur eine obere Schranke. Es gibt zwar genau $2^{|V|+|E|}$ Möglichkeiten ein Tupel (V', E') zu konstruieren, aber im Allgemeinen sind einige davon keine Graphen, beispielsweise wenn $\{v_i, v_j\} \in E'$ aber $v_i, v_j \notin V'$.

Deswegen kann man nur sagen, dass G höchstens so viele Teilgraphen besitzt.

Graphenisomorphie

Zwei Graphen $G = (V, E)$ und $H = (V', E')$ sind genau dann isomorph zueinander ($G \cong H$), wenn es eine Bijektion $h : V \to V'$ gibt, so dass für alle $u, v \in V$ gilt:

$$\{u, v\} \in E \iff \{h(u), h(v)\} \in E' \ .$$

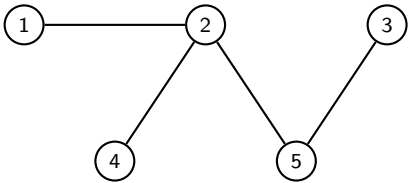
Intuitiv sind also G und H isomorph zueinander, wenn man die Knoten von G so umbenennen kann, dass G und H identisch sind.

Infos

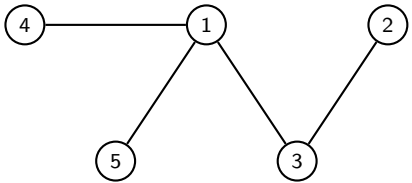
- Zwei Graphen sind isomorph zueinander, wenn sie sich nur in der Benennung der Knoten unterscheiden, d.h. wenn sie dieselbe „Form“ haben.
- Die Funktion h stellt eine mögliche Umbenennung der Knoten dar, so dass H das Ergebnis der Umbenennung der Knoten in G durch h ist. h wird Isomorphismus genannt.
- $\cong$ ist eine Äquivalenzrelation über Graphen, d.h. sie ist reflexiv, symmetrisch und transitiv.

Beispiel

Seien $G = (V, E)$ und $H = (V', E')$ folgende Graphen



G



H

Mögliche Isomorphismen $h_1, h_2 : V \to V'$ wären:

$$h_1 : 1 \mapsto 4, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 5, 5 \mapsto 3$$

und

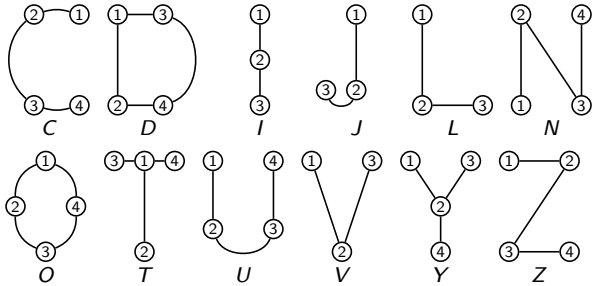
$$h_2 : 1 \mapsto 5, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 4, 5 \mapsto 3.$$

Info

Weil $\cong$ eine Äquivalenzrelation ist, gibt es für eine gegebene Menge $\mathcal{G}$ von Graphen auch eine Faktormenge $\mathcal{G}/\cong$, d.h. eine Partition von $\mathcal{G}$ in Äquivalenzklassen.

Beispiel

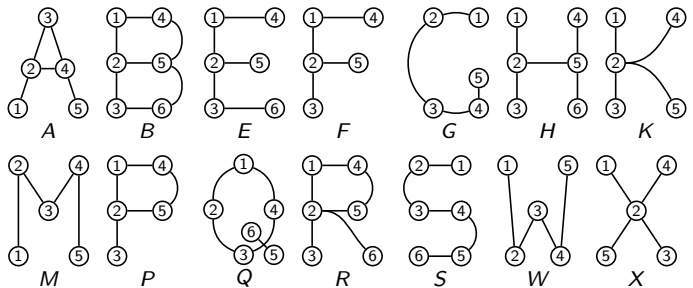
Sei $\mathcal{G} = \{C, D, I, J, L, N, O, T, U, V, Y, Z\}$ die Menge folgender Graphen.



Aus $I \cong J \cong L \cong V \ncong C \cong N \cong U \cong Z \ncong D \cong O \ncong T \cong Y$ folgt:

$$\mathcal{G}/\cong = \{\{I, J, L, V\}, \{C, N, U, Z\}, \{D, O\}, \{T, Y\}\}.$$

Sei $\mathcal{G} = \{A, B, E, F, G, H, K, M, P, Q, R, S, W, X\}$ die Menge folgender Graphen.



Welche der Graphen in $\mathcal{G}$ sind isomorph zueinander? Gib die Faktormenge $\mathcal{G}/\cong$ extensional an.

Es gilt:

$$A \cong F \ncong G \cong M \cong W \ncong K \cong X \ncong P \ncong B \ncong E \ncong H \ncong R.$$

Daraus folgt:

$$\mathcal{G}/\cong = \{\{A\}, \{F\}, \{G, M, W\}, \{K, X\}, \{P\}, \{B\}, \{E\}, \{H\}, \{R\}\}.$$

Wichtige Aussagen zu Graphen

1. Handshaking-Theorem. In jedem Graph $G = (V, E)$ gilt: $\sum_{v \in V} \deg(v) = 2|E|$.
2. Satz von Havel-Hakimi. Seien $d_1, \ldots, d_n \in \mathbb{N}_0$ mit $d_1 \leq \ldots \leq d_n$, dann gibt es genau dann einen Graph G mit Gradfolge $(d_1, \ldots, d_n)$, wenn es einen Graph G' gibt mit Gradfolge

$$(\underbrace{d_1, \ldots, d_{n-d_n-1}}_{n-d_n-1 \text{ gleich}}, \underbrace{d_{n-d_n} - 1, \ldots, d_{n-1} - 1}_{d_n \text{ mit „}-1\text{“}}).$$

3. Für jeden Graph $G = (V, E)$ gilt:
   - Es gibt eine Zusammenhangskomponente in G mit mindestens $\Delta(G) + 1$ Knoten.
   - Jede Zusammenhangskomponente in G besitzt mindestens $\delta(G) + 1$ Knoten.

Wichtige Aussagen zu Graphen

4. Für jeden Graph $G = (V, E)$ gilt:

G zusammenhängend	$\Longrightarrow$	$\lvert V\rvert \leq \lvert E\rvert + 1$	
G kreisfrei	$\Longrightarrow$	$\lvert V\rvert \geq \lvert E\rvert + 1$	
G kreisfrei	$\Longrightarrow$	$\lvert\{v \in V \mid \deg(v) = 1\}\rvert \geq 2$	(falls $\lvert V\rvert \geq 2$)
G kreisfrei	$\Longrightarrow$	G bipartit	(falls $\lvert E\rvert \geq 1$)
G bipartit	$\Longrightarrow$	$4\lvert E\rvert \leq \lvert V\rvert^2$	
$\Delta(G) + \delta(G) + 1 \geq \lvert V\rvert$	$\Longrightarrow$	G zusammenhängend	(folgt aus 3.)

Quizfragen

1. Gibt es für jedes $n \in \mathbb{N}$ einen 3-regulären Graph G mit n Knoten?
2. Gibt es einen Graph G mit Gradfolge $(1, 2, 3, 3, 3, 4, 4)$?
3. Gibt es einen Graph G mit Gradfolge $(2, 4, 4, 6, 6, 6, 7, 7)$?
4. Gibt es einen zusammenhängenden Graph G mit Gradfolge $(1, 1, 1, 1, 1, 1, 2, 2, 2, 3, 3)$?
5. Ist jeder Graph G mit Gradfolge $(2, 2, 3, 3, 4, 4, 6)$ zusammenhängend?
6. Ist jeder Graph G mit Gradfolge $(2, 2, 2, 3, 4, 5, 5, 6, 6, 7, 8)$ zusammenhängend?

1. Nein! Aus dem Handshaking-Theorem folgt, dass die Summe aller Grade gerade sein muss. Für n ungerade gibt es also keinen solchen Graph.
2. Ja! Aus dem Satz von Havel-Hakimi folgt, dass G genau dann existiert, wenn ein Graph mit Gradfolge $(0, 0, 0)$ (3 Knoten, keine Kanten) existiert.

Schritt	Gradfolge von G	Gradfolge von G'
1	$(1, 2, 3, 3, 3, 4, 4)$	$(1, 2, 2, 2, 2, 3)$
2	$(1, 2, 2, 2, 2, 3)$	$(1, 2, 1, 1, 1)$
3	$(1, 1, 1, 1, 2)$	$(1, 1, 0, 0)$
4	$(0, 0, 1, 1)$	$(0, 0, 0)$

Alternative Schreibweise:

$$(1,2,3,3,3,4,4) \xrightarrow{\text{HH}} (1,2,2,2,2,3) \xrightarrow{\text{HH}} (1,2,1,1,1) \xrightarrow{\text{sort}_\downarrow} (1,1,1,1,2)$$
$$\xrightarrow{\text{HH}} (1,1,0,0) \xrightarrow{\text{sort}_\downarrow} (0,0,1,1) \xrightarrow{\text{HH}} (0,0,0)$$

3. Nein! Aus dem Satz von Havel-Hakimi folgt, dass G genau dann existiert, wenn ein Graph mit Gradfolge $(0, -1, -1)$ existiert, was unmöglich ist.

Schritt	Gradfolge von G	Gradfolge von G'
1	$(2, 4, 4, 6, 6, 6, 7, 7)$	$(1, 3, 3, 5, 5, 5, 6)$
2	$(1, 3, 3, 5, 5, 5, 6)$	$(0, 2, 2, 4, 4, 4)$
3	$(0, 2, 2, 4, 4, 4)$	$(0, 1, 1, 3, 3)$
4	$(0, 1, 1, 3, 3)$	$(0, 0, 0, 2)$
5	$(0, 0, 0, 2)$	$(0, -1, -1)$

Alternative Schreibweise:

$$(2, 4, 4, 6, 6, 6, 7, 7) \xrightarrow{\text{HH}} (1, 3, 3, 5, 5, 5, 6) \xrightarrow{\text{HH}} (0, 2, 2, 4, 4, 4)$$
$$\xrightarrow{\text{HH}} (0, 1, 1, 3, 3) \xrightarrow{\text{HH}} (0, 0, 0, 2) \xrightarrow{\text{HH}} (0, -1, -1,)$$

4. Nein! Für $G = (V, E)$ würde gelten: $|V| = 11$ und $|E| = \frac{3+3+2+2+2+1+1+1+1+1+1}{2} = 9$. Wegen $|V| > |E| + 1$ kann G nicht zusammenhängend sein.

5. Ja! Für $G = (V, E)$ gilt $|V| = 7$ und $\Delta(G) = 6$, d.h. G besitzt eine Zusammenhangskomponente, die so groß ist, wie die Anzahl an Knoten.

6. Ja! Wegen $\Delta(G) = 8$ besitzt $G = (V, E)$ eine Zusammenhangskomponente mit mindestens 9 Knoten. Wegen $\delta(G) = 2$ hat jede Zusammenhangskomponente mindestens 3 Knoten. Damit G aus mindestens zwei Zusammenhangskomponenten besteht, müsste $|V| \geq 9 + 3 = 12$ gelten, was nicht stimmt. Deswegen gilt die Implikation:

$$\Delta(G) + \delta(G) + 1 \geq |V| \quad \Longrightarrow \quad G \text{ zusammenhängend.}$$

Wichtige Klassen von Graphen

Es gibt Graphen, die immer wieder vorkommen. Diese werden auf den nächsten Folien vorgestellt.

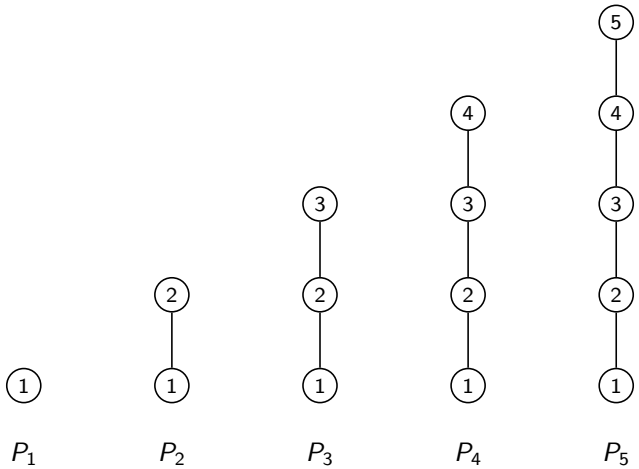
Pfade P_n

Sei $n \in \mathbb{N}$. Der Graph $G = (V, E)$ mit $V = [n]$ und

$$E = \left\{ \{u, v\} \in \binom{V}{2} \,\middle|\, v = u + 1 \right\}$$

heißt Pfad P_n.

Beispiele



Quizfrage

Wie viele Kanten besitzt P_n?

Eine weniger als es Knoten gibt. D.h.:

$$|E| = n - 1.$$

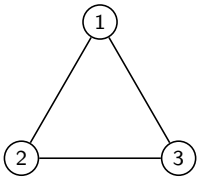
Kreise C_n

Sei $n \in \mathbb{N}$ eine natürliche Zahl mit $n \geq 3$ und $V = \{v_0, \ldots, v_{n-1}\}$ eine beliebige n-elementige Menge. Der Graph $G = (V, E)$ mit

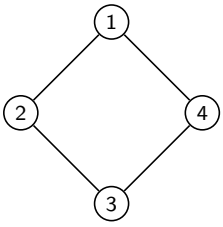
$$E = \left\{ \{v_i, v_j\} \in \binom{V}{2} \,\middle|\, j = (i+1) \bmod n \right\}$$

heißt Kreis C_n.

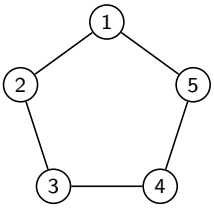
Beispiele



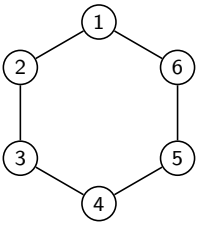
C_3



C_4



C_5



C_6

Quizfrage

Wie viele Kanten besitzt C_n?

Antwort

So viele, wie es Knoten gibt. D.h.:

$$|E| = n.$$

Vollständige Graphen K_n

Sei $n \in \mathbb{N}$ eine natürliche Zahl und $V = \{v_0, \ldots, v_{n-1}\}$ eine beliebige n-elementige Menge. Der Graph $G = (V, E)$ mit

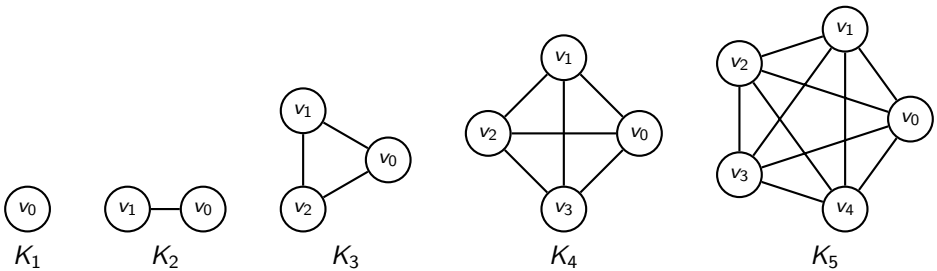
$$E = \binom{V}{2}$$

heißt vollständiger Graph K_n.

Info

In K_n ist also jeder Knoten mit jedem anderen durch eine Kante verbunden.

Beispiele



Quizfrage

Wie viele Kanten besitzt K_n?

So viele, wie es Möglichkeiten gibt, 2 Knoten aus den n zu wählen. D.h.:

$$|E| = \left|\binom{V}{2}\right| = \binom{n}{2} = \frac{n(n-1)}{2}.$$

Vollständige bipartite Graphen $K_{m,n}$

Seien $m, n \in \mathbb{N}$ natürliche Zahlen und $U = \{u_0, \ldots, u_{m-1}\}$ bzw. $V = \{v_0, \ldots, v_{n-1}\}$ beliebige m- bzw. n-elementige Mengen. Der bipartite Graph $G = (U, V, E)$ mit

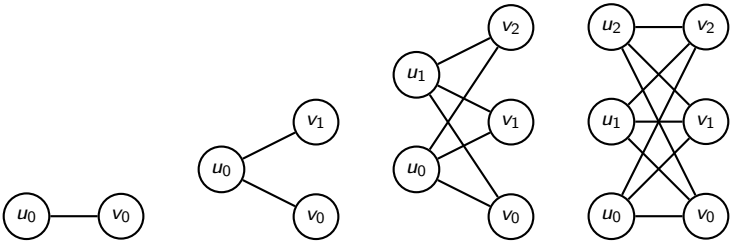
$$E = \left\{ \{v_i, v_j\} \in \binom{U \cup V}{2} \;\middle|\; v_i \in U \text{ und } v_j \in V \right\}$$

heißt vollständiger bipartiter Graph $K_{m,n}$.

Info

In $K_{m,n}$ ist also jeder Knoten aus U mit jedem aus V verbunden.

Beispiele



Quizfrage

Wie viele Kanten besitzt $K_{m,n}$?

So viele, wie es Möglichkeiten gibt, jedes der m Knoten aus U mit jedem der n Knoten aus V zu verbinden. D.h.:

$$|E| = m \cdot n.$$

Gittergraphen $M_{m,n}$

Seien $m, n \in \mathbb{N}$ natürliche Zahlen und $V = \{v_{i,j} \mid \in \{0, \ldots, m-1 \text{ und } j \in \{0, \ldots, n-1\}\}\}$ eine beliebige $(n \cdot m)$-elementige Menge. Graph $G = (V, E)$ mit

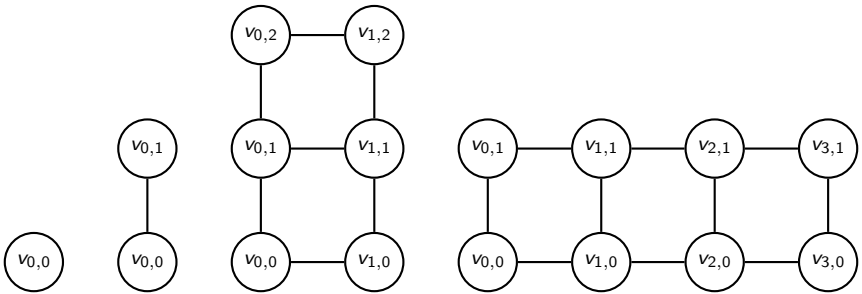
$$E = \left\{ \{v_{i,j}, v_{k,l}\} \in \binom{V}{2} \;\middle|\; |i-k| + |j-l| = 1 \right\}$$

heißt Gittergraph $M_{m,n}$.

Info

$v_{i,j}$ und $v_{k,l}$ sind also genau dann verbunden, wenn entweder i und k gleich sind und j und l sich um genau 1 unterscheiden oder j und l gleich sind und i und k sich um genau 1 unterscheiden.

Beispiele


$v_{0,0}$
$M_{1,1}$
$v_{0,1}$
$v_{0,0}$
$M_{1,2}$
$v_{0,2}$
$v_{1,2}$
$v_{0,1}$
$v_{1,1}$
$v_{0,0}$
$v_{1,0}$
$M_{2,3}$
$v_{0,1}$
$v_{1,1}$
$v_{2,1}$
$v_{3,1}$
$v_{0,0}$
$v_{1,0}$
$v_{2,0}$
$v_{3,0}$
$M_{4,2}$

Quizfrage

Wie viele Kanten besitzt $M_{m,n}$?

Es gibt $n(m-1)$ „horizontale“ und $m(n-1)$ „vertikale“ Kanten. D.h.:

$$|E| = n(m-1) + m(n-1) = 2mn - m - n.$$

Alternativ: Es gibt

- 4 Knoten mit zwei Grad 2 (die Knoten an den Ecken),
- $2(m-2) + 2(n-2)$ Knoten mit Grad 3 (die Knoten an den Seiten) und
- $(m-2)(n-2)$ Knoten mit Grad 4 (die inneren Knoten).

Mit dem Handshaking-Theorem erhalten wir:

$$|E| = \frac{2 \cdot 4 + 3 \cdot (2(m-2) + 2(n-2)) + 4 \cdot (m-2)(n-2)}{2} = 2mn - m - n.$$

Binäre Hyperwürfel Q_n

Sei $n \in \mathbb{N}_0$ eine natürliche Zahl. Der Graph $G = (V, E)$ heißt n-dimensionaler binärer Hyperwürfel Q_n, falls $V = \{0,1\}^n$ und

$$E = \left\{ \{u, v\} \in \binom{V}{2} \,\middle|\, d(u, v) = 1 \right\}$$

gelten. Der Hamming-Abstand $d(u, v)$ von u und v gibt die Anzahl der Stellen an, an denen sich u und v unterscheiden.

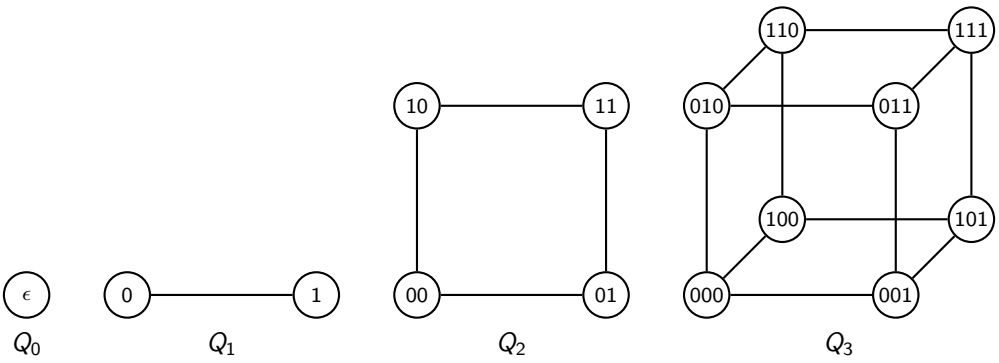
Info

Für Wörter $u = u_1 \dots u_n$ und $v = v_1 \dots v_n$ gilt:

$$d(u, v) = \sum_{i=1}^{n} |u_i - v_i|,$$

Beispiele: $d(0010, 0010) = 0$, $d(0011, 0110) = 2$ und $d(1011, 0100) = 4$.

Beispiele



Quizfrage

Wie viele Kanten besitzt Q_n?

Es gibt 2^n Knoten und jeder Knoten hat genau Grad n. Mit dem Handshaking-Theorem erhält man:

$$|E| = \frac{n \cdot 2^n}{2} = n \cdot 2^{n-1}.$$

Überblick: Wichtige Klassen von Graphen

Hier ist eine kleine Zusammenfassung der Antworten der letzten Quizfragen:

Graph	Parameter	Name	Knoten	Kanten
P_n	$n \geq 1$	Pfad	n	$n-1$
C_n	$n \geq 3$	Kreis	n	n
K_n	$n \geq 1$	Vollständiger Graph	n	$\frac{n(n-1)}{2}$
$K_{m,n}$	$m, n \geq 1$	Vollständiger bipartiter Graph	$n+m$	nm
$M_{m,n}$	$m, n \geq 1$	Gittergraph	nm	$2nm-n-m$
Q_n	$n \geq 0$	Binärer Hyperwürfel	2^n	$n2^{n-1}$

1. Für welche n und k ist P_n k-regulär?
2. Für welche n und k ist C_n k-regulär?
3. Für welche n und k ist K_n k-regulär?
4. Für welche m, n und k ist $K_{m,n}$ k-regulär?
5. Für welche m, n und k ist $M_{m,n}$ k-regulär?
6. Für welche n und k ist Q_n k-regulär?

1. P_n ist 0-regulär für $n = 1$ und 1-regulär für $n = 2$. Für $n \geq 3$ ist P_n nicht k-regulär.
2. C_n ist 2-regulär für alle $n \geq 3$.
3. K_n ist $(n-1)$-regulär für alle $n \geq 1$.
4. $K_{m,n}$ ist genau dann k-regulär, falls $k = m = n$ gilt.
5. $M_{m,n}$ ist nur dann k-regulär, wenn $m, n \leq 2$ gilt. Für $m = n = 2$ ist $M_{m,n}$ 2-regulär und für $m = n = 1$ 0-regulär. Sonst ist $M_{m,n}$ 1-regulär.
6. Q_n ist n-regulär für alle $n \geq 0$.

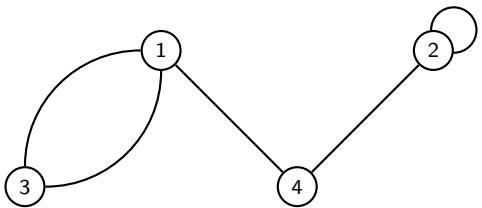
Verallgemeinerte Graphen

Ein verallgemeinerter Graph $G = (V, E)$ besteht aus einer Menge V von Knoten und einer Multimenge E von 2-elementigen Multimengen über V.

Man nennt solche Graphen auch Multigraphen.

Beispiel

$G = (V, E)$ mit $V = [4]$ und $E = \{\{\{1,3\}\}, \{\{1,3\}\}, \{\{1,4\}\}, \{\{2,2\}\}, \{\{2,4\}\}\}$:



Infos

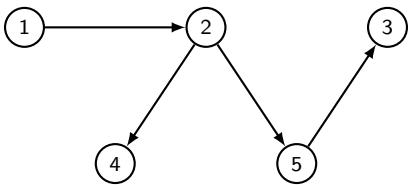
- Bei verallgemeinerten Graphen haben Kanten keine Richtung.
- Diesmal kann aber jede Kante beliebig oft vorkommen („Mehrfachkanten“).
- Auch Kanten von einem Knoten zu sich selbst („Schlingen“) sind erlaubt.

Gerichtete Graphen

Ein gerichteter Graph $G = (V, E)$ besteht aus einer Menge V von Knoten und einer Menge $E \subseteq V \times V$ von gerichteten Kanten.

Beispiel

$G = (V, E)$ mit $V = [5]$ und $E = \{(1,2), (2,4), (2,5), (5,3)\}$:



Info

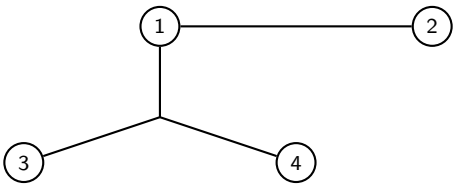
Bei gerichteten Graphen haben Kanten eine Richtung. Deswegen zeichnet man sie als Pfeile.

Hypergraphen

Ein Hypergraph $G = (V, E)$ besteht aus einer Menge V von Knoten und einer Menge $E \subseteq \mathcal{P}(V)$ von Hyperkanten.

Beispiel

$G = (V, E)$ mit $V = [4]$ und $E = \{\{1, 2\}, \{1, 3, 4\}\}$:



Infos

- Bei Hypergraphen haben Kanten keine Richtung.
- Eine Kante kann beliebig viele Knoten verbinden.

Quizfragen

1. Wie viele Kanten kann ein Graph mit n Knoten maximal haben?
2. Wie viele Kanten kann ein gerichteter Graph mit n Knoten maximal haben?
3. Wie viele verschiedene Kanten kann ein verallgemeinerter Graph mit n Knoten maximal haben?
4. Wie viele Kanten kann ein Hypergraph mit n Knoten maximal haben?

1. So viele wie, es Möglichkeiten gibt, 2 aus n Elementen ohne Zurücklegen und ohne Beachtung der Reihenfolge zu ziehen, d.h.: $\binom{n}{2} = \frac{n \cdot (n-1)}{2}$.
2. So viele wie, es Möglichkeiten gibt, 2 aus n Elementen mit Zurücklegen und mit Beachtung der Reihenfolge zu ziehen, d.h.: n^2.
3. So viele wie, es Möglichkeiten gibt, 2 aus n Elementen mit Zurücklegen und ohne Betrachtung der Reihenfolge zu ziehen, d.h.: $\binom{2+n-1}{2} = \binom{n+1}{2} = \frac{(n+1) \cdot n}{2}$.
4. So viele wie, es Teilmengen von V gibt, d.h.: 2^n.

Wichtig!

Es gibt keine Beziehung zwischen Graphen, gerichteten Graphen und Hypergraphen. Graphen sind zwar ein Spezialfall von verallgemeinerten Graphen, aber weder ein Spezialfall noch eine Verallgemeinerung von gerichteten Graphen oder Hypergraphen. Die letzten zwei stehen auch untereinander in keiner Beziehung.

Die Definitionen und Aussagen bis Folie 935 beziehen sich nur auf normale (bzw. „ungerichtete“ oder „einfache“) Graphen!

Für die gerichtete Graphen, verallgemeinerte Graphen und Hypergraphen müssten sie angepasst werden. Das wurde aber, soweit ich weiß, nicht in der Vorlesung gemacht :-)

Themenübersicht

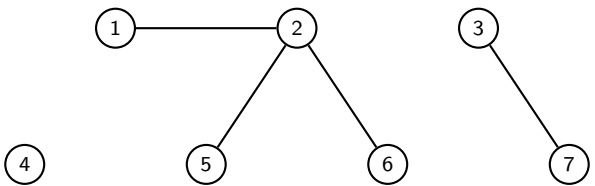
Wälder und Bäume

Sei $G = (V, E)$ ein Graph.

- G heißt Wald, falls er kreisfrei ist.
- G heißt Baum, falls er kreisfrei und zusammenhängend ist.
- Bei Bäumen und Wäldern heißen Knoten mit Grad 1 Blätter.

Beispiel

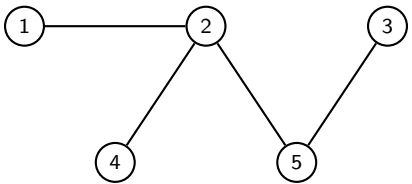
Sei $G = (V, E)$ folgender Graph:



G ist ein Wald, aber kein Baum. Die Blätter sind $1, 3, 5, 6, 7$.

Noch ein Beispiel

Sei $G = (V, E)$ folgender Graph:



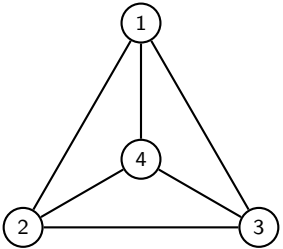
G ist ein Baum mit Blättern $1, 3, 4$.

Spannbäume

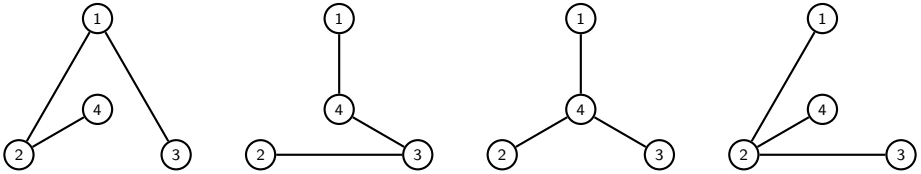
Ein Teilgraph $T = (V', E')$ von $G = (V, E)$ heißt Spannbaum von G, falls T ein Baum ist und $V' = V$ gilt.

Beispiel

Sei $G = (V, E)$ folgender Graph:



Einige Spannbäume von G sind:



Wichtige Aussagen zu Bäumen und Wäldern

1. Für jeden Graph $G = (V, E)$ gilt:

   G zshgd. $\iff$ Je zwei Knoten sind in G durch mindestens einen Pfad verbunden
   G kreisfrei $\iff$ Je zwei Knoten sind in G durch höchstens einen Pfad verbunden

2. Charakterisierung von Bäumen. Für jeden Graph $G = (V, E)$ gilt:

   G ist ein Baum $\iff$ G ist kreisfrei und zusammenhängend
   $\iff$ G ist zusammenhängend und es gilt $|V| = |E| + 1$
   $\iff$ G ist kreisfrei und es gilt $|V| = |E| + 1$
   $\iff$ Je zwei Knoten sind in G durch genau einen Pfad verbunden

Wichtige Aussagen zu Bäumen und Wäldern

3. Aus 2. folgt für jeden Graph $G = (V, E)$:

$$\begin{aligned} G \text{ Baum} &\implies G \text{ kreisfrei} \\ G \text{ Baum} &\implies G \text{ zusammenhängend} \\ G \text{ Baum} &\implies |V| = |E| + 1 \end{aligned}$$

4. Ist $T = (V, E)$ ein Baum mit $|V| \geq 2$ Knoten und $v \in V$ ein Blatt, so ist der durch $V \setminus \{v\}$ induzierte Graph ebenfalls ein Baum.

5. Jeder zusammenhängende Graph $G = (V, E)$ enthält mindestens einen Spannbaum.

6. Satz von Cayley. Es gibt genau n^{n-2} Bäume mit n Knoten.

Achtung!

Folgender logischer Schluss ist falsch:

Für jeden Graph $G = (V, E)$ gelten folgende Äquivalenzen:

$$\begin{array}{lcl} G \text{ Baum} & \iff & G \text{ zusammenhängend und kreisfrei} \\ G \text{ Baum} & \iff & G \text{ zusammenhängend und } |V| = |E| + 1 \end{array}$$

Daraus folgt:

$$G \text{ kreisfrei} \iff |V| = |E| + 1 \ .$$

Die letzte Äquivalenz gilt nur, falls G zusammenhängend ist!

Übrigens: Jeder Baum besitzt alle drei Eigenschaften kreisfrei, zusammenhängend und $|V| = |E| + 1$. Es reicht aber nur zwei davon zu beweisen, dann folgt die dritte automatisch. Von diesen drei Eigenschaften kann ein Graph also entweder keine, genau eine oder alle drei besitzen, aber niemals genau zwei.

Quizfrage

Sei $G = (V, E)$ ein Wald mit n Knoten und genau k Komponenten. Wie viele Kanten enthält G?

Jede der k Komponenten von G kann als Baum $G_i = (V_i, E_i)$ für $i = 1, \ldots, k$ betrachtet werden. Für jeden dieser Bäume gilt: $|V_i| = |E_i| + 1$. Daraus folgt:

$$\begin{aligned} |E| &= |E_1| + \ldots + |E_k| \\ &= (|V_1| - 1) + \ldots + (|V_k| - 1) \\ &= |V_1| + \ldots + |V_k| - k \\ &= |V| - k \\ &= n - k. \end{aligned}$$

Ein Wald mit n Knoten und k Komponenten hat $n - k$ Kanten.

Wichtig!

Weil das Thema Wurzelbäume bisher für die Übungsaufgaben irrelevant war, ist es auf diesen Folien nicht zu finden. Ihr findet es auf den Seiten 23-30 in den Vorlesungsfolien zum Thema Bäume.

Themenübersicht

Euler-Touren

Sei $G = (V, E)$ ein Graph.

- Eine Tour ist eine nichtleere Folge $(v_0, v_1, v_2, \ldots, v_k)$ von Knoten mit

$$\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{k-1}, v_k\} \in E$$

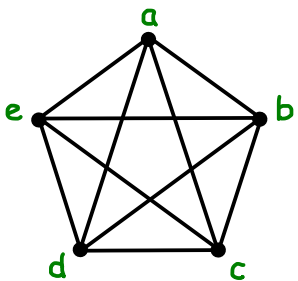
  und $v_0 = v_k$.
- Eine Tour in G, bei der jede Kante genau einmal benutzt wird, heißt Euler-Tour.
- Falls G eine Euler-Tour besitzt, dann heißt er eulersch.

Info

Touren sind Verallgemeinerungen von Kreisen bei denen die Knoten $v_0, \ldots, v_{k-1}$ nicht notwendigerweise verschieden sein müssen.

Beispiel

Der folgende Graph ist eulersch:



Eine mögliche Euler-Tour ist $(a, b, c, d, e, a, c, e, b, d, a)$.

Wichtige Aussage zu Euler-Touren

Satz von Euler. Ein Graph Graph $G = (V, E)$ ist genau dann eulersch, wenn er zusammenhängend ist und alle Knoten in ihm geraden Grad haben. D.h.:

$$G \text{ eulersch} \iff G \text{ zusammenhängend und } \forall v \in V : \deg(v) \text{ gerade} \ .$$

Info

Dieser Satz ist sowohl eine notwendige, als eine hinreichende Bedingung für Euler-Touren.

Quizfragen

1. Gibt es einen eulerschen Graph G mit Gradfolge $(2, 2, 3, 3, 4, 4)$?
2. Gibt es einen eulerschen Graph G mit Gradfolge $(2, 2, 2, 2, 2, 2)$?
3. Ist jeder Graph G mit Gradfolge $(2, 2, 2, 2, 2, 2)$ eulersch?

Antworten

1. Nein! G besitzt Knoten mit Grad 3 (ungerade).
2. Ja! Ein Kreis mit 6 Knoten, d.h. der C_6.
3. Nein! Es gibt auch nicht-zusammenhängende Graphen mit Gradfolge $(2, 2, 2, 2, 2, 2)$, z.B. zwei Kreise mit jeweils 3 Knoten.

Quizfragen

1. Für welche n ist P_n eulersch?
2. Für welche n ist C_n eulersch?
3. Für welche n ist K_n eulersch?
4. Für welche m und n ist $K_{m,n}$ eulersch?
5. Für welche m und n ist $M_{m,n}$ eulersch?
6. Für welche n ist Q_n eulersch?

Info: Alle 6 Graphen sind zusammenhängend. Es muss also nur überprüft werden, ob jeder Knoten einen geraden Grad besitzt.

1. P_n ist nur für $n = 1$ eulersch, weil er sonst mindestens einen Knoten mit Grad 1 besitzt.
2. C_n ist für alle $n \geq 3$ eulersch, da alle Knoten Grad 2 haben.
3. Jeder Knoten in K_n hat Grad $n - 1$. K_n ist also genau dann eulersch, wenn n ungerade ist.
4. Die Knoten in $K_{m,n}$ haben Grad n oder m. $K_{m,n}$ ist also genau dann eulersch, wenn m und n gerade sind.
5. $M_{m,n}$ ist nur für $m = n = 1$ oder $m = n = 2$ eulersch, sonst gibt es Knoten mit Grad 1 oder 3.
6. Jeder Knoten in Q_n hat Grad n. Q_n ist also genau dann eulersch, wenn n gerade ist.

Themenübersicht

Definition

Eine Knotenfärbung eines Graphen $G = (V, E)$ mit k Farben ist eine Abbildung $c : V \to [k]$, so dass keine benachbarte Knoten dieselbe Farbe haben. Es gilt also für alle Knoten $v_1, v_2 \in V$:

$$\{v_1, v_2\} \in E \quad \Longrightarrow \quad c(v_1) \neq c(v_2).$$

Die chromatische Zahl $\chi(G)$ („*Chi* von G“) von G ist die minimale Anzahl an Farben, die für eine Knotenfärbung von G benötigt werden.

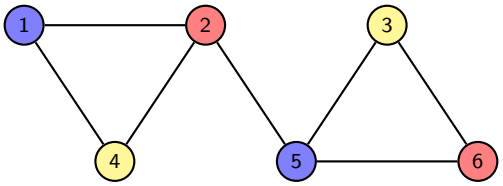
Infos

- Statt $\{\text{blau}, \text{rot}, \text{gelb}, \ldots\}$ ist unsere Farbpalette $[k] = \{1, \ldots, k\}$.
- Der Ausdruck $c(v)$ gibt die Farbe des Knotens v an.
- Der chromatische Index $\chi'(G)$ war bis 2005 Teil des DS-Stoffes. Er gibt die minimale Anzahl an Farben für eine Kantenfärbung von G an. In einer Kantenfärbung dürfen keine zwei benachbarten Kanten dieselbe Farbe haben, d.h. für alle $e_1, e_2 \in E$:

$$e_1 \cap e_2 \neq \emptyset \quad \Longrightarrow \quad c(e_1) \neq c(e_2).$$

Beispiel

Sei $G = (V, E)$ wieder folgender Graph:



G kann wie folgt gefärbt werden:

$$c(1) = 1\ ,\ c(2) = 2\ ,\ c(3) = 3\ ,\ c(4) = 3\ ,\ c(5) = 1\ ,\ c(6) = 2.$$

Man könnte ihn auch mit 4, 5 oder 6 Farben färben. Weil aber G Dreiecke enthält, ist das mit weniger als 3 Farben unmöglich. Die chromatische Zahl von G ist also

$$\chi(G) = 3.$$

1. Was ist $\chi(P_n)$ in Abhängigkeit von n?
2. Was ist $\chi(C_n)$ in Abhängigkeit von n?
3. Was ist $\chi(K_n)$ in Abhängigkeit von n?
4. Was ist $\chi(K_{m,n})$ in Abhängigkeit von m und n?
5. Was ist $\chi(M_{m,n})$ in Abhängigkeit von m und n?
6. Was ist $\chi(Q_n)$ in Abhängigkeit von n?

1. $\chi(P_n) = \begin{cases} 1 & \text{falls } n = 1 \\ 2 & \text{sonst} \end{cases}$.
2. $\chi(C_n) = \begin{cases} 2 & \text{falls } n \text{ gerade} \\ 3 & \text{sonst} \end{cases}$.
3. $\chi(K_n) = n$.
4. $\chi(K_{m,n}) = 2$.
5. $\chi(M_{m,n}) = \begin{cases} 1 & \text{falls } n = 1 \text{ und } m = 1 \\ 2 & \text{sonst} \end{cases}$.
6. $\chi(Q_n) = \begin{cases} 1 & \text{falls } n = 1 \\ 2 & \text{sonst} \end{cases}$.

Wichtige Aussagen zur Färbbarkeit von Graphen

1. Für jeden Graph $G = (V, E)$ mit $|V| \geq k$ gilt:

$$G \text{ ist } k\text{-partit} \iff G \text{ ist } k\text{-färbbar} \iff \chi(G) \leq k \ .$$

2. Für jeden Graph $G = (V, E)$ gilt:

$$\begin{array}{lll} G \text{ planar} & \Longrightarrow & \chi(G) \leq 4 \quad \text{(Vier-Farben-Satz)} \\ G \text{ Baum} & \Longrightarrow & \chi(G) = 2 \quad \text{(falls } |V| \geq 2\text{)} \end{array}$$

3. Greedy-Färbung. Für jeden Graph G gilt:

$$\chi(G) \leq \Delta(G) + 1.$$

Themenübersicht

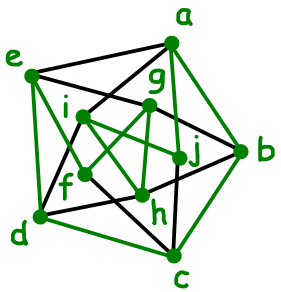
Hamilton-Kreise

Sei $G = (V, E)$ ein Graph.

- Ein Kreis in G, bei dem jeder Knoten genau einmal besucht wird, heißt Hamilton-Kreis.
- Falls G einen Hamilton-Kreis besitzt, dann heißt er hamiltonsch.

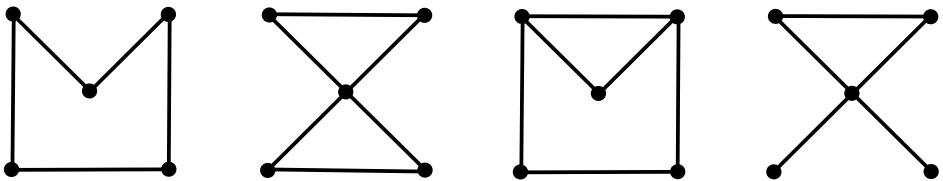
Beispiel

Der folgende Graph ist hamiltonsch:



Ein möglicher Hamilton-Kreis ist $(a, b, c, d, e, f, g, h, i, j, a)$.

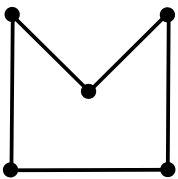
Gegeben seien folgende Graphen:



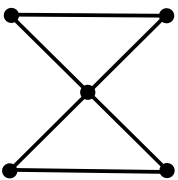
G_1 G_2 G_3 G_4

Welche davon sind eulersch und welche hamiltonsch?

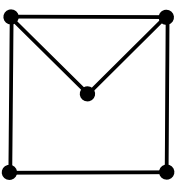
Antworten



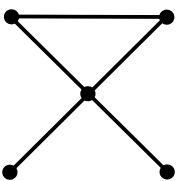
eulersch ✓
hamiltonsch ✓



eulersch ✓
hamiltonsch ✗



eulersch ✗
hamiltonsch ✓



eulersch ✗
hamiltonsch ✗

Wichtige Aussagen zu Hamilton-Kreisen

1. Kriterium von Ore. Jeder zusammenhängende Graph $G = (V, E)$ mit $|V| \geq 3$, bei dem die Summe der Grade je zwei nicht-benachbarter Knoten mindestens $|V|$ ist, ist hamiltonsch.
2. Für jeden Graph $G = (V, E)$ gilt:

$$\begin{array}{lcll} \delta(G) \geq \frac{|V|}{2} & \Longrightarrow & G \text{ hamiltonsch} & \text{(folgt aus 1.)} \\ G \text{ hamiltonsch} & \Longrightarrow & \forall v \in V : \deg(v) \geq 2 & \text{(ist logisch ;-))} \end{array}$$

3. Für jeden bipartiten Graph $G = (V_1, V_2, E)$ gilt:

$$G \text{ hamiltonsch} \quad \Longrightarrow \quad |V_1| = |V_2| \quad \text{(folgt aus TA 11.2)}$$

Info

Das Kriterium von Ore ist, im Gegensatz zum Satz von Euler, nur eine hinreichende Bedingung. Ein Graph kann insbesondere hamiltonsch sein, ohne diese Bedingung zu erfüllen!

Quizfragen

1. Für welche n ist P_n hamiltonsch?
2. Für welche n ist C_n hamiltonsch?
3. Für welche n ist K_n hamiltonsch?
4. Für welche m und n ist $K_{m,n}$ hamiltonsch?

1. P_n ist nur für $n = 1$ hamiltonsch.
2. C_n ist für alle $n \geq 3$ hamiltonsch.
3. K_n ist für alle $n \geq 1$ hamiltonsch (jede Anordnung $(v_1, \ldots, v_n)$ der Knoten ist ein Hamilton-Kreis).
4. $K_{m,n}$ ist nur für $m, n \geq 2$ und $m = n$ hamiltonsch. Dass $K_{m,n}$ für $m \leq 1$, $n \leq 1$ oder $m \neq n$ nicht hamiltonsch sein kann, erkennt man leicht. Für $n \geq 2$ enthält $K_{n,n}$ genau $2n$ Knoten mit jeweils Grad n. Somit ist die Summe der Grade zweier beliebiegen Knoten mindestens $2n$ und der Graph ist nach dem Kriterium von Ore hamiltonsch.

Themenübersicht

Matchings

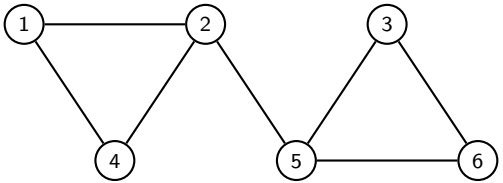
Sei $G = (V, E)$ ein Graph. Ein Matching M ist eine Menge $M \subseteq E$ von paarweise disjunkten Kanten.

Ein Matching ist perfekt, falls jeder Knoten zu genau einer Kante von M gehört, d.h. falls gilt:

$$|M| = \frac{|V|}{2}.$$

Beispiel

Sei $G = (V, E)$ wieder folgender Graph:



- $M_1 = \{\{1,2\},\{2,5\},\{3,6\}\}$ ist kein Matching, weil die Kanten $\{1,2\}$ und $\{2,5\}$ nicht disjunkt sind.
- $M_2 = \{\{1,2\},\{5,6\}\}$ ist ein Matching, aber kein perfektes Matching, weil die Knoten 3 und 4 in M_2 nicht vorkommen.
- $M_3 = \{\{1,4\},\{2,5\},\{3,6\}\}$ ist ein perfektes Matching.

Heiratssatz von Hall

Für einen bipartiten Graphen $G = (V_1, V_2, E)$ gibt es genau dann ein Matching M der Kardinalität $|V_1|$, wenn gilt:

$$\forall X \subseteq V_1 : |\Gamma(X)| \geq |X|.$$

Hierbei ist $\Gamma(X)$ die Menge der Nachbarn aller Knoten aus X.

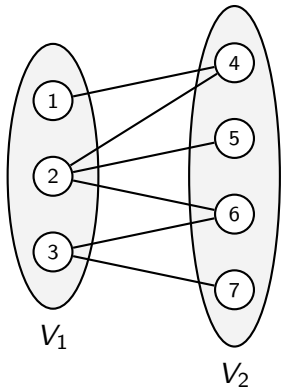
Info

Eine sehr sehr wichtige Folgerung von diesem Satz ist, dass jeder bipartite, k-reguläre Graph G ein perfektes Matching hat. D.h.:

$$G \text{ bipartit und } k\text{-regulär} \implies G \text{ hat perfektes Matching } .$$

Beispiel

Sei $G = (V_1, V_2, E)$ folgender bipartite Graph:



X	$\Gamma(X)$
$\{\}$	$\{\}$
$\{1\}$	$\{4\}$
$\{2\}$	$\{4, 5, 6\}$
$\{3\}$	$\{6, 7\}$
$\{1, 2\}$	$\{4, 5, 6\}$
$\{1, 3\}$	$\{4, 6, 7\}$
$\{2, 3\}$	$\{4, 5, 6, 7\}$
$\{1, 2, 3\}$	$\{4, 5, 6, 7\}$

Beispiel

Da für alle $X \subseteq V_1$ die Ungleichung $|X| \leq |\Gamma(X)|$ gilt, gibt es ein Matching M mit $|M| = |V_1| = 3$, z.B.:

$$M = \{\{1,4\},\{2,5\},\{3,6\}\}.$$

Wichtig!

Weil das Thema Stabile Heiraten sehr selten in Übungsaufgaben vorkommt, ist es auf diesen Folien nicht zu finden. Falls das Thema im aktuellen Semester relevant ist, solltet ihr euch unbedingt die Vorlesungsfolien dazu anschauen.

Wichtige Aussagen zu Matchings

1. Heiratssatz von Hall. Für einen bipartiten Graphen $G = (V_1, V_2, E)$ gibt es genau dann ein Matching M der Kardinalität $|V_1|$, wenn gilt:

$$\forall X \subseteq V_1 : |\Gamma(X)| \geq |X|.$$

2. Für jeden Graph $G = (V, E)$ gilt:

$$G \text{ hat perfektes Matching} \implies |V| \text{ ist gerade}$$

3. Für jeden bipartiten Graph $G = (V_1, V_2, E)$ gilt:

$$\begin{array}{lll} G \text{ ist } k\text{-regulär} & \implies & G \text{ hat perfektes Matching} \quad \text{(folgt aus 1.)} \\ G \text{ hat perfektes Matching} & \implies & |V_1| = |V_2| \end{array}$$

Quizfragen

1. Für welche n besitzt P_n ein perfektes Matching?
2. Für welche n besitzt C_n ein perfektes Matching?
3. Für welche n besitzt K_n ein perfektes Matching?
4. Für welche m und n besitzt $K_{m,n}$ ein perfektes Matching?
5. Für welche m und n besitzt $M_{m,n}$ ein perfektes Matching?
6. Für welche n besitzt Q_n ein perfektes Matching?

1. P_n besitzt genau dann ein perfektes Matching, wenn n gerade ist.
2. C_n besitzt genau dann ein perfektes Matching, wenn n gerade ist.
3. K_n besitzt genau dann ein perfektes Matching, wenn n gerade ist.
4. $K_{m,n}$ besitzt genau dann ein perfektes Matching, wenn $m = n$ gilt.
5. $M_{m,n}$ besitzt genau dann ein perfektes Matching, wenn m oder n gerade sind.
6. Q_n besitzt für alle $n \geq 1$ ein perfektes Matching.

Themenübersicht

Planarität von Graphen

Ein Graph ist planar bzw. eben, falls man ihn auf einer Ebene zeichnen kann, so dass sich keine Kanten überschneiden.

Info

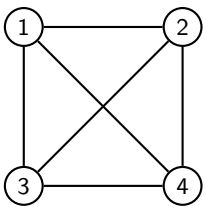
Man darf Knoten beliebig positionieren und Kanten verbiegen!

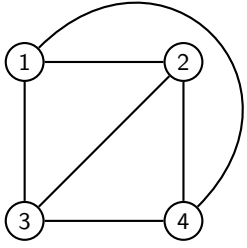
Rezept

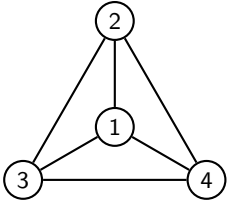
Frage: Wie zeigt man, dass ein Graph planar ist?
Methode: Durch eine schöne Zeichnung :-)

Beispiel

Der folgende Graph ist planar.

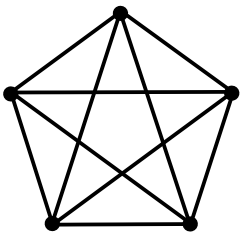




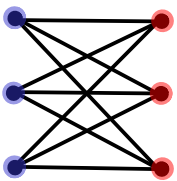


Satz von Kuratowski

- Ein Graph ist genau dann nicht planar, wenn er einen Teilgraph H besitzt, der eine Unterteilung des K_5 oder des $K_{3,3}$ ist.



K_5



$K_{3,3}$

- Eine *Unterteilung* eines Graphen G ist ein Graph, der dadurch entsteht, in dem Kanten von G durch Pfade ersetzt werden.

Infos

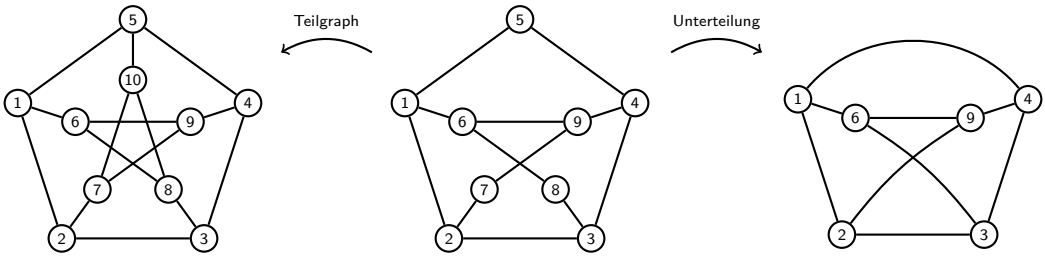
- Jeder Graph ist ein Teilgraph von sich selbst.
- Jeder Graph ist eine Unterteilung von sich selbst.

Rezept

Frage: Wie zeigt man, dass ein Graph G nicht planar ist?
Methode: Man findet einen Teilgraph H von G, der eine Unterteilung des K_5 oder des $K_{3,3}$ ist. (Der Graph H kann auch genau K_5 oder $K_{3,3}$ sein.)

Beispiel

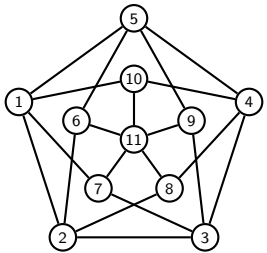
Der folgende Graph G ist nicht planar, weil er einen Teilgraph H besitzt, der eine Unterteilung des $K_{3,3}$ ist.



Die Partitionsklassen des $K_{3,3}$ sind hier $\{1, 3, 9\}$ und $\{2, 4, 6\}$.

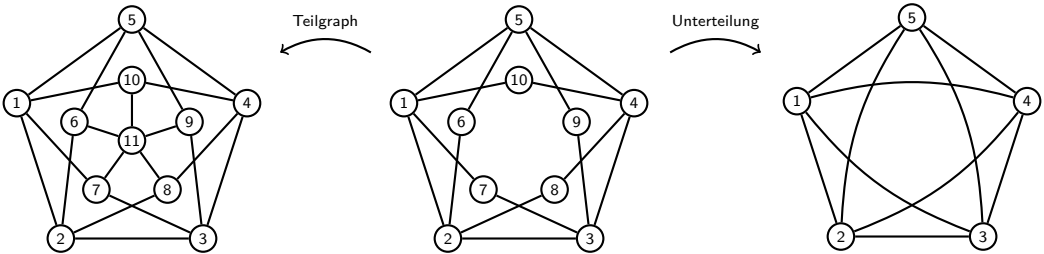
Quizfrage

Ist der folgende Graph G planar?

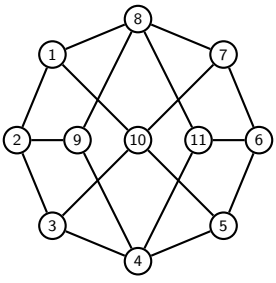


G

Der Graph G ist nicht planar, weil er einen Teilgraph H besitzt, der eine Unterteilung des K_5 ist.

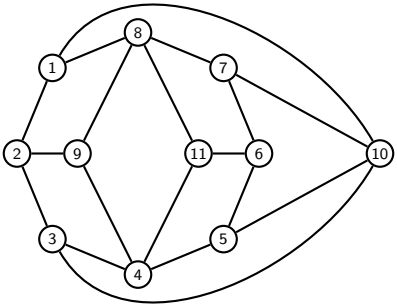


Ist der folgende Graph G planar?



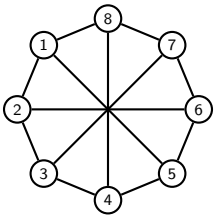
G

G ist planar, weil man den mittleren Knoten auch woanders zeichnen kann.



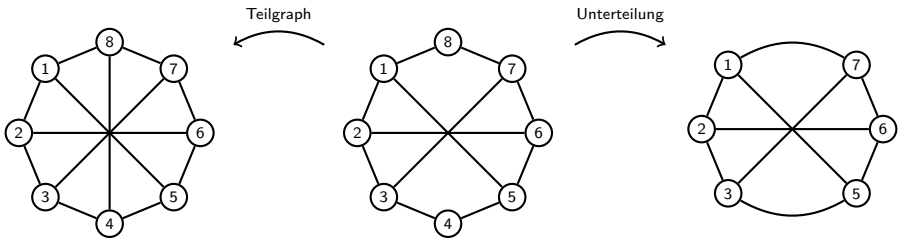
G

Ist der folgende Graph G planar?



G

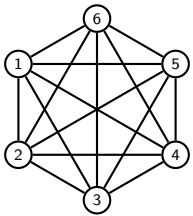
Der Graph G ist nicht planar, weil er einen Teilgraph H besitzt, der eine Unterteilung des $K_{3,3}$ ist.



Die Partitionsklassen des $K_{3,3}$ sind h $\{1, 3, 6\}$ und $\{2, 5, 7\}$.

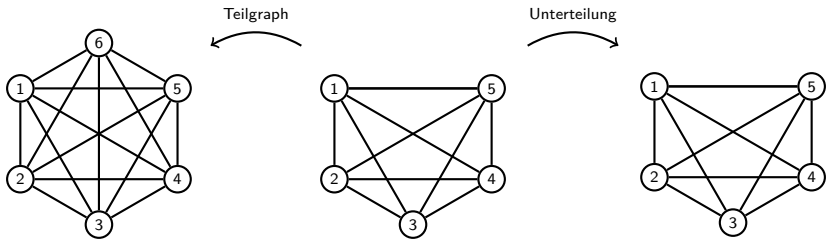
Quizfrage

Ist der folgende Graph G planar?



G

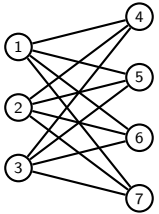
Der Graph G ist nicht planar, weil er einen Teilgraph H besitzt, der eine Unterteilung des K_5 ist.



In diesem Fall sind H und K_5 gleich.

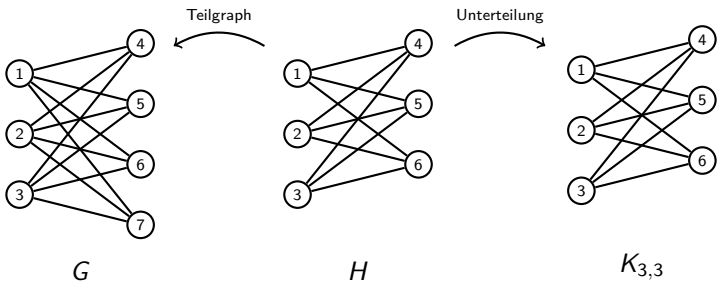
Quizfrage

Ist der folgende Graph G planar?



G

Der Graph G ist nicht planar, weil er einen Teilgraph H besitzt, der eine Unterteilung des $K_{3,3}$ ist.



In diesem Fall sind H und $K_{3,3}$ gleich. Die Partitionsklassen des $K_{3,3}$ sind hier $\{1, 2, 3\}$ und $\{4, 5, 6\}$.

Eulersche Polyederformel

Sei $G = (V, E)$ ein planarer Graph.

- Falls G zusammenhängend ist, dann gilt:

$$|R| = |E| - |V| + 2 \ .$$

- Falls G genau k Zusammenhangskomponenten besitzt, dann folgt daraus:

$$|R| = |E| - |V| + k + 1 \ .$$

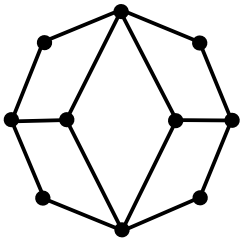
R ist die Menge aller Gebiete (engl. *regions*).

Info

Ein Gebiet ist einfach ein Stück Zeichenfläche, das von Kanten eingeschlossen wird. Das „äußere“ Gebiet zählt auch mit!

Beispiel

Sei G wieder folgender Graph:



Für die Anzahl $|R|$ der Gebiete in G gilt:

$$|R| = |E| - |V| + 2 = 14 - 10 + 2 = 6.$$

Wichtige Aussagen zur Planarität von Graphen

1. Eulersche Polyederformel. Für die Anzahl $|R|$ der Gebiete eines zusammenhängenden planaren Graphen $G = (V, E)$ gilt:

$$|R| = |E| - |V| + 2.$$

2. Für jeden Graph $G = (V, E)$:

$$\begin{array}{lcll} G \text{ planar} & \Longrightarrow & |E| \leq 3 \cdot |V| - 6 & (\text{falls } |V| \geq 3) \\ G \text{ planar} & \Longrightarrow & \exists v \in V : \deg(v) \leq 5 & \\ G \text{ kreisfrei} & \Longrightarrow & G \text{ planar} & \end{array}$$

3. Satz von Kuratowski. Ein Graph $G = (V, E)$ ist genau dann nicht planar, wenn er einen Teilgraph besitzt, der eine Unterteilung von K_5 oder $K_{3,3}$ ist. Daraus folgt:

$$\underbrace{|\{v \in V\} \deg(v) \geq 4|}_{\substack{\text{Anzahl der Knoten} \\ \text{mit mindestens Grad 4}}} < 5 \text{ und } \underbrace{|\{v \in V\} \deg(v) \geq 3|}_{\substack{\text{Anzahl der Knoten} \\ \text{mit mindestens Grad 3}}} < 6 \quad \Longrightarrow \quad G \text{ planar}$$

Quizfragen

1. Gibt es einen planaren Graph G mit Gradfolge $(6, 6, 6, 6, 6, 6, 7, 7, 8, 8, 8)$?
2. Gibt es einen nicht-planaren Graph G mit Gradfolge $(1, 2, 2, 2, 3, 4, 4, 4, 4)$?
3. Wie viele Gebiete besitzt ein planarer Graph $G = (V, E)$ mit k Zusammenhangskomponenten in Abhängigkeit von $|V|$, $|E|$ und k?

1. Nein! Kein Knoten v hat Grad $\deg(v) \leq 5$ bzw. es gilt: $|E| = 37 > 27 = 3 \cdot |V| - 6$.
2. Nein! Damit G einen Teilgraph enthält, der eine Unterteilung von K_5 oder $K_{3,3}$ sollte er mindestens 5 Knoten mit mindestens Grad 4 oder mindestens 6 Knoten mit mindestens Grad 3. Dies ist nicht der Fall.
3. G besteht aus k planeren Graphen $G_i = (V_i, E_i)$ mit $|R_i|$ Gebieten für $i = 1, \ldots, k$. Das „äußere Gebiet“ ist das einzige Gebiet, was sie alle gemeinsam haben. Daraus folgt:

$$\begin{aligned}
|R| &= (|R_1| - 1) + \ldots + (|R_k| - 1) + 1 \\
&= |R_1| + \ldots + |R_k| - k + 1 \\
&= (|E_1| - |V_1| + 2) + \ldots + (|E_k| - |V_k| + 2) - k + 1 \\
&= |E_1| + \ldots + |E_k| - |V_1| - \ldots - |V_k| + 2k - k + 1 \\
&= |E| - |V| + k + 1.
\end{aligned}$$

Quizfragen

1. Für welche n ist P_n planar?
2. Für welche n ist C_n planar?
3. Für welche n ist K_n planar?
4. Für welche m und n ist $K_{m,n}$ planar?
5. Für welche m und n ist $M_{m,n}$ planar?

Antworten

1. P_n ist für alle $n \geq 1$ planar.
2. C_n ist für alle $n \geq 3$ planar.
3. K_n ist nur für $n \leq 4$ planar.
4. $K_{m,n}$ ist nur für $m, n \leq 2$ planar.
5. $M_{m,n}$ ist für alle $m, n \geq 1$ planar.

Themenübersicht

Prüfer-Code

Sei $n \in \mathbb{N}$ mit $n \geq 2$. Der Prüfer-Code c zu einem Baum $T = ([n], E)$ ist ein $(n-2)$-Tupel

$$c = (c_1, c_2, \ldots, c_{n-2})$$

mit $c_1, c_2, \ldots, c_{n-2} \in [n]$. Dabei gilt:

- Jeder Baum lässt sich durch genau einen Prüfer-Code darstellen.
- Jeder Prüfer-Code stellt genau einen Baum dar.

Rezept

Frage: Wie kodiert und dekodiert man Bäume mit dem Prüfer-Code?
Methoden:

(1) Von Baum zu Code:

1. Solange der Baum mehr als 2 Knoten hat, wiederhole:
2. Entferne das kleinste Blatt vom Baum und füge seinen einzigen Nachbarn in den Code hinzu;
3. Die letzten zwei Knoten einfach ignorieren;

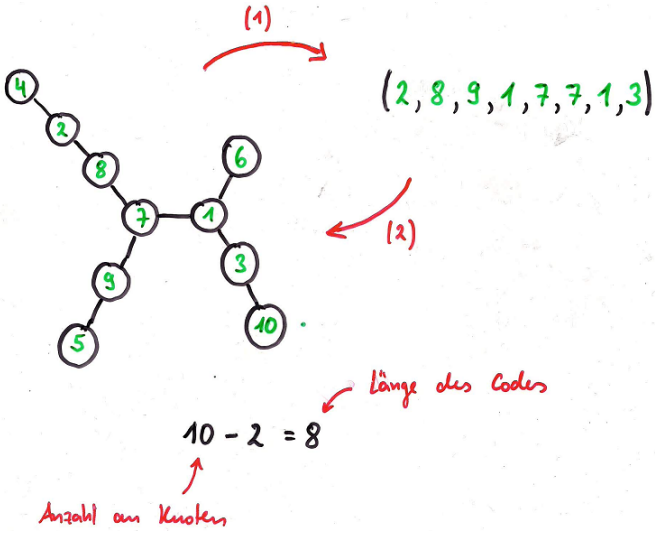
(2) Von Code zu Baum:

1. Starte die Zeichnung mit allen Knoten die nicht im Code vorkommen;
2. Gehe den Code $c = (c_1, c_2, \ldots, c_{n-2})$ von links nach rechts durch und für jeden Eintrag c_i wiederhole:

Rezept

3. Von den von c_i verschiedenen, noch unmarkierten Knoten im Baum, die nicht mehr im restlichen Code vorkommen, nimm den kleinsten, markiere ihn und verbinde ihn mit c_i;
4. Verbinde die letzten 2 unmarkierten Knoten miteinander;

Beispiel


(1)
(2, 8, 9, 1, 7, 7, 1, 3)
(2)
4
2
8
6
7
1
3
9
5
10
Länge des Codes
10 - 2 = 8
Anzahl an Knoten

Infos

- Diese Methode stellt eine Bijektion zwischen der Menge aller Bäume mit n Knoten und der Menge

$$[n]^{n-2} = \underbrace{[n] \times [n] \times \ldots \times [n]}_{(n-2) \text{ mal}}$$

  aller $(n-2)$-Tupel über $[n]$ dar.
- Daraus folgt der Satz von Cayley aus Folie 957.
- Prüfer-Codes prüfen nichts. Sie wurden von Heinz Prüfer entwickelt! ;-)

Gegeben seien folgende Bäume T_1, T_2 und T_3:

1. $T_1 = ([6], \{\{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,6\}\})$,
2. $T_2 = ([6], \{\{1,3\}, \{1,6\}, \{2,6\}, \{3,4\}, \{5,6\}\})$,
3. $T_3 = ([6], \{\{1,2\}, \{2,4\}, \{2,5\}, \{3,4\}, \{5,6\}\})$.

Wie sieht der entsprechende Prüfer-Code c_i zu jedem Baum T_i aus?

Antworten

1. $c_1 = (1, 1, 1, 2)$.
2. $c_2 = (6, 3, 1, 6)$.
3. $c_3 = (2, 4, 2, 5)$.

Gegeben seien folgende Prüfer-Codes c_1, c_2 und c_3:

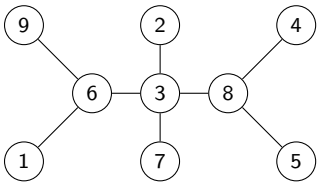
1. $c_1 = (1, 3, 3, 1)$,
2. $c_2 = (6, 4, 2, 5)$,
3. $c_3 = (1, 1, 1, 1)$.

Wie sieht der entsprechende Baum T_i zu jedem Prüfer-Code c_i aus?

1. $T_1 = ([6], \{\{1,2\}, \{1,3\}, \{1,6\}, \{3,4\}, \{3,5\}\})$.
2. $T_2 = ([6], \{\{1,6\}, \{2,4\}, \{2,5\}, \{3,4\}, \{5,6\}\})$.
3. $T_3 = ([6], \{\{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{1,6\}\})$.

Bemerkung: In der Regel wird nicht erwartet, dass man Graphen als Tupel (V, E) darstellt. Eine Zeichnung reicht hier und in den meisten Fällen völlig aus :-)

1. Was ist der Prüfer-Code c_1 zu folgendem Baum T_1?

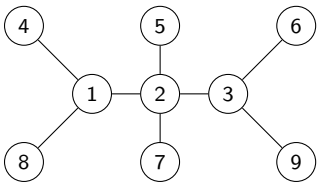


T_1

2. Wie sieht der Baum T_2 zu folgendem Prüfer-Code c_2 graphisch aus?

$$c_2 = (1, 2, 3, 2, 1, 2, 3)$$

3. Was stellt man fest, wenn man die Bäume und Prüfer-Codes der letzten zwei Fragen miteinander vergleicht?

1. $c_1 = (6, 3, 8, 8, 3, 3, 6)$.
2. 

T_2
3. Dass man die Namen der Knoten im Baum vertauscht, heißt nicht, dass man einfach die Namen der Komponenten im Code entsprechend vertauschen kann.

Themenübersicht

Themenübersicht

Operatoren

- Ein Operator $\circ$ über einer Menge B mit Arität (oder Stelligkeit) n ist eine Funktion

$$\circ : B^n \to B.$$

- Eine Menge $A \subseteq B$ heißt in $\circ$ abgeschlossen, falls für alle $a_1, \ldots, a_n \in A$ gilt:

$$\circ(a_1, \ldots, a_n) \in A.$$

Beispiele

Folgende sind Operatoren über $\mathbb{R}$:

Operator	Symbol	Arität
Addition	$+$	2
Subtraktion	$-$	2
Multiplikation	$\cdot$	2
Maximum	max	2
Minimum	min	2
Negation	$-$	1

Die Division : ist ein Operator über $\mathbb{R} \setminus \{0\}$ mit Stelligkeit 2. Sie ist kein Operator über $\mathbb{R}$, weil man durch Null nicht dividieren darf.

Mehr Beispiele

Für eine beliebige Menge A sind folgende Operatoren über $\mathcal{P}(A)$:

Operator	Symbol	Arität
Schnitt	$\cap$	2
Vereinigung	$\cup$	2
Differenz	$\setminus$	2
Symmetrische Differenz	$\triangle$	2
Komplement	$\overline{}$	1

$\mathcal{P}(B)$ ist für jede Menge $B \subseteq A$ in $\cap$, $\cup$, $\setminus$ und $\triangle$ abgeschlossen. Nur $\mathcal{P}(A)$ ist in $\overline{}$ abgeschlossen.

Quizfrage

Für eine beliebige Menge A ist die Komposition von Funktionen $\circ$ ein Operator mit Arität 2 über der Menge A^A aller Funktionen $f : A \to A$.

Welche interessanten Teilmengen von A^A sind in $\circ$ abgeschlossen?

Einige coole Teilmengen von A^A, die in $\circ$ abgeschlossen sind, sind:

- die Menge aller injektiven Funktionen $f : A \to A$,
- die Menge aller surjektiven Funktionen $f : A \to A$,
- die Menge aller bijektiven Funktionen $f : A \to A$.

Erinnerung: Im Abschnitt „Beweismethoden“ haben wir bewiesen, dass die Komposition von zwei injektiven (bzw. surjektiven) Funktionen wieder injektiv (bzw. surjektiv) ist.

Infos

- Operatoren mit Stelligkeit 1 heißen unär, mit Stelligkeit 2 binär und mit Stelligkeit 3 ternär.
- Für unäre Operatoren $\circ$ schreiben wir oft $\overset{\circ}{a}$ (z.B. beim Komplement) oder $\circ a$ (z.B. bei der Negation).
- Für binäre Operatoren $\circ$ schreiben wir oft $a \circ b$. Man nennt diese Schreibweise Infixnotation.

Algebren

- Eine Algebra $(A, \circ_1, \ldots, \circ_n)$ besteht aus einer Trägermenge A und beliebig vielen Operatoren $\circ_1, \ldots, \circ_n$, so dass A in ihnen abgeschlossen ist.
- $(B, \circ)$ heißt Unteralgebra von $(A, \circ)$, falls $B \subseteq A$ gilt und $(B, \circ)$ selber eine Algebra ist.

Infos

- A kann eine beliebige Menge sein und $\circ_1, \ldots, \circ_n$ beliebige Operatoren über diese Menge. Der Fantasie sind hier keine Grenzen gesetzt ;-)
- Das Symbol $\circ$ (oft auch $\bullet$, $*$, $\odot$ oder $\oplus$) ist nur ein Platzhalter für einen beliebigen Operator und nicht notwendigerweise das Relationenprodukt oder die Komposition von Funktionen!

Beispiele

Einige Algebren über Zahlen sind:

- $(\mathbb{Q}, +, -, \cdot, \min, \max)$,
- $(\mathbb{Z}, +, -, \cdot, \min, \max)$,
- $(\mathbb{N}_0, +, \cdot, \min, \max)$,
- $(\mathbb{N}, +, \cdot, \min, \max)$.

Für eine beliebige Menge M sind auch

- $(\mathcal{P}(M), \cap, \cup, \setminus, \triangle, \overline{\ })$ und
- $(M^M, \circ)$

Algebren

Gegenbeispiele

- $(\mathbb{Z}, :)$, $(\mathbb{N}, :)$ und $(\mathbb{N}_0, :)$ sind keine Algebren, da beispielsweise $1 : 2 = 0,5$ gilt und $0,5$ in keine der drei Mengen enthalten ist.
- $(\mathbb{Q}, :)$ist keine Algebra, da die Division durch 0 nicht definiert ist.
- $(\mathbb{Q} \setminus \{0\}, :)$ ist eine Algebra. $(\mathbb{Z} \setminus \{0\}, :)$ und $(\mathbb{N} \setminus \{0\}, :)$ dagegen nicht, da beispielsweise $1 : 2$ weder in $\mathbb{Z}$ noch in $\mathbb{N}$ enthalten ist.
- $(\mathbb{N}_0, -)$ und $(\mathbb{N}, -)$ sind keine Algebren, da beispielsweise $1 - 2$ keine natürliche Zahl ist.

Halbgruppen

- Eine Algebra $(A, \circ)$ mit einem binären Operator $\circ$ heißt Halbgruppe, falls $\circ$ in A assoziativ ist, d.h.:
$$\forall a, b, c \in A : (a \circ b) \circ c = a \circ (b \circ c).$$
- Eine Halbgruppe $(A, \circ)$ heißt kommutativ, falls gilt:
$$\forall a, b \in A : a \circ b = b \circ a.$$

Beispiele

Aus den Algebren aus Folie 1048 lassen sich folgende Halbgruppen gewinnen.

- Über Zahlenmengen:

$$\begin{array}{llll} (\mathbb{Q},+), & (\mathbb{Q},\cdot), & (\mathbb{Q},\min), & (\mathbb{Q},\max), \\ (\mathbb{Z},+), & (\mathbb{Z},\cdot), & (\mathbb{Z},\min), & (\mathbb{Z},\max), \\ (\mathbb{N}_0,+), & (\mathbb{N}_0,\cdot), & (\mathbb{N}_0,\min), & (\mathbb{N}_0,\max), \\ (\mathbb{N},+), & (\mathbb{N},\cdot), & (\mathbb{N},\min), & (\mathbb{N},\max). \end{array}$$

- Über einer beliebigen Menge M:

$$(\mathcal{P}(M),\cap), \quad (\mathcal{P}(M),\cup), \quad (\mathcal{P}(M),\triangle), \quad (M^M,\circ).$$

Alle hier aufgelisteten Halbgruppen sind, mit $(M^M,\circ)$ als einzige Ausnahme, kommutativ.

Gegenbeispiele

- $(\mathcal{P}(M), \overline{\ })$ ist für keine Menge M eine Halbgruppe, da das Komplement $\overline{\ }$ nicht binär ist.
- $(\mathbb{Q} \setminus \{0\}, :)$ ist keine Halbgruppe, da die Division $:$ nicht assoziativ ist. Es gilt beispielsweise:
$$(8 : 4) : 2 = 1 \neq 4 = 8 : (4 : 2).$$
- $(\mathbb{Z}, -)$ ist keine Halbgruppe, da die Subtraktion $-$ nicht assoziativ ist. Es gilt beispielsweise:
$$(5 - 3) - 2 = 0 \neq 4 = 5 - (3 - 2).$$
- $(\mathcal{P}(M), \setminus)$ ist nur für $M = \emptyset$ eine Halbgruppe. Für $|M| \geq 1$ ist die Differenz $\setminus$ nicht assoziativ. Beispielsweise gilt:
$$(\{1\} \setminus \emptyset) \setminus \{1\} = \emptyset \neq \{1\} = \{1\} \setminus (\emptyset \setminus \{1\}).$$

Sei $\mathbb{Q} = \left\{ \frac{p}{q} \right\} p \in \mathbb{Z}, q \in \mathbb{N}$ die Menge aller rationalen Zahlen und $x \circ y$ der Mittelwert von x und y, d.h.:

$$x \circ y := \frac{x + y}{2}.$$

1. Ist $(\mathbb{Q}, \circ)$ eine Algebra?
2. Ist $(\mathbb{Q}, \circ)$ eine Halbgruppe?
3. Ist $(\mathbb{Q}, \circ)$ kommutativ?

1. Ja! $\circ$ ist ein Operator über $\mathbb{Q}$, da der Mittelwert zweier Brüche wieder ein Bruch ist. Für beliebige $p, r \in \mathbb{Z}$ und $q, s \in \mathbb{N}$ gilt:

$$\frac{p}{q} \circ \frac{r}{s} = \frac{\frac{p}{q} + \frac{r}{s}}{2} = \frac{ps + qr}{2qs}.$$

2. Nein! $\circ$ ist nicht assoziativ. Beispielsweise gilt:

$$(9 \circ 5) \circ 1 = 4 \neq 6 = 9 \circ (5 \circ 1).$$

3. Ja! $\circ$ ist kommutativ, da für alle $x, y \in \mathbb{Q}$ gilt:

$$x \circ y = \frac{x + y}{2} = \frac{y + x}{2} = y \circ x.$$

Monoide

Eine Halbgruppe $(A, \circ)$ heißt Monoid, falls sie ein Element $e \in A$ mit folgender Eigenschaft besitzt:

$$\forall a \in A : a \circ e = a = e \circ a.$$

Dieses Element wird neutrales Element genannt.

Infos

- Ein Element $e \in A$ heißt linksneutral, falls für alle $a \in A$ gilt: $e \circ a = a$ und rechtsneutral, falls für alle $a \in A$ gilt: $a \circ e = a$.
- Man nennt das neutrale Element e oft auch Einselement 1.
- Existiert ein neutrales Element e, dann kann man auch $(A, \circ, e)$ statt nur $(A, \circ)$ schreiben.
- Es gibt in A entweder nur linksneutrale Elemente, nur rechtsneutrale Elemente oder genau ein neutrales Element.

Beispiele

Folgende Halbgruppen aus aus Folie 1051 sind Monoide.

- Mit neutralem Element 0:

$$(\mathbb{Q}, +), \quad (\mathbb{Z}, +), \quad (\mathbb{N}_0, +), \quad (\mathbb{N}_0, \max).$$

- Mit neutralem Element 1:

$$(\mathbb{Q}, \cdot), \quad (\mathbb{Z}, \cdot), \quad (\mathbb{N}_0, \cdot), \quad (\mathbb{N}, \cdot), \quad (\mathbb{N}, \max).$$

Alle hier aufgelisteten Monoide sind kommutativ.

Gegenbeispiele

Keine Monoide sind:

$$(\mathbb{Q}, \min), \quad (\mathbb{Z}, \min), \quad (\mathbb{N}_0, \min), \quad (\mathbb{N}, \min), \quad (\mathbb{Q}, \max), \quad (\mathbb{Z}, \max), \quad (\mathbb{N}, +).$$

Sei A eine beliebige Menge. Was ist in folgenden Monoiden das neutrale Element?

1. $(\mathcal{P}(A), \cap)$,
2. $(\mathcal{P}(A), \cup)$,
3. $(\mathcal{P}(A), \triangle)$,
4. $(A^A, \circ)$.

Hinweise:

- Welche Mengen sind für jedes A in $\mathcal{P}(A)$ enthalten?
- Welche Funktion ist für jedes A in A^A enthalten?

1. Das neutrale Element ist A, da für alle $X \in \mathcal{P}(A)$ gilt:

$$X \cap A = X = A \cap X.$$

2. Das neutrale Element ist $\emptyset$, da für alle $X \in \mathcal{P}(A)$ gilt:

$$X \cup \emptyset = X = \emptyset \cup X.$$

3. Das neutrale Element ist $\emptyset$, da für alle $X \in \mathcal{P}(A)$ gilt:

$$A \triangle \emptyset = A = \emptyset \triangle A.$$

4. Das neutrale Element ist die Identitätsfunktion id_A, da für alle Funktionen $f \in A^A$ und alle $x \in A$ gilt:

$$(f \circ \mathrm{id}_A)(x) = f(\mathrm{id}_A(x)) = f(x) = \mathrm{id}_A(f(x)) = (\mathrm{id}_A \circ f)(x).$$

Gruppen

- Ein Monoid $(A, \circ)$ mit neutralem Element e heißt Gruppe, falls es für jedes Element $a \in A$ ein Element $a^{-1} \in A$ gibt mit:

$$a \circ a^{-1} = e = a^{-1} \circ a.$$

- Eine kommutative Gruppe heißt auch abelsch.

Infos

- a^{-1} wird inverses Element von a genannt und kann in manchen Fällen a selbst sein.
- a^{-1} ist nur eine Schreibweise und bedeutet nicht unbedingt $\frac{1}{a}$.
- Ein Element $a \in A$ besitzt entweder nur linksinverse Elemente, nur rechtsinverse Elemente oder genau ein inverses Element.

Beispiele

Die einzigen Monoide aus Folie 1057, die Gruppen sind, sind:

$$(\mathbb{Q}, +) \quad \text{und} \quad (\mathbb{Z}, +).$$

Außerdem ist auch $(\mathbb{Q} \setminus \{0\}, \cdot)$ eine Gruppe. Alle drei Gruppen sind kommutativ.

Gegenbeispiele

- $(\mathbb{N}_0, +)$ und $(\mathbb{N}_0, \max)$ sind keine Gruppen, weil nur die 0 ein inverses Element besitzt (nämlich die 0 selber).
- $(\mathbb{N}_0, \cdot)$, $(\mathbb{N}, \cdot)$, $(\mathbb{N}, \max)$ und $(\mathbb{Z}, \cdot)$ sind keine Gruppen, weil nur die 1 ein inverses Element besitzt (nämlich die 1 selber).
- $(\mathbb{Q}, \cdot)$ ist keine Gruppe, weil die 0 kein inverses Element besitzt.

Philosophische Quizfrage

Ist $(\emptyset, \circ)$ mit dem leeren Operator $\circ : \emptyset \times \emptyset \to \emptyset$ eine Gruppe?

Nö! Weil es keine Elemente gibt, gibt es insbesondere kein neutrales Element. Also ist $(\emptyset, \circ)$ zwar eine Halbgruppe, aber kein Monoid und somit auch keine Gruppe.

Info

Für jede Menge A und jeden binären Operator $\circ$ gilt:

1. A ist in $\circ$ abgeschlossen

   $\forall a, b \in A\colon a \circ b \in A$

2. Die Einschränkung von $\circ$ auf A ist assoziativ

   $\forall a, b, c \in A\colon (a \circ b) \circ c = a \circ (b \circ c)$

3. A besitzt ein neutrales Element bezüglich $\circ$

   $\exists e \in A\colon \forall a \in A\colon a \circ e = a = e \circ a$

4. Jedes Element aus A besitzt ein inverses Element bezüglich $\circ$

   $\forall a \in A\colon \exists a^{-1} \in A\colon a \circ a^{-1} = e = a^{-1} \circ a$

Algebra

Halbgruppe

Monoid

Gruppe

Daraus folgt folgende Hierarchie:

$$(A, \circ) \text{ Gruppe} \implies (A, \circ) \text{ Monoid} \implies (A, \circ) \text{ Halbgruppe} \implies (A, \circ) \text{ Algebra.}$$

Beispiele

Aus den letzen Beispielen ergibt sich folgende Hierarchie:

1. Gruppen sind:
$$(\mathbb{Q}, +), \quad (\mathbb{Z}, +), \quad (\mathbb{Q} \setminus \{0\}, \cdot).$$
2. Monoide, aber keine Gruppen sind:
$$(\mathbb{N}_0, +), \quad (\mathbb{N}_0, \max), \quad (\mathbb{N}_0, \cdot), \quad (\mathbb{N}, \cdot), \quad (\mathbb{N}, \max), \quad (\mathbb{Z}, \cdot), \quad (\mathbb{Q}, \cdot).$$
3. Halbgruppen, aber keine Monoide sind:
$$(\mathbb{Q}, \min), \quad (\mathbb{Z}, \min), \quad (\mathbb{N}_0, \min), \quad (\mathbb{N}, \min), \quad (\mathbb{Q}, \max), \quad (\mathbb{Z}, \max), \quad (\mathbb{N}, +).$$
4. Algebren, aber keine Halbgruppen sind:
$$(\mathbb{Q} \setminus \{0\}, :), \quad (\mathbb{Z}, -), \quad (\mathcal{P}(M), \setminus).$$

Sei $\Sigma = \{a, b, c\}$ ein Alphabet und Σ^* die Menge aller Wörter über Σ. Ist Σ^* zusammen mit der Konkatenation von Wörtern ...

1. eine Algebra?
2. eine Halbgruppe?
3. ein Monoid?
4. eine Gruppe?
5. kommutativ?

Erinnerung: Das leere Wort ϵ ist auch in Σ^* enthalten!

1. Ja! Die Konkatenation zweier Wörter aus Σ^* ergibt wieder ein Wort aus Σ^*.
2. Ja! Die Konkatenation ist assoziativ, denn für beliebige Wörter $u, v, w \in \Sigma^*$ gilt $(uv)w = uvw = u(vw)$ (es ist egal welche zwei man zuerst „aneinander klebt“).
3. Ja! Das leere Wort ϵ ist das neutrale Element, denn für ein beliebiges Wort $u \in \Sigma^*$ gilt $\epsilon u = u = u\epsilon$.
4. Nein! Kein Wort u hat ein Inverses u^{-1}. Dieses müsste nämlich eine negative Länge haben, damit $uu^{-1} = \epsilon$ bzw. $u^{-1}u = \epsilon$ gilt.
5. Nein! Nicht für beliebige Wörter $u, v \in \Sigma^*$ gilt $uv = vu$, z.B. für $u = ab$ und $v = bc$.

$(G, \circ)$ bildet mit $G = \mathbb{Q} \setminus \{-1\}$ und $x \circ y := x + y + xy$ eine abelsche Gruppe.

1. Wieso ist G in $\circ$ abgeschlossen?
2. Wieso ist $\circ$ assoziativ?
3. Was ist das neutrale Element in $(G, \circ)$?
4. Besitzt jedes Element $a \in \mathbb{Q} \setminus \{-1\}$ ein Inverses a^{-1}?
5. Was ist das inverse Element x^{-1} zu $x = \frac{3}{4}$?
6. Wieso ist $(G, \circ)$ kommutativ?

Hinweis zu 1.: Da für beliebige $a, b \in \mathbb{Q} \setminus \{-1\}$ offensichtlich $a \circ b \in \mathbb{Q}$ gilt, muss nur

$$a, b \in \mathbb{Q} \setminus \{-1\} \implies a \circ b \neq -1$$

gezeigt werden. Zeige dies mit einem Widerspruchsbeweis: Nimm $a, b \in \mathbb{Q} \setminus \{-1\}$ und $a \circ b = -1$ an und leite daraus einen Widerspruch her.

1. Seien $a, b \in \mathbb{Q} \setminus \{-1\}$ beliebig mit $a \circ b = -1$. Dann gilt:

$$\begin{aligned} a \circ b = -1 &\implies a + b + ab = -1 \\ &\implies a + ab = -1 - b \\ &\implies a(1 + b) = -(1 + b) \\ &\implies b = -1 \text{ oder } a = \frac{-(1 + b)}{1 + b} = -1 \end{aligned}$$

□

2. Seien $a, b, c \in \mathbb{Q} \setminus \{-1\}$ beliebig. Dann gilt:

$$\begin{aligned}(a \circ b) \circ c &= (a + b + ab) \circ c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc\ , \\ a \circ (b \circ c) &= a \circ (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + ab + ac + bc + abc.\end{aligned}$$

Somit gilt $(a \circ b) \circ c = a \circ (b \circ c)$.

3. Sei e das neutrale Element. Dann gilt für ein beliebiges $a \in \mathbb{Q} \setminus \{-1\}$:

$$\begin{aligned} a \circ e = a &\iff a + e + ae = a \\ &\iff e + ae = 0 \\ &\iff e(1 + a) = 0 \\ &\iff e = 0. \end{aligned}$$

Das neutrale Element ist $e = 0$.

4. Sei $a \in \mathbb{Q} \setminus \{-1\}$ beliebig. Dann gilt:

$$\begin{aligned} a \circ a^{-1} = e &\iff a + a^{-1} + aa^{-1} = 0 \\ &\iff a^{-1} + aa^{-1} = -a \\ &\iff a^{-1}(1 + a) = -a \\ &\iff a^{-1} = \frac{-a}{1 + a}. \end{aligned}$$

   Somit ist für jedes a das inverse Element $\frac{-a}{1+a}$ in der Menge $\mathbb{Q} \setminus \{-1\}$ enthalten.

5. Das Inverse zu $a = \frac{3}{4}$ ist $a^{-1} = \frac{-\frac{3}{4}}{1+\frac{3}{4}} = -\frac{3}{7}$.

6. Seien $a, b \in \mathbb{Q} \setminus \{-1\}$ beliebig. Dann gilt:

$$a \circ b = a + b + ab = b + a + ba = b \circ a.$$

Verknüpfungstafeln

Eine Algebra $(A, \circ)$ über einer endlichen Menge $A = \{a_1, \ldots, a_n\}$ und einem binären Operator $\circ$ über A lässt sich sehr schön mit einer sogenannten Verknüpfungstafel oder Multiplikationstafel darstellen.

Jedes Element aus A bekommt eine bestimmte Zeile und Spalte einer Tabelle. Dann verknüpft man jedes Element mit jedem und trägt das Ergebnis in der entsprechenden Zelle ein.

Beispiel

Sei $(G, \circ)$ eine kommutative Gruppe über einer 4-elementige Menge $G = \{a, b, c, d\}$ mit folgender Verknüpfungstafel für $\circ$:

$\circ$	a	b	c	d
a	b	a	d	c
b	a	b	c	d
c	d	c	a	b
d	c	d	b	a

Woran erkennt man anhand der Verknüpfungstafel, dass $(G, \circ)$ eine kommutative Gruppe ist?

Beispiel

1. G ist abgeschlossen in $\circ$, da in der Tabelle nur Elemente aus G vorkommen.
2. G ist assoziativ. Hierfür muss man alle Kombinationen ausprobieren. Zum Beispiel:

$$c \circ (d \circ a) = c \circ c = a = b \circ a = (c \circ d) \circ a$$

   Es sind insgesamt $|S|^3 = 4^3 = 64$ solche Rechnungen. Nehmen wir einfach mal an, dass wir alle 64 überprüft haben ;-)
3. b ist das neutrale Element.
4. Jedes Element besitzt ein Inverses:

$$a^{-1} = a, \quad b^{-1} = b, \quad c^{-1} = d, \quad d^{-1} = c.$$

5. $(G, \circ)$ ist kommutativ. Dies erkennt man an der diagonalen Spiegelachse.

Info

Bis auf die Assoziativität, kann man alle Eigenschaften endlicher Algebren an der Verknüpfungstafel erkennen. Die Assoziativität des Operators muss leider mit brute force überprüft oder allgemein bewiesen werden.

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

1. Was ist das inverse Element a^{-1} von jedem $a \in G$?
2. Ist $(G, \circ)$ kommutativ?

1. Es gilt:
$$e^{-1} = e, \quad x^{-1} = x, \quad y^{-1} = y, \quad z^{-1} = z.$$
2. Ja! Das erkennt man an der diagonales Spiegelachse in der Verknüpfungstafel.

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b

1. Was ist das inverse Element a^{-1} von jedem $a \in G$?
2. Ist $(G, \circ)$ kommutativ?

1. Es gilt:
$$e^{-1} = e, \quad a^{-1} = d, \quad b^{-1} = c, \quad c^{-1} = b, \quad d^{-1} = a.$$
2. Ja! Das erkennt man an der diagonales Spiegelachse in der Verknüpfungstafel.

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	t	s	r	q
q	q	s	e	t	p	r
r	r	t	s	e	q	p
s	s	q	r	p	t	e
t	t	r	p	q	e	s

1. Was ist das inverse Element a^{-1} von jedem $a \in G$?
2. Ist $(G, \circ)$ kommutativ?

1. Es gilt:

$$e^{-1} = e, \quad p^{-1} = p, \quad q^{-1} = q, \quad r^{-1} = r, \quad s^{-1} = t, \quad t^{-1} = s.$$

2. Nein! Es gilt beispielsweise:

$$p \circ q = t \neq s = q \circ p.$$

Quizfrage

Wir betrachten die logischen Junktoren $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, $\oplus$, $\bar{\wedge}$ und $\bar{\vee}$ nun als Operatoren $\mathbb{B} \times \mathbb{B} \to \mathbb{B}$ für $\mathbb{B} = \{0, 1\}$ und bilden Algebren mit folgenden Verknüpfungstafeln:

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\rightarrow$	0	1
0	1	1
1	0	1

$\leftrightarrow$	0	1
0	1	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

$\bar{\wedge}$	0	1
0	1	1
1	1	0

$\bar{\vee}$	0	1
0	1	0
1	0	0

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\rightarrow$	0	1
0	1	1
1	0	1

$\leftrightarrow$	0	1
0	1	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

$\bar{\wedge}$	0	1
0	1	1
1	1	0

$\bar{\vee}$	0	1
0	1	0
1	0	0

Wo sind diese Algebren in der Hierarchie einzuordnen?

Hinweis: Mit Wahrheitstafeln kann man überprüfen, dass nur $\wedge$, $\vee$, $\leftrightarrow$ und $\oplus$ assoziativ sind.

- Algebren sind sie alle, weil sie alle abgeschlossen sind.
- Halbgruppen sind:
$$(\mathbb{B}, \wedge), \quad (\mathbb{B}, \vee), \quad (\mathbb{B}, \leftrightarrow), \quad (\mathbb{B}, \oplus).$$
- Monoide sind:
$$(\mathbb{B}, \wedge), \quad (\mathbb{B}, \vee), \quad (\mathbb{B}, \leftrightarrow), \quad (\mathbb{B}, \oplus).$$
- Gruppen sind:
$$(\mathbb{B}, \leftrightarrow), \quad (\mathbb{B}, \oplus).$$
- Kommutativ sind:
$$(\mathbb{B}, \wedge), \quad (\mathbb{B}, \vee), \quad (\mathbb{B}, \leftrightarrow), \quad (\mathbb{B}, \oplus), \quad (\mathbb{B}, \bar{\wedge}), \quad (\mathbb{B}, \bar{\vee}).$$

Themenübersicht

Eigenschaften von Gruppen

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Dann gelten folgende Rechenregeln:

1. Eindeutigkeit des neutralen Elements. Es gibt genau ein neutrales Element e.
2. Eindeutigkeit der inversen Elemente. Jedes Element $a \in G$ besitzt ein inverses Element a^{-1}.
3. Involutionsgesetz. Für jedes $a \in G$ gilt: $(a^{-1})^{-1} = a$
4. Kürzungsregel. Für alle $a, b, c \in G$ gilt:

$$\begin{aligned} a \circ c = b \circ c &\iff a = b \\ c \circ a = c \circ b &\iff a = b \end{aligned}$$

5. Eindeutige Lösung linearer Gleichungen. Für alle $a, b, x \in G$ gilt:

$$\begin{aligned} a \circ x = b &\iff x = a^{-1} \circ b \\ x \circ a = b &\iff x = b \circ a^{-1} \end{aligned}$$

Infos

- Weil Gruppen assoziativ sind, können wir die Klammern oft weglassen. Beispielsweise können wir $a \circ b \circ c$ statt $(a \circ b) \circ c$ oder $a \circ (b \circ c)$ schreiben.
- Weil wir bei Gruppen nur einen Operator zur Verfügung haben, können wir diesen auch einfach weglassen und ab statt $a \circ b$ schreiben.

Sei $(G, \circ)$ eine beliebige, nicht notwendigerweise kommutative Gruppe mit neutralem Element e und seien $a, b, x \in G$ beliebige Elemente.

Was ist die Lösung der Gleichung

$$b \circ (a \circ x)^{-1} = b \circ a$$

nach x?

Weil $\circ$ assoziativ ist, können Klammern weggelassen werden.

$$
\begin{aligned}
b \circ (a \circ x)^{-1} = b \circ a \quad &\iff \quad b^{-1} \circ b \circ (a \circ x)^{-1} = b^{-1} \circ b \circ a \\
&\iff \quad e \circ (a \circ x)^{-1} = e \circ a \\
&\iff \quad (a \circ x)^{-1} = a \\
&\iff \quad ((a \circ x)^{-1})^{-1} = a^{-1} \\
&\iff \quad a \circ x = a^{-1} \\
&\iff \quad a^{-1} \circ a \circ x = a^{-1} \circ a^{-1} \\
&\iff \quad e \circ x = a^{-1} \circ a^{-1} \\
&\iff \quad x = a^{-1} \circ a^{-1}
\end{aligned}
$$

Kürzungsregel

Die Kürzungsregel besagt, dass für alle $a, b, c \in G$ gilt:

$$\begin{aligned} a \circ c = b \circ c \quad &\iff \quad a = b \\ c \circ a = c \circ b \quad &\iff \quad a = b \end{aligned}$$

Intuitiv heißt das, dass es in jeder Zeile und Spalte der Verknüpfungstafel jedes Element genau einmal vorkommt.

Info

Man nennt diese Regel auch Sudoku-Regel ;-)

Sei $(G, \circ)$ eine Gruppe mit $G = \{a, b, c, d, e, f\}$ und folgender (unvollständigen) Verknüpfungstafel:

$\circ$	a	b	c	d	e	f
a						
b		d	e			a
c		f		c		
d						
e	c					d
f	b					

Wie sieht die eindeutige, vollständige Verknüpfungstafel von $(G, \circ)$ aus?
Hinweis: $(G, \circ)$ ist eine Gruppe, d.h.:

Quizfrage

- es gilt die Kürzungsregel,
- es gibt ein eindeutiges neutrales Element und
- $\circ$ ist assoziativ, z.B.: $f \circ b = (c \circ b) \circ b = c \circ (b \circ b) = c \circ d = c$

Wegen $c \circ d = c$ ist d das neutrale Element. Wir erhalten:

$\circ$	a	b	c	d	e	f
a				a		
b		d	e	b		a
c		f		c		
d	a	b	c	d	e	f
e	c			e		d
f	b			f		

Mit der Kürzungsregel folgt:

$\circ$	a	b	c	d	e	f
a				a		
b	f	d	e	b	c	a
c		f		c		
d	a	b	c	d	e	f
e	c	a		e		d
f	b			f		

Aus der Assoziativität von $\circ$ folgt: $f \circ b = (c \circ b) \circ b = c \circ (b \circ b) = c \circ d = c$.

$\circ$	a	b	c	d	e	f
a				a		
b	f	d	e	b	c	a
c		f		c		
d	a	b	c	d	e	f
e	c	a		e		d
f	b	c		f		

Mit der Kürzungsregel folgt:

$\circ$	a	b	c	d	e	f
a	d	e		a		c
b	f	d	e	b	c	a
c	e	f		c		b
d	a	b	c	d	e	f
e	c	a		e		d
f	b	c		f		e

Aus der Assoziativität von $\circ$ folgt: $a \circ c = a \circ (f \circ b) = (a \circ f) \circ b = c \circ b = f$.

$\circ$	a	b	c	d	e	f
a	d	e	f	a		c
b	f	d	e	b	c	a
c	e	f		c		b
d	a	b	c	d	e	f
e	c	a		e		d
f	b	c		f		e

Mit der Kürzungsregel folgt:

$\circ$	a	b	c	d	e	f
a	d	e	f	a	b	c
b	f	d	e	b	c	a
c	e	f		c		b
d	a	b	c	d	e	f
e	c	a	b	e	f	d
f	b	c		f		e

Aus der Assoziativität von $\circ$ folgt: $c \circ c = c \circ (a \circ f) = (c \circ a) \circ f = e \circ f = d$.

$\circ$	a	b	c	d	e	f
a	d	e	f	a	b	c
b	f	d	e	b	c	a
c	e	f	d	c		b
d	a	b	c	d	e	f
e	c	a	b	e	f	d
f	b	c		f		e

Mit der Kürzungsregel folgt die fertige Verknüpfungstafel:

$\circ$	a	b	c	d	e	f
a	d	e	f	a	b	c
b	f	d	e	b	c	a
c	e	f	d	c	a	b
d	a	b	c	d	e	f
e	c	a	b	e	f	d
f	b	c	a	f	d	e

Potenzen von Elementen

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Für ein beliebiges Element $a \in G$ und $n \in \mathbb{N}$ gilt:

$$a^0 := e, \quad a^n := a^{n-1} \circ a \quad \text{und} \quad a^{-n} := (a^{-1})^n.$$

Info

Intuitiv heißt das:

$$a^n = \underbrace{a \circ a \circ \ldots \circ a}_{\text{genau } n \text{ as}} \quad \text{und} \quad a^{-n} = \underbrace{a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1}}_{\text{genau } n \ a^{-1}\text{s}}.$$

Ordnung von Elementen

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e und $a \in G$. Dann ist

$$\text{ord}(a) := \min \{n \in \mathbb{N}\}\, a^n = e$$

die Ordnung von a in $(G, \circ)$

Infos

- Es gilt $\min \emptyset := \infty$, d.h. dass $\text{ord}(a) = \infty$ gesetzt wird, wenn kein $n \in \mathbb{N}$ mit $a^n = e$ existiert.
- Das einzige Element mit Ordnung 1 ist das neutrale Element.
- Nicht verwechseln: Die Ordnung eines Elements x ist $\text{ord}(x)$. Die Ordnung der Gruppe ist $|G|$.
- Diese Definition könnte auch auf Monoide erweitert werden, obwohl das in DS nicht explizit gemacht wird.

Beispiel

Sei $(G, \circ)$ eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	x	e
z	z	y	e	x

Es gilt:

$$
\begin{aligned}
e & && && && \rightsquigarrow && \operatorname{ord}(e) = 1, \\
x & \xrightarrow{\circ x} e && && && \rightsquigarrow && \operatorname{ord}(x) = 2, \\
y & \xrightarrow{\circ y} x & \xrightarrow{\circ y} z & \xrightarrow{\circ y} e && && \rightsquigarrow && \operatorname{ord}(y) = 4, \\
z & \xrightarrow{\circ z} x & \xrightarrow{\circ z} y & \xrightarrow{\circ z} e && && \rightsquigarrow && \operatorname{ord}(z) = 4.
\end{aligned}
$$

Noch ein Beispiel

Sei $(G, \circ)$ eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	t	s	r	q
q	q	s	e	t	p	r
r	r	t	s	e	q	p
s	s	q	r	p	t	e
t	t	r	p	q	e	s

Es gilt:

$$
\begin{aligned}
e &\quad\rightsquigarrow\quad \operatorname{ord}(e) = 1,\\
p \xrightarrow{\circ p} e &\quad\rightsquigarrow\quad \operatorname{ord}(p) = 2,\\
q \xrightarrow{\circ q} e &\quad\rightsquigarrow\quad \operatorname{ord}(q) = 2,\\
r \xrightarrow{\circ r} e &\quad\rightsquigarrow\quad \operatorname{ord}(r) = 2,\\
s \xrightarrow{\circ s} t \xrightarrow{\circ s} e &\quad\rightsquigarrow\quad \operatorname{ord}(s) = 3,\\
t \xrightarrow{\circ t} s \xrightarrow{\circ t} e &\quad\rightsquigarrow\quad \operatorname{ord}(t) = 3.
\end{aligned}
$$

Zwei unendliche Beispiele

- In der Gruppe $(\mathbb{Z}, +)$ gilt:

$$\operatorname{ord}(x) = \begin{cases} 1 & \text{falls } x = 0 \\ \infty & \text{sonst} \end{cases}$$

- In der Gruppe $(\mathbb{Q} \setminus \{0\}, \cdot)$ gilt:

$$\operatorname{ord}(x) = \begin{cases} 1 & \text{falls } x = 1 \\ 2 & \text{falls } x = -1 \\ \infty & \text{sonst} \end{cases}$$

Erzeugnisse

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Für ein $a \in G$ wird die Menge

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}.$$

Erzeugnis von a genannt.

Info

- Ist $\operatorname{ord}(a) < \infty$, dann gilt: $\langle a \rangle = \left\{ a, a^2, \ldots, a^{\operatorname{ord}(a)} \right\}$.
- Für alle $a \in G$ gilt: $\operatorname{ord}(a) = |\langle a \rangle|$.

Zyklische Gruppen

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e.

- Ein Element $a \in G$ heißt Erzeuger oder Generator von $(G, \circ)$, falls $\langle a \rangle = G$ gilt.
- Besitzt G einen Erzeuger, so heißt G zyklisch.

Infos

- Falls G endlich ist, dann ist $(G, \circ)$ genau dann zyklisch, wenn ein Element $a \in G$ die Ordnung $\text{ord}(a) = |G|$ hat.
- Jede zyklische Gruppe ist kommutativ, aber nicht jede kommutative Gruppe ist zyklisch.

Beispiel

Sei $(G, \circ)$ wieder eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	x	e
z	z	y	e	x

$(G, \circ)$ ist zyklisch, weil sie von y und z generiert wird:

$$\begin{array}{lcl} e & \rightsquigarrow & \langle e \rangle = \{e\}\,, \\ x \xrightarrow{\circ x} e & \rightsquigarrow & \langle x \rangle = \{x, e\}\,, \\ y \xrightarrow{\circ y} x \xrightarrow{\circ y} z \xrightarrow{\circ y} e & \rightsquigarrow & \langle y \rangle = \{y, x, z, e\}\,, \\ z \xrightarrow{\circ z} x \xrightarrow{\circ z} y \xrightarrow{\circ z} e & \rightsquigarrow & \langle z \rangle = \{z, x, y, e\}\,. \end{array}$$

Noch ein Beispiel

Sei $(G, \circ)$ wieder eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	t	s	r	q
q	q	s	e	t	p	r
r	r	t	s	e	q	p
s	s	q	r	p	t	e
t	t	r	p	q	e	s

$(G, \circ)$ ist nicht zyklisch, weil sie von keinem Element generiert wird:

$$
\begin{aligned}
e &\quad\rightsquigarrow\quad \langle e \rangle = \{e\}, \\
p \xrightarrow{\circ p} e &\quad\rightsquigarrow\quad \langle p \rangle = \{p, e\}, \\
q \xrightarrow{\circ q} e &\quad\rightsquigarrow\quad \langle q \rangle = \{q, e\}, \\
r \xrightarrow{\circ r} e &\quad\rightsquigarrow\quad \langle r \rangle = \{r, e\}, \\
s \xrightarrow{\circ s} t \xrightarrow{\circ s} e &\quad\rightsquigarrow\quad \langle s \rangle = \{s, t, e\}, \\
t \xrightarrow{\circ t} s \xrightarrow{\circ t} e &\quad\rightsquigarrow\quad \langle t \rangle = \{t, s, e\}.
\end{aligned}
$$

Drei unendliche Beispiele

- In der Gruppe $(\mathbb{Z}, +)$ generiert jedes Element alle Vielfachen von sich selbst. Beispielsweise gilt:

$$\begin{aligned}
\langle 0 \rangle &= \{0\}, \\
\langle 1 \rangle &= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}, \\
\langle 2 \rangle &= \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}, \\
\langle 3 \rangle &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}, \\
&\vdots
\end{aligned}$$

  Für ein beliebiges $k \in \mathbb{Z}$ gilt: $\langle k \rangle = \{k \cdot n\}\, n \in \mathbb{Z}$. Somit ist das einzige Element, was endlich viele Elemente erzeugt, die 0.

- In der Gruppe $(\mathbb{Q} \setminus \{0\}, \cdot)$ gibt es zwei Elemente, die endlich viele Elemente generieren: 1 und -1. Es gilt: $\langle 1 \rangle = \{1\}$ und $\langle -1 \rangle = \{-1, 1\}$.

- Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch, da sie sowohl von der 1 als auch von der -1 generiert wird. Die Gruppe $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist nicht zyklisch.

Sei $(G, \circ)$ wieder eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

1. Was ist das Erzeugnis $\langle a \rangle$ und die Ordnung $\text{ord}(a)$ von jedem $a \in G$?
2. Ist $(G, \circ)$ zyklisch?

1. Als sogenannte Erzeugnistafel:

a	$\langle a \rangle$	$\mathrm{ord}(a)$
e	$\{e\}$	1
x	$\{x, e\}$	2
y	$\{y, e\}$	2
z	$\{z, e\}$	2

2. Nein! Kein Element hat Ordnung 4.

Sei $(G, \circ)$ wieder eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b

1. Was ist das Erzeugnis $\langle a \rangle$ und die Ordnung $\mathrm{ord}(a)$ von jedem $a \in G$?
2. Ist $(G, \circ)$ zyklisch?

1. Als Erzeugnistafel:

a	$\langle a \rangle$	$\operatorname{ord}(a)$
e	$\{e\}$	1
a	$\{a, c, b, d, e\}$	5
b	$\{b, a, d, c, e\}$	5
c	$\{c, d, a, b, e\}$	5
d	$\{d, b, c, a, e\}$	5

2. Ja! $(G, \circ)$ wird von a, b, c und d erzeugt.

Sei $(G, \circ)$ wieder eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	r	q	t	s
q	q	r	s	t	p	e
r	r	q	t	s	e	p
s	s	t	p	e	r	q
t	t	s	e	p	q	r

1. Was ist das Erzeugnis $\langle a \rangle$ und die Ordnung $\mathrm{ord}(a)$ von jedem $a \in G$?
2. Ist $(G, \circ)$ zyklisch?

1. Als Erzeugnistafel:

a	$\langle a \rangle$	$\mathrm{ord}(a)$
e	$\{e\}$	1
p	$\{p, e\}$	2
q	$\{q, s, p, r, t, e\}$	6
r	$\{r, s, e\}$	3
s	$\{s, r, e\}$	3
t	$\{t, r, p, s, q, e\}$	6

2. Ja! $(G, \circ)$ wird von q und t erzeugt.

Quizfrage

Die imaginäre Einheit $i \in \mathbb{C}$ besitzt die Eigenschaft $i^2 = -1$. Wie sehen die Erzeugnisse $\langle i \rangle$ und $\langle -i \rangle$ in der Gruppe $(\mathbb{C} \setminus \{0\}, \cdot)$ aus?

$$
\begin{aligned}
i \xrightarrow{\cdot i} -1 \xrightarrow{\cdot i} -i \xrightarrow{\cdot i} 1 \quad &\rightsquigarrow \quad \langle i \rangle = \{i, -1, -i, 1\}\,, \\
-i \xrightarrow{\cdot(-i)} -1 \xrightarrow{\cdot(-i)} i \xrightarrow{\cdot(-i)} 1 \quad &\rightsquigarrow \quad \langle -i \rangle = \{-i, -1, i, 1\}\,.
\end{aligned}
$$

Untergruppen

Sei $(G, \circ)$ eine Gruppe mit neutralem Element e. $(H, \circ)$ ist eine Untergruppe von $(G, \circ)$, falls $H \subseteq G$ und $(H, \circ)$ selber eine Gruppe ist.

Infos

- Damit eine Teilmenge von G mit $\circ$ eine Gruppe bilden kann, muss sie das neutrale Element enthalten.
- $(G, \circ)$ und $(\{e\}, \circ)$ sind immer Untergruppen von $(G, \circ)$. Diese werden triviale Untergruppen genannt.
- Für jedes $a \in G$ ist $(\langle a \rangle, \circ)$ eine zyklische Untergruppe von $(G, \circ)$.
- Ist $(G, \circ)$ endlich, dann ist jede Unteralgebra $(A, \circ)$ von $(G, \circ)$ eine Untergruppe. D.h. man muss nur auf die Abgeschlossenheit von $(A, \circ)$ achten.

Beispiel

Sei $(G, \circ)$ wieder eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	x	e
z	z	y	e	x

Folgende Mengen bilden mit $\circ$ Untergruppen von $(G, \circ)$:

$$\{e\}, \quad \{e, x\}, \quad \{e, x, y, z\}.$$

Noch ein Beispiel

Sei $(G, \circ)$ wieder eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	t	s	r	q
q	q	s	e	t	p	r
r	r	t	s	e	q	p
s	s	q	r	p	t	e
t	t	r	p	q	e	s

Folgende Mengen bilden mit $\circ$ Untergruppen von $(G, \circ)$:

$$\{e\}, \quad \{e, p\}, \quad \{e, q\}, \quad \{e, r\}, \quad \{e, s, t\}, \quad \{e, p, q, r, s, t\}.$$

Mehr Beispiele

- Für jedes $k \in \mathbb{Z}$ ist $(T, +)$ mit
$$T = \{k \cdot n\}\, n \in \mathbb{Z}$$
eine Untergruppe von $(\mathbb{Z}, +)$. Beispielsweise ist T für $k = 2$ die Menge aller geraden Zahlen. Die einzige endliche Untergruppe von $(\mathbb{Z}, +)$ ist $(\{0\}, +)$.
- Die Gruppe $(\mathbb{Q} \setminus \{0\}, \cdot)$ hat genau zwei endliche Untergruppen: $(\{1\}, \cdot)$ und $(\{-1, 1\}, \cdot)$.

Sei $(G, \circ)$ wieder eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

Welche der folgenden Teilmengen von S bilden mit $\circ$ eine Untergruppe?

$$\{e\}, \quad \{e, x\}, \quad \{e, z\}, \quad \{e, x, y\}, \quad \{e, y, z\}, \quad \{e, x, y, z\}.$$

Weil G endlich ist, müssen wir nur auf die Abgeschlossenheit der Teilmenge achten.
Untergruppen sind dann:

$$\{e\}, \quad \{e, x\}, \quad \{e, z\}, \quad \{e, x, y, z\}.$$

Sei $(G, \circ)$ wieder eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	c	d	b	e
b	b	d	a	e	c
c	c	b	e	d	a
d	d	e	c	a	b

Welche der folgenden Teilmengen von S bilden mit $\circ$ eine Untergruppe?

$$\{e\}, \quad \{e, a\}, \quad \{e, a, c\}, \quad \{e, b, d\}, \quad \{e, a, b, c\}, \quad \{e, a, b, c, d\}.$$

Weil G endlich ist, müssen wir nur auf die Abgeschlossenheit der Teilmenge achten.
Untergruppen sind dann:

$$\{e\}\,, \quad \{e, a, b, c, d\}\,.$$

Sei $(G, \circ)$ wieder eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	r	q	t	s
q	q	r	s	t	p	e
r	r	q	t	s	e	p
s	s	t	p	e	r	q
t	t	s	e	p	q	r

Welche der folgenden Teilmengen von S bilden mit $\circ$ eine Untergruppe?

$$\{e\}\,, \quad \{e, p\}\,, \quad \{e, q\}\,, \quad \{e, q, s\}\,, \quad \{e, s, r\}\,, \quad \{e, p, q, r, s, t\}\,.$$

Weil G endlich ist, müssen wir nur auf die Abgeschlossenheit der Teilmenge achten.
Untergruppen sind dann:

$$\{e\}, \quad \{e, p\}, \quad \{e, s, r\}, \quad \{e, p, q, r, s, t\}.$$

Welche der folgenden Mengen $T_1, T_2, T_3 \subseteq \mathbb{Z}$ bilden mit $+$ eine Untergruppe von $(\mathbb{Z}, +)$?

1. $T_1 = \{0\}$
2. $T_2 = \{2n\}\ n \in \mathbb{Z}$
3. $T_3 = \{2n + 1\}\ n \in \mathbb{Z}$
4. $T_4 = \mathbb{N}$
5. $T_5 = \mathbb{N}_0$

Antworten

1. Ja! T_1 enthält nur das neutrale Element und ist somit eine der trivialen Untergruppen. Sie ist sogar die einzige endliche Untergruppe von $(\mathbb{Z}, +)$.
2. Ja! T_2 ist abgeschlossen, enthält das neutrale Elemente und alle inversen Elemente. T_2 ist die durch 2 bzw. -2 erzeugte Untergruppe.
3. Nein! T_3 enthält alle ungeraden Zahlen und ist deswegen nicht abgeschlossen. Außerdem enthält T_2 nicht das neutrale Element 0.
4. Nein! T_4 ist zwar abgeschlossen, aber enthält nicht das neutrale Element 0. Außerdem enthält sie keine inverse Elemente.
5. Nein! T_5 ist zwar abgeschlossen und enthält das neutrale Element 0, aber die 0 ist das einzige Element was ein Inverses in T_5 besitzt.

Nebenklassen

Sei $(G, \circ)$ eine Gruppe und $(H, \circ)$ eine Untergruppe von $(G, \circ)$. Für jedes $a \in G$ definieren wir:

$$
\begin{aligned}
H \circ a &:= \{b \circ a\}\, b \in H \quad \text{(rechte Nebenklasse von } (H, \circ) \text{ zu } a) \\
a \circ H &:= \{a \circ b\}\, b \in H \quad \text{(linke Nebenklasse von } (H, \circ) \text{ zu } a)
\end{aligned}
$$

Info

Die Menge der rechten bzw. linken Nebenklassen bildet eine Partition von G.

Beispiel

Sei $(G, \circ)$ wieder eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	x	e
z	z	y	e	x

a	$\{e, x\} \circ a$	$a \circ \{e, x\}$
e	$\{e, x\}$	$\{e, x\}$
x	$\{x, e\}$	$\{x, e\}$
y	$\{y, z\}$	$\{y, z\}$
z	$\{z, y\}$	$\{z, y\}$

Die Untergruppe $(\{e, x\}, \circ)$ besitzt folgende rechte Nebenklassen:

$$\{e, x\}, \quad \{y, z\}.$$

Diese stimmen mit den linken Nebenklassen überein.

Noch ein Beispiel

Sei $(G, \circ)$ wieder eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	t	s	r	q
q	q	s	e	t	p	r
r	r	t	s	e	q	p
s	s	q	r	p	t	e
t	t	r	p	q	e	s

a	$\{e,p\} \circ a$	$a \circ \{e,p\}$
e	$\{e,p\}$	$\{e,p\}$
p	$\{p,e\}$	$\{p,e\}$
q	$\{q,t\}$	$\{q,s\}$
r	$\{r,s\}$	$\{r,t\}$
s	$\{s,r\}$	$\{s,q\}$
t	$\{t,q\}$	$\{t,r\}$

Die Untergruppe $(\{e,p\}, \circ)$ besitzt die rechten Nebenklassen

$$\{e,p\}, \quad \{q,t\}, \quad \{r,s\}$$

und die linken Nebenklassen

$$\{e,p\}, \quad \{q,s\}, \quad \{r,t\}.$$

Der Satz von Lagrange

Sei $(G, \circ)$ eine endliche Gruppe mit neutralem Element e. Dann gilt für jede Untergruppe $(H, \circ)$ von $(G, \circ)$: $|H|$ teilt $|G|$.

Info

Eine sehr wichtige Folgerung ist, dass die Ordnung $\text{ord}(a)$ aller Elemente $a \in G$ auch die Gruppenordnung $|G|$ teilen muss. Sonst wäre $(\langle a \rangle, \circ)$ eine Untergruppe, deren Ordnung $|\langle a \rangle|$ die Gruppenordnung $|G|$ nicht teilt.

Sei $(G, \circ)$ eine Gruppe mit $G = [307]$, neutralem Element $6 \in G$ und einer hochkomplizierten Operation $\circ$, die kein Mensch versteht.

1. Wie viele verschiedene Untergruppen besitzt $(G, \circ)$?
2. Welche Ordnung hat das Element $28 \in G$?

Erinnerung: $[307] = \{1, 2, \ldots, 307\}$.
Info: 307 ist prim und Lagrange toll.

1. Weil $|G| = 307$ prim ist, kann die Anzahl der Elemente einer Untergruppe nach dem Satz von Lagrange nur 1 oder 307 sein. Das sind genau die zwei trivialen Untergruppen $(G, \circ)$ und $(\{6\}, \circ)$. Es gibt also genau zwei Untergruppen.
2. Weil $|G| = 307$ prim ist, muss ord(28) nach dem Satz von Lagrange entweder 1 oder 307 sein. Ordnung 1 hat nur das neutrale Element 6, d.h. 28 muss die Ordnung $\text{ord}(28) = 307$ haben.

Gibt es eine nicht-zyklische Gruppe $(G, \circ)$ mit $|G|$ prim?

Nein!

Für jede Gruppe $(G, \circ)$ mit $|G|$ prim gilt nach dem Satz von Lagrange, dass alle Elemente in G entweder 1 oder $|G|$ als Ordnung haben. Da das neutrale Element das einzige Element mit Ordnung 1 ist, haben alle andere Ordnung $|G|$. G enthält also $|G| - 1$ verschiedene Erzeuger und ist somit automatisch zyklisch.

Wichtige Aussagen zu Gruppen

1. Sind $(H_1, \circ)$ und $(H_2, \circ)$ Untergruppen von $(G, \circ)$, dann auch $(H_1 \cap H_2, \circ)$.
2. $(\langle a \rangle, \circ)$ ist für jedes $a \in G$ eine zyklische Untergruppe von $(G, \circ)$.
3. Die Menge der rechten bzw. linken Nebenklassen einer Untergruppe $(H, \circ)$ von $(G, \circ)$ bildet eine Partition von G.
4. Jede Untergruppe einer zyklischen Gruppe $(G, \circ)$ ist auch zyklisch.
5. Jede zyklische Gruppe ist kommutativ.
6. Für jedes Element a einer Gruppe gilt: $\text{ord}(a) = |\langle a \rangle|$.

Wichtige Aussagen zu endlichen Gruppen

1. Jede Unteralgebra einer endlichen Gruppe ist eine Untergruppe.
2. Satz von Lagrange:
   Für jede Untergruppe $(H, \circ)$ einer endlichen Gruppe $(G, \circ)$ gilt: $|H|$ teilt $|G|$.
3. Satz von Lagrange (Folgerung):
   Für alle Elemente $a \in G$ einer endlichen Gruppe $(G, \circ)$ gilt: $\mathrm{ord}(a)$ teilt $|G|$.
4. Wenn $|G|$ prim ist, dann ist $(G, \circ)$ zyklisch.
5. Für jede endliche Gruppe $(G, \circ)$ gilt:

$$(G, \circ) \text{ zyklisch} \iff \exists a \in G : \mathrm{ord}(a) = |G| \ .$$

6. NEU: Für jedes Element a einer Gruppe $(G, \circ)$ gilt: $a^{-1} = a^{|G|-1}$.

Rezept

Frage: Wie findet man alle Untergruppen einer Gruppe $(G, \circ)$?
Methode: Bestimme für jedes $a \in G$ das Erzeugnis $\langle a \rangle$ und die Ordnung $\operatorname{ord}(a)$. Die Menge aller Erzeugnisse ist genau die Menge aller zyklischen Untergruppen. Dann:

1. Ist $(G, \circ)$ zyklisch, so gibt es keine weitere Untergruppen mehr.
2. Sind alle nichttrivialen Teiler von $|G|$ (also alle außer 1 und $|G|$) prim, so gibt es nur triviale und zyklische Untergruppen.
3. Für jeden nichttrivialen Teiler k von $|G|$, der nicht prim ist, versuche eine Untergruppe mit k Elementen durch Ausprobieren zu konstruieren. Die Ordnungen dieser Elemente sollen alle k teilen!

Beispiel

Sei $(G, \circ)$ wieder eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	p	q	r	s	t
e	e	p	q	r	s	t
p	p	e	r	q	t	s
q	q	r	s	t	p	e
r	r	q	t	s	e	p
s	s	t	p	e	r	q
t	t	s	e	p	q	r

$(G, \circ)$ besitzt folgende Erzeugnistafel:

a	$\langle a \rangle$	$\operatorname{ord}(a)$
e	$\{e\}$	1
p	$\{p, e\}$	2
q	$\{q, s, p, r, t, e\}$	6
r	$\{r, s, e\}$	3
s	$\{s, r, e\}$	3
t	$\{t, r, p, s, q, e\}$	6

Die Gruppe ist zyklisch, weil sie von q bzw. t erzeugt wird. D.h. es gibt nur zyklische Untergruppen:

$$\{e\}, \quad \{e, p\}, \quad \{e, r, s\}, \quad \{e, p, q, r, s, t\}.$$

Noch ein Beispiel

Sei $(G, \circ)$ wieder eine Gruppe mit neutralem Element e und folgender Verknüpfungstafel:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

$(G, \circ)$ besitzt folgende Erzeugnistafel:

a	$\langle a \rangle$	$\operatorname{ord}(a)$
e	$\{e\}$	1
x	$\{x, e\}$	2
y	$\{y, e\}$	2
z	$\{z, e\}$	2

Die Gruppe ist zwar nicht zyklisch, aber der einzige nichttriviale Teiler von $|G| = 4$ ist 2, also prim. Die Untergruppen sind also alle zyklisch oder trivial:

$$\{e\}, \quad \{e, x\}, \quad \{e, y\}, \quad \{e, z\}, \quad \{e, x, y, z\}.$$

Ein letztes Beispiel

Sei $(G, \circ)$ eine Gruppe mit folgender Verknüpfungstafel:

$\circ$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	1	3	6	8	5	7
3	3	1	4	2	7	5	8	6
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	8	5	7	2	4	1	3
7	7	5	8	6	3	1	4	2
8	8	7	6	5	4	3	2	1

$(G, \circ)$ besitzt folgende Erzeugnistafel:

a	$\langle a \rangle$	$\operatorname{ord}(a)$
1	$\{1\}$	1
2	$\{2, 4, 3, 1\}$	4
3	$\{3, 4, 2, 1\}$	4
4	$\{4, 1\}$	2
5	$\{5, 1\}$	2
6	$\{6, 4, 7, 1\}$	4
7	$\{7, 4, 6, 1\}$	4
8	$\{8, 1\}$	2

$(G, \circ)$ ist nicht zyklisch und $|G| = 8$ besitzt den nicht-trivialen Teiler 4. D.h. es könnte nicht-zyklische Untergruppen mit 4 Elementen geben.

Für diese Untergruppen kommen nur Elemente infrage, deren Ordnung kleiner oder gleich 4 ist (sonst wären sie zyklisch), aber 4 teilt (laut Lagrange).

In diesem Fall ist $\{1, 4, 5, 8\}$ die einzige Kandidatin für eine solche Untergruppe. Stellt man eine Verknüpfungstafel für sie auf, so stellt man fest, dass sie eine Unteralgebra und somit auch eine Untergruppe von $(G, \circ)$ bildet:

$\circ$	1	4	5	8
1	1	4	5	8
4	4	1	8	5
5	5	8	1	4
8	8	5	4	1

Die Untergruppen von $(G, \circ)$ sind also:

$$\underbrace{\{1\}, \{1,4\}, \{1,5\}, \{1,8\}, \{1,2,3,4\}, \{1,4,6,7\}}_{\text{zyklische Untergruppen}}, \underbrace{\{1,4,5,8\}, \{1,2,3,4,5,6,7,8\}}_{\text{nicht-zyklische Untergruppen}}.$$

Welche der folgenden Kongruenzen sind richtig? Streiche bei den falschen das Symbol $\equiv_n$ durch.

$$\begin{array}{rcl@{\qquad}rcl} -7 & \equiv_3 & 8, & 7 & \equiv_5 & -11, \\ 2 & \equiv_6 & 8, & -10 & \equiv_{11} & 22, \\ 3 & \equiv_{12} & 27, & 6 & \equiv_4 & 18, \\ -4 & \equiv_7 & -11, & 15 & \equiv_3 & -13, \\ 11 & \equiv_1 & -5, & -4 & \equiv_2 & 108. \end{array}$$

Hinweis: Was die Kongruenzrelation modulo n ist, muss bestimmt wieder aufgefrischt werden! Die Definition und ein paar Beispiele gibt es auf Folie 416.

$$
\begin{array}{rcl}
-7 & \equiv_3 & 8, \\
2 & \equiv_6 & 8, \\
3 & \equiv_{12} & 27, \\
-4 & \equiv_7 & -11, \\
11 & \equiv_1 & -5,
\end{array}
\qquad
\begin{array}{rcl}
7 & \not\equiv_5 & -11, \\
-10 & \not\equiv_{11} & 22, \\
6 & \equiv_4 & 18, \\
15 & \not\equiv_3 & -13, \\
-4 & \equiv_2 & 108.
\end{array}
$$

Themenübersicht

Additive Gruppe Modulo n

Seien $n \in \mathbb{N}$, $\mathbb{Z}_n := \{0, \ldots, n-1\}$ die Menge aller möglichen Reste einer Division durch n und $+_n$ die Addition modulo n mit

$$a +_n b := (a + b) \bmod n.$$

Dann ist $(\mathbb{Z}_n, +_n)$ für alle $n \in \mathbb{N}$ eine Gruppe.

Info

Weil wir $\mathbb{Z}_n$ immer nur in Kombination mit $+_n$ betrachten werden, schreiben wir oft einfach $\mathbb{Z}_n$ statt $(\mathbb{Z}_n, +_n)$.

Beispiel

$(\mathbb{Z}_3, +_3)$ ist eine Gruppe mit Trägermenge

$$\mathbb{Z}_3 = \{0, 1, 2\}$$

und folgender Verknüpfungstafel:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\longleftarrow$ z.B. $1 +_3 2 = (1 + 2) \bmod 3 = 0$

Noch ein Beispiel

$(\mathbb{Z}_4, +_4)$ ist eine Gruppe mit Trägermenge

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

und folgender Verknüpfungstafel:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\longleftarrow$ z.B. $2 +_4 3 = (2 + 3) \bmod 4 = 1$

Ein letztes Beispiel

$(\mathbb{Z}_5, +_5)$ ist eine Gruppe mit Trägermenge

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

und folgender Verknüpfungstafel:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\longleftarrow$ z.B. $3 +_5 4 = (3 + 4) \bmod 5 = 2$

Eigenschaften von $(\mathbb{Z}_n, +_n)$

Die Gruppe $\mathbb{Z}_n$ besitzt für jedes $n \in \mathbb{N}$ folgende Eigenschaften:

- $|\mathbb{Z}_n| = n$.
- Das neutrale Element ist die 0.
- Das inverse Element von $m \in \mathbb{Z}_n$ ist $m^{-1} = (-m) \bmod n$.
- $(\mathbb{Z}_n, +_n)$ ist kommutativ und zyklisch.
- Die Elemente 1 und $n-1$ sind immer Erzeuger der Gruppe. Es können aber mehr als die zwei sein!
- Die Ordnung von $m \in \mathbb{Z}_n$ ist $\text{ord}(m) = \frac{n}{\text{ggT}(m,n)}$.

Themenübersicht

Die Menge $\mathbb{Z}_n^*$

Für jedes $n \in \mathbb{N}$ enthält die Menge

$$\mathbb{Z}_n^* := \{m \in \mathbb{Z}_n\}\, \mathsf{ggT}(m, n) = 1$$

alle Zahlen aus $\mathbb{Z}_n$, die zu n teilerfremd sind.

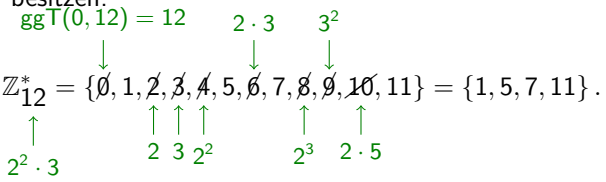
Infos

- Sind m und n klein, dann kann man sie in Primfaktoren zerlegen und überprüfen, ob sie mindestens einen gemeinsamen Primfaktor haben ($\mathrm{ggT}(m,n) > 1$) oder nicht ($\mathrm{ggT}(m,n) = 1$).
- Hat man keine Lust zu Faktorisieren, dann kann man $\mathrm{ggT}(m,n)$ mit dem euklidischen Algorithmus berechnen.
- Erinnerung: Für alle $n \in \mathbb{N}_0$ gilt $\mathrm{ggT}(0,n) = n$ und $\mathrm{ggT}(1,n) = 1$.

Beispiel

12 besitzt die Primteiler 2 und 3. Somit enthält $\mathbb{Z}_{12}^*$ alle Elemente aus $\mathbb{Z}_{12}$, die weder 2 als auch 3 als Primteiler besitzen.

Daraus folgt:



Quizfragen

1. Was ist $\mathbb{Z}_1^*$ extensional?
2. Was ist $\mathbb{Z}_2^*$ extensional?
3. Was ist $\mathbb{Z}_3^*$ extensional?
4. Was ist $\mathbb{Z}_4^*$ extensional?
5. Was ist $\mathbb{Z}_5^*$ extensional?
6. Was ist $\mathbb{Z}_6^*$ extensional?
7. Was ist $\mathbb{Z}_7^*$ extensional?
8. Was ist $\mathbb{Z}_8^*$ extensional?
9. Was ist $\mathbb{Z}_9^*$ extensional?
10. Was ist $\mathbb{Z}_{10}^*$ extensional?
11. Was ist $\mathbb{Z}_{18}^*$ extensional?
12. Was muss für n gelten, damit $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$ gilt?

Antworten

1. $\mathbb{Z}_1^* = \{0\}$ (wegen ggT$(0,1) = 1$, s. Infos auf Folie 1171),
2. $\mathbb{Z}_2^* = \{\cancel{0}, 1\} = \{1\}$,
3. $\mathbb{Z}_3^* = \{\cancel{0}, 1, 2\} = \{1, 2\}$,
4. $\mathbb{Z}_4^* = \{\cancel{0}, 1, \cancel{2}, 3\} = \{1, 3\}$,
5. $\mathbb{Z}_5^* = \{\cancel{0}, 1, 2, 3, 4\} = \{1, 2, 3, 4\}$,
6. $\mathbb{Z}_6^* = \{\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5\} = \{1, 5\}$,
7. $\mathbb{Z}_7^* = \{\cancel{0}, 1, 2, 3, 4, 5, 6\} = \{1, 2, 3, 4, 5, 6\}$.
8. $\mathbb{Z}_8^* = \{\cancel{0}, 1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7\} = \{1, 3, 5, 7\}$.
9. $\mathbb{Z}_9^* = \{\cancel{0}, 1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8\} = \{1, 2, 4, 5, 7, 8\}$.
10. $\mathbb{Z}_{10}^* = \{\cancel{0}, 1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9\} = \{1, 3, 7, 9\}$.

11. $\mathbb{Z}_{18}^* = \{\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17\} = \{1, 5, 7, 11, 13, 17\}$.
12. n muss teilerfremd zu $1, 2, 3, \ldots, n-1$ sein, d.h. n muss prim sein.

Info: $0 \in \mathbb{Z}_n^*$ gilt nur falls $n = 1$.

Eulersche Phi-Funktion

Die eulersche Phi-Funktion gibt die Anzahl der Elemente in $\mathbb{Z}_n^*$ an. Es gilt:

$$\varphi(n) := |\mathbb{Z}_n^*|.$$

Ist die Primfaktorzerlegung $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$ von n bekannt, dann kann man den Wert von $\varphi(n)$ ganz einfach mit folgender Formel berechnen:

$$\varphi(n) = p_1^{e_1-1} \cdot (p_1 - 1) \cdot p_2^{e_2-1} \cdot (p_2 - 1) \cdot \ldots \cdot p_k^{e_k-1} \cdot (p_k - 1).$$

Beispiel

Für 400 gilt:

$$\varphi(400) = 2^{4-1} \cdot (2-1) \cdot 5^{2-1} \cdot (5-1) = 8 \cdot 20 = 160.$$

$$\uparrow$$

$$2^4 \cdot 5^2$$

1. Was ist $\varphi(36)$?
2. Was ist $\varphi(64)$?
3. Was ist $\varphi(72)$?
4. Was ist $\varphi(210)$?
5. Was ist $\varphi(1000)$?
6. Ist φ monoton wachsend?

Info: Eine Funktion f heißt *monoton wachsend*, wenn für alle m, n im Definitionsbereich gilt:

$$m \leq n \implies f(m) \leq f(n) \ .$$

Antworten

1. $\varphi(36) = 2^{2-1} \cdot (2-1) \cdot 3^{2-1} \cdot (3-1) = 12$.
2. $\varphi(64) = 2^{6-1} \cdot (2-1) = 32$.
3. $\varphi(72) = 2^{3-1} \cdot (2-1) \cdot 3^{2-1} \cdot (3-1) = 24$.
4. $\varphi(210) = 2^{1-1} \cdot (2-1) \cdot 3^{1-1} \cdot (3-1) \cdot 5^{1-1} \cdot (5-1) \cdot 7^{1-1} \cdot (7-1) = 1 \cdot 2 \cdot 4 \cdot 6 = 48$.
5. $\varphi(1000) = 2^{3-1} \cdot (2-1) \cdot 5^{3-1} \cdot (5-1) = 4 \cdot 100 = 400$.
6. Nö! Es gilt $64 \leq 72$, aber $\varphi(64) > \varphi(72)$.

Multiplikative Gruppe Modulo n

Seien $n \in \mathbb{N}$ und $\cdot_n$ die Multiplikation modulo n mit

$$a \cdot_n b := (a \cdot b) \bmod n.$$

Dann ist $(\mathbb{Z}_n^*, \cdot_n)$ eine Gruppe.

Infos

- Die Menge $\mathbb{Z}_n$ (ohne Stern) bildet mit $\cdot_n$ ein Monoid, aber nicht immer eine Gruppe.
- $\mathbb{Z}_n^*$ enthält genau die Elemente aus $\mathbb{Z}_n$, die ein Inverses bezüglich $\cdot_n$ besitzen.
- Weil wir $\mathbb{Z}_n^*$ immer nur in Kombination mit $\cdot_n$ betrachten werden, schreiben wir oft einfach $\mathbb{Z}_n^*$ statt $(\mathbb{Z}_n^*, \cdot_n)$.

Beispiel

$(\mathbb{Z}_6^*, \cdot_6)$ ist eine Gruppe mit Trägermenge

$$\mathbb{Z}_6^* = \{1, 5\}$$

und folgender Verknüpfungstafel:

$\cdot_6$	1	5
1	1	5
5	5	1

← z.B. $5 \cdot_6 5 = (5 \cdot 5) \bmod 6 = 25 \bmod 6 = 1$

Noch ein Beispiel

$(\mathbb{Z}_{10}^*, \cdot_{10})$ ist eine Gruppe mit Trägermenge

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

und folgender Verknüpfungstafel:

$\cdot_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

← z.B. $7 \cdot_{10} 9 = (7 \cdot 9) \bmod 10 = 63 \bmod 10 =$

Ein letztes Beispiel

$(\mathbb{Z}_{18}^*, \cdot_{18})$ ist eine Gruppe mit Trägermenge

$$\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$$

und folgender Verknüpfungstafel:

$\cdot_{18}$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

← z.B. $11 \cdot_{18} 17 = (11 \cdot 17) \bmod 18 = 18$

Quizfragen

1. Wie sieht die Verknüpfungstafel von $(\mathbb{Z}_8^*, \cdot_8)$ aus?
2. Wie sieht die Verknüpfungstafel von $(\mathbb{Z}_{12}^*, \cdot_{12})$ aus?

1. Wir hatten bereits:

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}\,.$$

Die Verknüpfungstafel von $(\mathbb{Z}_8^*, \cdot_8)$ ist dann:

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

2. Wir hatten bereits:

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}\,.$$

Die Verknüpfungstafel von $(\mathbb{Z}_{12}^*, \cdot_{12})$ ist dann:

$\cdot_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Inverse Elemente in $(\mathbb{Z}_n^*, \cdot_n)$

Um das inverse Element von $m \in \mathbb{Z}_n^*$ zu bestimmen, führt man den erweiterten euklidischen Algorithmus mit n und m aus. So erhält man ganze Zahlen a, b mit:

$$a \cdot m + b \cdot n = 1.$$

Nimmt man beide Seiten der Gleichung modulo n, so erhält man wegen

$$(a \cdot m + b \cdot n) \bmod n = (a \cdot m) \bmod n \qquad = ((a \bmod n) \cdot m) \bmod n = (a \bmod n) \cdot_n m$$

die Gleichung

$$(a \bmod n) \cdot_n m = 1.$$

Daraus folgt: $m^{-1} = a \bmod n$.

Beispiel

Der Verknüpfungstafel auf Folie 1185 können wir entnehmen, dass 13 das multiplikative Invere von 7 in $\mathbb{Z}_{18}^*$ ist. Wir überprüfen dies mit dem erweiterten euklidischen Algorithmus.

r_i	s_i	t_i
18	–	-5
7	2	2
4	1	-1
3	1	1
1	5	0
0	–	–

Dann gilt $18 \cdot 2 + 7 \cdot (-5) = 1$ und daher:

$$7^{-1} = -5 \bmod 18 = 13.$$

Noch ein Beispiel

Gesucht ist das inverse Element 21^{-1} zu 21 bezüglich $\mathbb{Z}_{100}^*$. Aus dem Beispiel auf Folie 453 haben wir folgende Ausführung des erweiterten euklidischen Algorithmus:

r_i	s_i	t_i
100	–	-19
21	4	4
16	1	-3
5	3	1
1	5	0
0	–	–

Dann gilt $100 \cdot 4 + 21 \cdot (-19) = 1$ und daher:

$$21^{-1} = -19 \bmod 100 = 81.$$

Infos

- Erinnerung: m besitzt genau dann ein multiplikatives Inverses bezüglich $\cdot_n$, wenn $\mathrm{ggT}(m, n) = 1$ gilt.
- Das multiplikative Inverse zu einer Zahl $m \in \mathbb{Z}_n^*$ wird immer an derselben Position in der Tabelle zu finden sein! :-)

Gegeben seien folgende Zahlenpaare m, n mit $n \in \mathbb{N}$ und $m \in \mathbb{Z}_n^*$:

1. $m = 81$, $n = 128$.
2. $m = 73$, $n = 215$.
3. $m = 32$, $n = 91$.
4. $m = 41$, $n = 106$.
5. $m = 157$, $n = 432$.
6. $m = 73$, $n = 255$.

Was ist das Inverse m^{-1} zu m in $\mathbb{Z}_n^*$?

Antworten (ohne Rechnungen)

1. In $\mathbb{Z}_{128}^*$ gilt: $81^{-1} = 49$.
2. In $\mathbb{Z}_{215}^*$ gilt: $73^{-1} = 162$.
3. In $\mathbb{Z}_{91}^*$ gilt: $32^{-1} = 37$.
4. In $\mathbb{Z}_{106}^*$ gilt: $41^{-1} = 75$.
5. In $\mathbb{Z}_{432}^*$ gilt: $157^{-1} = 421$.
6. In $\mathbb{Z}_{255}^*$ gilt: $73^{-1} = 7$.

Eigenschaften von $(\mathbb{Z}_n^*, \cdot_n)$

Die Gruppe $\mathbb{Z}_n^*$ besitzt für jedes $n \in \mathbb{N}$ mit $n \geq 2$ folgende Eigenschaften:

- $|\mathbb{Z}_n^*| = \varphi(n)$
- Das neutrale Element ist die 1.
- Inverse Elemente bestimmt man mit dem erweitertem euklidischen Algorithmus
- $(\mathbb{Z}_n^*, \cdot_n)$ ist kommutativ, aber nicht immer zyklisch.
- Die Ordnung $\text{ord}(m)$ von $m \in \mathbb{Z}_n^*$ muss man leider durch systematisches Ausprobieren bestimmen (s. nächste Folie).

Für $n = 1$ ist $(\mathbb{Z}_n^*, \cdot_n)$ identisch zu $(\mathbb{Z}_n, +_n)$. Für die Eigenschaften siehe Folie 1169.

Beispiel

Wir bestimmen die Ordnung von 7 in $\mathbb{Z}_{22}^*$.

Wegen

$$|\mathbb{Z}_{22}^*| = \varphi(22) = 2^{1-1} \cdot (2-1) \cdot 11^{1-1} \cdot (11-1) = 10$$

muss nach Lagrange $\mathrm{ord}(m) \in \{1, 2, 5, 10\}$ für alle $m \in \mathbb{Z}_{22}^*$ gelten.

$$\begin{array}{lcl} 7 \bmod 22 = 7 \neq 1 & \leadsto & \mathrm{ord}(7) \neq 1 \\ 7^2 \bmod 22 = 5 \neq 1 & \leadsto & \mathrm{ord}(7) \neq 2 \\ 7^5 \bmod 22 = 21 \neq 1 & \leadsto & \mathrm{ord}(7) \neq 5 \end{array}$$

Daraus folgt sofort: $\mathrm{ord}(7) = 10$.

Satz von Euler

Sind $a, n \in \mathbb{N}$ zueinander teilerfremd, dann gilt:

$$a^{\varphi(n)} \equiv_n 1.$$

Daraus folgt:

$$a^m \bmod n = a^{m \bmod \varphi(n)} \bmod n.$$

Beispiel

Da 3 und 4 teilerfremd sind, gilt:

$$3^{61} \bmod 4 = 3^{61 \bmod 2} \bmod 4 = 3^1 \bmod 4 = 3.$$

$\uparrow$

$\varphi(4) = 2$

Noch ein Beispiel

Auf

$$5^{73} \bmod 110$$

kann der Satz von Euler nicht direkt angewendet werden, da 5 und 110 nicht teilerfremd sind. Es gilt nämlich $\text{ggT}(5, 110) = 5$.

Mithilfe der Rechenregeln auf Folie 433 erhalten wir:

$$5^{73} \bmod 110 = 5 \cdot (5^{72} \bmod 22) = 5 \cdot (5^{72 \bmod 10} \bmod 22) = 5 \cdot (5^2 \bmod 22) = 5 \cdot 3 = 15.$$

$\uparrow$

$\varphi(22) = 10$

Was ist $2^{308} \bmod 250$?

$$2^{308} \bmod 250 = 2 \cdot (2^{307} \bmod 125) = 2 \cdot (2^{307 \bmod 100} \bmod 125) = 2 \cdot (2^7 \bmod 125) = 6.$$

$\uparrow$

$\varphi(125) = 100$

Themenübersicht

Rechnen mit Permutationen

Im Abschnitt *Relationen und Abbildungen* haben wir gelernt, was Permutationen sind (s. ab Folie 503). Im Abschnitt *Fundamentale Zählkoeffizienten* haben wir die Zyklenschreibweise für Permutationen kennengelernt (s. ab Folie 784).

Weil Permutationen Funktionen über eine Menge A sind, kann man Permutationen p_1, p_2 mit der Komposition von Funktionen $\circ$ verknüpfen und eine neue Permutation $p_3 = p_1 \circ p_2$ erhalten. Dann gilt für alle $x \in A$:

$$p_3(x) = (p_1 \circ p_2)(x) = p_1(p_2(x)).$$

Beispiele:

- Matrixschreibweise:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

- Zyklenschreibweise:

$$(1,3)(2)(4) \circ (1,4,2)(3) = (1,4,2,3)$$

Gegeben seien folgende Permutationen p_1, p_2 und p_3 über $[6]$ in Zyklendarstellung:

1. $p_1 = (1,4)(2,6,3)(5)$,
2. $p_2 = (3,2,4,1,5,6)$,
3. $p_3 = (1,4)(2,5)(3,6)$.

Wie sehen die Umkehrfunktionen p_1^{-1}, p_2^{-1} und p_3^{-1} in Zyklendarstellung aus?

Einfach die Zyklen umdrehen!

1. $p_1^{-1} = (1,4)(2,3,6)(5)$,
2. $p_2^{-1} = (1,4,2,3,6,5)$,
3. $p_3^{-1} = (1,4)(2,5)(3,6)$.

Bei den Zyklen wurde außerdem so lange geshiftet, bis die kleinste Zahl links steht. Das ist aber nicht nötig.

Was sind die Ergebnisse in Zyklendarstellung folgender Kompositionen?

1. $(2,6)(3,1,4,5) \circ (1)(3,2,4,6)(5)$,
2. $(6,3,4)(2,5,1) \circ (6,2,4,3,1,5)$,
3. $(3,1)(5,4)(2,6) \circ (4,6)(2,3,1)(5)$.

Antworten

1. $(1, 4, 2, 5, 3, 6)$.
2. $(1)(2, 6, 5, 3)(4)$.
3. $(1, 6, 5, 4, 2)(3)$.

Was ist

$$(1,3,5,4)(2,6) \circ (1,4)(2,5,6)(3) \circ (1,5,6)(2,4,3)$$

in Zyklenschreibweise?

Hinweis: Für alle Permutationen p, q, r über A und alle $x \in A$ gilt:

$$(p \circ q \circ r)(x) = p(q(r(x))).$$

D.h. die eingesetzte Zahl x „wandert von rechts nach links“.

Antwort

$$(1,3,5,4)(2,6) \circ (1,4)(2,5,6)(3) \circ (1,5,6)(2,4,3) = (1,2,3,4,5,6).$$

Seien p und q Permutationen über $[6]$ mit

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 6 & 1 & 4 \end{pmatrix} \qquad \text{und} \qquad q = (1,4,3)(2,6,5).$$

1. Was ist p in Zyklenschreibweise?
2. Was ist q in Matrixschreibweise?
3. Was ist $p \circ q$ in Matrixschreibweise?
4. Was ist $q \circ p$ in Zyklenschreibweise?
5. Was ist p^{-1} in Matrixschreibweise?
6. Was ist q^{-1} in Zyklenschreibweise?

Antworten

1. $p = (1,3,5)(2)(4,6)$.
2. $q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 2 & 5 \end{pmatrix}$.
3. $p \circ q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$.
4. $q \circ p = (1)(2,6,3)(4,5)$.
5. $p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$.
6. $q^{-1} = (1,3,4)(2,5,6)$.

Symmetrische Gruppe

Seien $n \in \mathbb{N}$, S_n die Menge aller Permutationen über $[n]$ und $\circ$ die Komposition von Funktionen. Dann ist $(S_n, \circ)$ für alle $n \in \mathbb{N}$ eine Gruppe.

Infos

- Weil wir S_n immer nur in Kombination mit $\circ$ betrachten werden, schreiben wir oft einfach S_n statt $(S_n, \circ)$.
- Obwohl $(S_n, \circ)$ Symmetrische Gruppe heißt, hat ihre Verknüpfungstafel nichts mit Symmetrie zu tun. $(S_1, \circ)$ und $(S_2, \circ)$ sind zwar kommutativ, aber

$$(S_3, \circ), (S_4, \circ), (S_5, \circ), (S_6, \circ), (S_7, \circ), \ldots$$

alle nicht!

Beispiel

$(S_1, \circ)$ ist eine Gruppe mit

$$S_1 = \{(1)\}$$

und folgender Verknüpfungstafel:

$\circ$	(1)
(1)	(1)

Beispielsweise gilt: $(1) \circ (1) = (1)$.

Noch ein Beispiel

$(S_2, \circ)$ ist eine Gruppe mit

$$S_2 = \{(1)(2), (1,2)\}$$

und folgender Verknüpfungstafel:

$\circ$	$(1)(2)$	$(1,2)$
$(1)(2)$	$(1)(2)$	$(1,2)$
$(1,2)$	$(1,2)$	$(1)(2)$

Beispielsweise gilt: $(1,2) \circ (1,2) = (1)(2)$.

Ein letztes Beispiel

$(S_3, \circ)$ ist eine Gruppe mit

$$S_3 = \{(1)(2)(3), (1,2)(3), (1,3)(2), (1)(2,3), (1,2,3), (1,3,2)\}$$

und folgender Verknüpfungstafel:

$\circ$	$(1)(2)(3)$	$(1,2)(3)$	$(1,3)(2)$	$(1)(2,3)$	$(1,2,3)$	$(1,3,2)$
$(1)(2)(3)$	$(1)(2)(3)$	$(1,2)(3)$	$(1,3)(2)$	$(1)(2,3)$	$(1,2,3)$	$(1,3,2)$
$(1,2)(3)$	$(1,2)(3)$	$(1)(2)(3)$	$(1,3,2)$	$(1,2,3)$	$(1)(2,3)$	$(1,3)(2)$
$(1,3)(2)$	$(1,3)(2)$	$(1,2,3)$	$(1)(2)(3)$	$(1,3,2)$	$(1,2)(3)$	$(1)(2,3)$
$(1)(2,3)$	$(1)(2,3)$	$(1,3,2)$	$(1,2,3)$	$(1)(2)(3)$	$(1,3)(2)$	$(1,2)(3)$
$(1,2,3)$	$(1,2,3)$	$(1,3)(2)$	$(1)(2,3)$	$(1,2)(3)$	$(1,3,2)$	$(1)(2)(3)$
$(1,3,2)$	$(1,3,2)$	$(1)(2,3)$	$(1,2)(3)$	$(1,3)(2)$	$(1)(2)(3)$	$(1,2,3)$

Beispielsweise gilt: $(1,2,3) \circ (1,3)(2) = (1)(2,3)$.

Quizfrage

Wie viele Elemente enthält S_n für ein allgemeines $n \in \mathbb{N}$?

Antwort

$$|S_n| = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$$

Seien $p = (1,2,3,4)$, $q = (1,3)(2,4)$, $r = (1,4,3,2)$ und $\mathrm{id} = (1)(2)(3)(4)$ vier Permutationen über [4] und $(G, \circ)$ eine Untergruppe der symmetrischen Gruppe $(S_4, \circ)$ mit $G = \{\mathrm{id}, p, q, r\}$.

1. Wie sieht die Verknüpfungstafel von $(G, \circ)$ aus?
2. Was ist das inverse Element a^{-1} von jedem $a \in G$?
3. Was ist die Ordnung $\mathrm{ord}(a)$ von jedem $a \in G$?
4. Ist $(G, \circ)$ zyklisch?

1. Die Verknüpfungstafel von $(G, \circ)$ ist:

$\circ$	id	p	q	r
id	id	p	q	r
p	p	q	r	id
q	q	r	id	p
r	r	id	p	q

2. $$\mathrm{id}^{-1} = \mathrm{id}, \quad p^{-1} = r, \quad q^{-1} = q, \quad r^{-1} = p.$$

3. $$\mathrm{ord}(\mathrm{id}) = 1, \quad \mathrm{ord}(p) = 4, \quad \mathrm{ord}(q) = 2, \quad \mathrm{ord}(r) = 4.$$

4. Ja! p und r sind Erzeuger.

Eigenschaften von $(S_n, \circ)$

Die Gruppe S_n besitzt für jedes $n \in \mathbb{N}$ folgende Eigenschaften:

- $|S_n| = n!$.
- Das neutrale Element ist die Identitätsfunktion $\mathrm{id} = (1)(2)\dots(n)$.
- Das inverse Element p^{-1} von $p \in S_n$ ist einfach die Umkehrfunktion von p.
- $(S_n, \circ)$ ist kommutativ (abelsch) und zyklisch für $n = 1$ und $n = 2$, ansonsten ist sie weder kommutativ noch zyklisch.
- Die Ordnung $\mathrm{ord}(p)$ von einem Element $p \in S_n$ ist das kleinste gemeinsame Vielfache $\mathrm{kgV}\{l_1, l_2, \dots, l_k\}$ der Zyklenlängen $l_1, l_2, \dots, l_k$, z.B. gilt in S_9:

$$\mathrm{ord}\big(\underbrace{(1,7,4,3)}_{\text{Länge 4}}\underbrace{(2,8,6)}_{\text{Länge 3}}\underbrace{(5,9)}_{\text{Länge 2}}\big) = \mathrm{kgV}\{4,3,2\} = 12$$

Welche Ordnung besitzen folgende Permutationen aus $(S_9, \circ)$?

1. $p = (4, 6, 2, 5)(3, 1, 9)(7, 8)$
2. $q = (1, 6)(5)(3, 8, 2)(4)(9, 7)$
3. $r = (3, 5, 7)(9, 1, 2)(8, 4, 6)$
4. $s = (5, 9)(1, 3)(2, 7)(4, 6, 8)$

Antworten

1. $\mathrm{ord}(p) = \mathrm{kgV}\,\{4, 3, 2\} = 12$.
2. $\mathrm{ord}(q) = \mathrm{kgV}\,\{2, 1, 3, 1, 2\} = 6$.
3. $\mathrm{ord}(r) = \mathrm{kgV}\,\{3, 3, 3\} = 3$.
4. $\mathrm{ord}(s) = \mathrm{kgV}\,\{2, 2, 2, 3\} = 6$.

1. Für welche Permutation $p \in S_9$ gilt $\mathrm{ord}(p) = 15$?
2. Für welche Permutation $q \in S_9$ gilt $\mathrm{ord}(q) = 9$?
3. Für welche Permutation $r \in S_9$ gilt $\mathrm{ord}(r) = 5$?
4. Für welche Permutation $s \in S_9$ gilt $\mathrm{ord}(s) = 14$?

Gib jeweils ein Beispiel an.

1. p muss Zyklen der Längen 1, 3 und 5 haben, z.B.

$$p = (1)(2,3,4)(5,6,7,8,9).$$

2. q muss einen Zyklus der Länge 9 haben, z.B.

$$q = (1,2,3,4,5,6,7,8,9).$$

3. r muss vier Zyklen der Länge 1 und einen der Länge 5 haben, z.B.

$$r = (1)(2)(3)(4)(5,6,7,8,9).$$

4. s muss einen Zyklus der Länge 2 und einen der Länge 7 haben, z.B.

$$s = (1,2)(3,4,5,6,7,8,9).$$

Überblick: Eigenschaften der Gruppen $(\mathbb{Z}_n, +_n)$, $(\mathbb{Z}_n^*, \cdot_n)$ und $(S_n, \circ)$

	$(\mathbb{Z}_n, +_n)$	$(\mathbb{Z}_n^*, \cdot_n)$	$(S_n, \circ)$
Gruppenordnung	n	$\varphi(n)$	$n!$
Neutrales Element	0	1	$\mathrm{id} = (1)(2)\dots(n)$
Inversenbildung	durch Negation und Modulobildung $m^{-1} = -m \bmod n$	mit dem erweiterten euklidischen Algorithmus: $m^{-1} = a \bmod n$	durch Bildung der Umkehrfunktion p^{-1} von p
Kommutativ	immer	immer	nur falls $n \leq 2$
Zyklisch	immer	manchmal	nur falls $n \leq 2$
Elementenordnung	$\mathrm{ord}(m) = \frac{n}{\mathrm{ggT}(m,n)}$	ausprobieren	$\mathrm{ord}(p) = \mathrm{kgV}\{l_1, l_2, \dots, l_k\}$

Info

Siehe Folien 1169, 1195 und 1222.

Themenübersicht

Inneres Produkt

Seien $(A, \circ)$ und $(B, \bullet)$ beliebige Algebren. Dann heißt

$$(A, \circ) \times (B, \bullet) := (A \times B, \circ \times \bullet)$$

mit

$$(a, b)(\circ \times \bullet)(c, d) = (a \circ c, b \bullet d)$$

das innere Produkt (oder direkte Produkt) aus $(A, \circ)$ und $(B, \bullet)$.

Beispiel

Seien $(A, \circ)$ und $(B, \bullet)$ mit $A = \{a, b, c\}$, $B = \{d, e\}$ und:

$(A, \circ)$:

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$(B, \bullet)$:

$\bullet$	d	e
d	d	e
e	e	d

Dann besitzt $(A, \circ) \times (B, \bullet)$ folgende Verknüpfungstafel:

$\circ \times \bullet$	(a, d)	(a, e)	(b, d)	(b, e)	(c, d)	(c, e)
(a, d)	(a, d)	(a, e)	(b, d)	(b, e)	(c, d)	(c, e)
(a, e)	(a, e)	(a, d)	(b, e)	(b, d)	(c, e)	(c, d)
(b, d)	(b, d)	(b, e)	(c, d)	(c, e)	(a, d)	(a, e)
(b, e)	(b, e)	(b, d)	(c, e)	(c, d)	(a, e)	(a, d)
(c, d)	(c, d)	(c, e)	(a, d)	(a, e)	(b, d)	(b, e)
(c, e)	(c, e)	(c, d)	(a, e)	(a, d)	(b, e)	(b, d)

z.B.: $(b, d)(\circ \times \bullet)(c, e) = (b \circ c, d \bullet e) = (a, e)$

Mehr Beispiele

Seien $(\mathbb{Z}_2, +_2)$ und $(\mathbb{Z}_2, \cdot_2)$ mit folgenden Verknüpfungstafeln:

$(\mathbb{Z}_2, +_2)$:

$+_2$	0	1
0	0	1
1	1	0

$(\mathbb{Z}_2, \cdot_2)$:

$\cdot_2$	0	1
0	0	0
1	0	1

- $(\mathbb{Z}_2, +_2) \times (\mathbb{Z}_2, \cdot_2)$ besitzt folgende Verknüpfungstafel:

$+_2 \times \cdot_2$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,0)$	$(0,0)$	$(0,0)$
$(1,1)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$

Eigenschaften des inneren Produkts $(A, \circ) \times (B, \bullet)$

Für Algebren $(A, \circ)$ und $(B, \bullet)$ gilt immer:

- $(A, \circ) \times (B, \bullet)$ besitzt $|G| \cdot |T|$ Elemente.
- $(A, \circ) \times (B, \bullet)$ ist nur dann assoziativ, wenn A und B jeweils assoziativ sind.
- $(A, \circ) \times (B, \bullet)$ hat nur dann ein neutrales Element (e_A, e_B), wenn A und B jeweils neutrale Elemente $e_A \in G$ und $e_B \in T$ haben.
- In $(A, \circ) \times (B, \bullet)$ haben alle Elemente $(x, y) \in G \times T$ ein Inverses $(x, y)^{-1} = (x^{-1}, y^{-1})$ nur, wenn jedes $x \in G$ ein Inverses x^{-1} in A und jedes $y \in T$ ein Inverses y^{-1} in B besitzen.
- $(A, \circ) \times (B, \bullet)$ ist nur dann kommutativ, wenn A und B jeweils kommutativ sind.

Ist die Aussage

„Für beliebige zyklische Gruppen A und B ist auch $(A, \circ) \times (B, \bullet)$ zyklisch“

wahr oder falsch?

Falsch! $(\mathbb{Z}_2, +_2)$ ist zyklisch ($\text{ord}(1) = 2 = |\mathbb{Z}_2|$), aber $(\mathbb{Z}_2 \times \mathbb{Z}_2, +_2 \times +_2)$ nicht. Es gilt nämlich $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, aber kein Element hat Ordnung 4:

$+_2 \times +_2$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

$\text{ord}((0,0)) = 1$ $\text{ord}((0,1)) = 2$ $\text{ord}((1,0)) = 2$ $\text{ord}((1,1)) = 2$

Themenübersicht

Isomorphismus bei Algebren

Für beliebige Algebren $(A, \circ)$ und $(B, \bullet)$ gilt $(A, \circ) \cong (B, \bullet)$ genau dann, wenn es eine bijektive Funktion $h : A \to B$ mit der Homomorphieeigenschaft

$$\forall x, y \in A : h(x \circ y) = h(x) \bullet h(y)$$

gibt.

Eine solche Funktion h wird Isomorphismus genannt.

Infos

- Für $(A, \circ) \cong (B, \bullet)$ sagen wir „$(A, \circ)$ und $(B, \bullet)$ sind isomorph zueinander“.
- Ein Homomorphismus ist eine Verallgemeinerung des Isomorphismus, bei dem h nicht notwendigerweise bijektiv sein muss.

Intuitiv heißt das, dass $(A, \circ)$ und $(B, \bullet)$ zwar unterschiedliche Objekte mit unterschiedlichen Namen sind, aber dieselbe „Struktur“ haben und somit auch dieselben Eigenschaften:

$(A, \circ)$:

$\circ$	$\cdots$	y	$\cdots$
$\vdots$		$\vdots$	
x	$\cdots$	$x \circ y$	$\cdots$
$\vdots$		$\vdots$	

$(B, \bullet)$:

$\bullet$	$\cdots$	$h(y)$	$\cdots$
$\vdots$		$\vdots$	
$h(x)$	$\cdots$	$h(x \circ y)$	$\cdots$
$\vdots$		$\vdots$	

D.h. man kann die linke Verknüpfungstafel nehmen, die Elemente in ihr nach h unbenennen und man würde die rechte Tabelle erhalten (mit eventuellen Zeilen- bzw. Spaltenvertauschungen).

Beispiel

Seien $(A, \circ)$ und $(B, \bullet)$ zwei Algebren mit $A = \{a, b, c\}$ und $B = \{r, s, t\}$ und $h : \{a, b, c\} \to \{r, s, t\}$ eine Funktion wie folgt:

$(A, \circ)$:

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$(B, \bullet)$:

$\bullet$	r	s	t
r	t	r	s
s	r	s	t
t	s	t	r

h :

x	$h(x)$
a	s
b	r
c	t

h ist ein Isomorphismus zwischen $(A, \circ)$ und $(B, \bullet)$. Intuitiv heißt das, dass wir durch die Umbenennung h der Elemente in $(A, \circ)$ wir genau $(B, \bullet)$ erhalten. D.h., dass $(A, \circ)$ und $(B, \bullet)$ bis auf Unbenennung der Elemente gleich sind (dieselbe „Struktur“ haben).

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

umbenennen $\rightsquigarrow$

$\bullet$	s	r	t
s	s	r	t
r	r	t	s
t	t	s	r

umordnen $\rightsquigarrow$

$\bullet$	r	s	t
r	t	r	s
s	r	s	t
t	s	t	r

Beispiel

Formal muss die Homomorphieeigenschaft gezeigt werden. Wir müssen also

$$h(x \circ y) = h(x) \bullet h(y)$$

für alle $x, y \in \{a, b, c\}$ zeigen. Weil $(A, \circ)$ und $(B, \bullet)$ beide endlich sind kann man einfach alle $3^2 = 9$ Gleichungen getrennt überprüfen.

Beispiel

$(A, \circ)$:

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$(B, \bullet)$:

$\bullet$	r	s	t
r	t	r	s
s	r	s	t
t	s	t	r

h :

x	$h(x)$
a	s
b	r
c	t

Beispiel

Beweis mit Brute Force:

$$
\begin{aligned}
h(a \circ a) = h(a) &= s = s \bullet s = h(a) \bullet h(a) \\
h(a \circ b) = h(b) &= r = s \bullet r = h(a) \bullet h(b) \\
h(a \circ c) = h(c) &= t = s \bullet t = h(a) \bullet h(c) \\
h(b \circ a) = h(b) &= r = r \bullet s = h(b) \bullet h(a) \\
h(b \circ b) = h(c) &= t = r \bullet r = h(b) \bullet h(b) \\
h(b \circ c) = h(a) &= s = r \bullet t = h(b) \bullet h(c) \\
h(c \circ a) = h(c) &= t = t \bullet s = h(c) \bullet h(a) \\
h(c \circ b) = h(a) &= s = t \bullet r = h(c) \bullet h(b) \\
h(c \circ c) = h(b) &= r = t \bullet t = h(c) \bullet h(c)
\end{aligned}
$$

Noch ein Beispiel

Die Gruppen $\mathbb{Z}_8^*$ und $\mathbb{Z}_{12}^*$ besitzen folgende Verknüpfungstafeln:

$\mathbb{Z}_8^*$:

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\mathbb{Z}_{12}^*$:

$\cdot_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Hier erkennt man sofort, dass folgende Funktion $h : \mathbb{Z}_8^* \to \mathbb{Z}_{12}^*$ ein Isomorphismus ist:

$$h(1) = 1, \quad h(3) = 5, \quad h(5) = 7, \quad h(7) = 11.$$

Letztes Beispiel

Für die Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}^+, \cdot)$ gilt $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$, d.h. sie sind isomorph zueinander. Ein möglicher Isomorphismus ist $h : \mathbb{R} \to \mathbb{R}^+$ mit:

$$h(x) = e^x$$

h ist (offensichtlich ;-)) bijektiv und es gilt für beliebige $x, y \in \mathbb{R}$:

$$h(x + y) = e^{x+y} = e^x \cdot e^y = h(x) \cdot h(y)$$

□

Infos

- Es ist einfach zu beweisen, dass eine gegebene Funktion h ein Isomorphismus ist.
- Am schwierigsten ist es aber, einen Isomorphismus selber zu finden.

Rezept

Frage: Wie kann man ein Gruppenisomorphismus finden?
Methode: Bei Gruppenisomorphismen h gilt folgende Implikation:

$$h(x) = y \quad \Longrightarrow \quad \text{ord}(x) = \text{ord}(y)$$

Daraus entsteht folgende Strategie:

1. Liste die Ordnungen aller Elemente beider Gruppen auf.
2. Verbinde diejenigen Elemente, deren Ordnung nur einmal vorkommen (z.B. neutrale Elemente).
3. überlege, wie der Rest aussehen könnte (eventuell durch ausprobieren!) .
4. Beweise, ob die entstandene Funktion tatsächlich ein Isomorphismus ist.

Info

Bei der Konstruktion von Isomorphismen gibt es drei wichtige Spezialfälle, die für uns in DS völlig ausreichend sind:

- Sind die Gruppen unterschiedlich groß, dann können sie nicht isomorph sein.
- Stellt man fest, dass die Ordnungen beider Gruppen anders sind, dann sind sie automatisch nicht isomorph.
- Sind beide Gruppen zyklisch, so kann man einen beliebigen Erzeuger der einen Gruppe mit einem beliebigen Erzeuger der anderen verbinden und sich den Rest systematisch konstruieren :-)

Beispiel

Für die Gruppen $\mathbb{Z}_6$ und $\mathbb{Z}_7^*$ gilt:

$\mathbb{Z}_6$:

x	0	1	2	3	4	5
$\text{ord}(x)$	1	6	3	2	3	6

$\mathbb{Z}_7^*$:

x	1	2	3	4	5	6
$\text{ord}(x)$	1	3	6	3	6	2

$\mathbb{Z}_6$ und $\mathbb{Z}_7^*$ sind beide zyklisch. Mögliche Erzeuger sind $1 \in \mathbb{Z}_6$ und $3 \in \mathbb{Z}_7^*$.
$\mathbb{Z}_6$ wird wie folgt von 1 erzeugt:

$$1 \xrightarrow{+_6 1} 2 \xrightarrow{+_6 1} 3 \xrightarrow{+_6 1} 4 \xrightarrow{+_6 1} 5 \xrightarrow{+_6 1} 0$$

Analog wird $\mathbb{Z}_7^*$ wird wie folgt von 3 erzeugt:

$$3 \xrightarrow{\cdot_7 3} 2 \xrightarrow{\cdot_7 3} 6 \xrightarrow{\cdot_7 3} 4 \xrightarrow{\cdot_7 3} 5 \xrightarrow{\cdot_7 3} 1$$

Beispiel

Wir setzen also z.B. $h : \mathbb{Z}_6 \to \mathbb{Z}_7^*$ mit $h(1) = 3$ und berechnen die restlichen Werte von h systematisch:

$$
\begin{aligned}
h(2) &= h(1 +_6 1) = h(1) \cdot_7 h(1) = 3 \cdot_7 3 = 2 \\
h(3) &= h(1 +_6 2) = h(1) \cdot_7 h(2) = 3 \cdot_7 2 = 6 \\
h(4) &= h(1 +_6 3) = h(1) \cdot_7 h(3) = 3 \cdot_7 6 = 4 \\
h(5) &= h(1 +_6 4) = h(1) \cdot_7 h(4) = 3 \cdot_7 4 = 5 \\
h(0) &= h(1 +_6 5) = h(1) \cdot_7 h(5) = 3 \cdot_7 5 = 1
\end{aligned}
$$

Man kann an folgendem Diagramm sehr schön erkennen wieso das funktioniert:

$$
\begin{array}{cccccccccccc}
 & 1 & \xrightarrow{+_6 1} & 2 & \xrightarrow{+_6 1} & 3 & \xrightarrow{+_6 1} & 4 & \xrightarrow{+_6 1} & 5 & \xrightarrow{+_6 1} & 0 \\
h: & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 & 3 & \xrightarrow{\cdot_7 3} & 2 & \xrightarrow{\cdot_7 3} & 6 & \xrightarrow{\cdot_7 3} & 4 & \xrightarrow{\cdot_7 3} & 5 & \xrightarrow{\cdot_7 3} & 1
\end{array}
$$

Seien $S_2 = \{\mathrm{id}, p\}$ mit $\mathrm{id} = (1)(2)$ und $p = (1,2)$, $\leftrightarrow\colon \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ mit $\mathbb{B} = \{0,1\}$ und folgende Verknüpfungstafeln von $(S_2, \circ)$ und $(\mathbb{B}, \leftrightarrow)$ gegeben:

$(S_2, \circ)$:

$\circ$	id	p
id	id	p
p	p	id

$(\mathbb{B}, \leftrightarrow)$:

$\leftrightarrow$	0	1
0	1	0
1	0	1

Wieso sind $(S_2, \circ)$ und $(\mathbb{B}, \leftrightarrow)$ isomorph zueinander?

Überlege dir, wie ein Isomorphismus $h : S_2 \to \mathbb{B}$ aussehen könnte und überprüfe die Homomorphieeigenschaft von h:

$$\begin{aligned} h(\mathrm{id} \circ \mathrm{id}) &= h(\mathrm{id}) \leftrightarrow h(\mathrm{id}) \\ h(\mathrm{id} \circ p) &= h(\mathrm{id}) \leftrightarrow h(p) \\ h(p \circ \mathrm{id}) &= h(p) \leftrightarrow h(\mathrm{id}) \\ h(p \circ p) &= h(p) \leftrightarrow h(p) \end{aligned}$$

Es gibt nur zwei bijektive Funktionen $h : S_2 \to \mathbb{B}$:

$$h(\mathrm{id}) = 0, h(p) = 1 \quad \text{und} \quad h(\mathrm{id}) = 1, h(p) = 0.$$

Weil id und 1 jeweils die neutralen Elemente sind (bzw. p und 0 jeweils die Erzeuger), entscheiden wir uns für die zweite Variante.

Beweis der Homomorphieeigenschaft:

$$\begin{array}{lllllllll}
h(\mathrm{id} \circ \mathrm{id}) & = & h(\mathrm{id}) & = & 1 & = & 0 \leftrightarrow 0 & = & h(\mathrm{id}) \leftrightarrow h(\mathrm{id}) \quad \checkmark \\
h(\mathrm{id} \circ p) & = & h(p) & = & 0 & = & 0 \leftrightarrow 1 & = & h(\mathrm{id}) \leftrightarrow h(p) \quad \checkmark \\
h(p \circ \mathrm{id}) & = & h(p) & = & 0 & = & 1 \leftrightarrow 0 & = & h(p) \leftrightarrow h(\mathrm{id}) \quad \checkmark \\
h(p \circ p) & = & h(\mathrm{id}) & = & 1 & = & 1 \leftrightarrow 1 & = & h(p) \leftrightarrow h(p) \quad \checkmark
\end{array}$$

Info: Wir dürfen hier beispielsweise „$1 = 0 \leftrightarrow 0$“ statt „true $\equiv$ false $\leftrightarrow$ false“ schreiben, weil wir $\leftrightarrow$ als Operation $\leftrightarrow\colon \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ über $\mathbb{B} = \{0, 1\}$ definiert haben.

Sei $\oplus : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ mit $\mathbb{B} = \{0, 1\}$ und folgende Verknüpfungstafeln von $(\mathbb{Z}_2, +_2)$ und $(\mathbb{B}, \oplus)$ gegeben:

$(\mathbb{Z}_2, +_2)$:

$+_2$	0	1
0	0	1
1	1	0

$(\mathbb{B}, \oplus)$:

$\oplus$	0	1
0	0	1
1	1	0

Wieso sind $(\mathbb{Z}_2, +_2)$ und $(\mathbb{B}, \oplus)$ isomorph zueinander?

Überlege dir wieder, analog zur letzten Quizfrage, wie ein Isomorphismus $h : \mathbb{Z}_2 \to \mathbb{B}$ aussehen könnte und überprüfe die Homomorphieeigenschaft von h.

Es gibt nur zwei bijektive Funktionen $h : \mathbb{Z}_2 \to \mathbb{B}$:

$$h(0) = 0, h(1) = 1 \quad \text{und} \quad h(0) = 1, h(1) = 0.$$

Weil 0 und 0 jeweils die neutralen Elemente sind (bzw. 1 und 1 jeweils die Erzeuger), entscheiden wir uns für die erste Variante.

Beweis der Homomorphieeigenschaft:

$$\begin{array}{lllllllll}
h(0 +_2 0) & = & h(0) & = & 0 & = & 0 \oplus 0 & = & h(0) \oplus h(0) \quad \checkmark \\
h(0 +_2 1) & = & h(1) & = & 1 & = & 0 \oplus 1 & = & h(0) \oplus h(1) \quad \checkmark \\
h(1 +_2 0) & = & h(1) & = & 1 & = & 1 \oplus 0 & = & h(1) \oplus h(0) \quad \checkmark \\
h(1 +_2 1) & = & h(0) & = & 0 & = & 1 \oplus 1 & = & h(1) \oplus h(1) \quad \checkmark
\end{array}$$

Info: Auch hier dürfen wir beispielsweise „$0 = 0 \oplus 0$“ statt „$\text{false} \equiv \text{false} \oplus \text{false}$“ schreiben, weil wir $\oplus$ als Operation $\oplus : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ über $\mathbb{B} = \{0, 1\}$ definiert haben.

Seien $(G, \circ)$ und $(H, \bullet)$ zwei Gruppen mit folgenden Verknüpfungstafeln:

G :

$\circ$	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

H :

$\bullet$	4	5	6
4	6	4	5
5	4	5	6
6	5	6	4

Es gilt $(G, \circ) \cong (H, \bullet)$. Welche Isomorphismen zwischen $(G, \circ)$ und $(H, \bullet)$ gibt es?

Die Erzeugnistafeln beider Gruppen sind:

$(G, \circ)$:

a	$\langle a \rangle$	$\mathrm{ord}(a)$
1	$\{1, 2, 3\}$	3
2	$\{2, 1, 3\}$	3
3	$\{3\}$	1

$(H, \bullet)$:

a	$\langle a \rangle$	$\mathrm{ord}(a)$
4	$\{4, 6, 5\}$	3
5	$\{5\}$	1
6	$\{6, 4, 5\}$	3

Dies ergibt, analog zum Beispiel auf Folie 1249, folgende Isomorphismen $h_1, h_2 : \{1, 2, 3\} \to \{4, 5, 6\}$:

$$h_1(1) = 4, h_1(2) = 6, h_1(3) = 5 \quad \text{und} \quad h_2(1) = 6, h_2(2) = 4, h_2(3) = 5.$$

Welche Isomorphismen gibt es zwischen $\mathbb{Z}_6$ und $\mathbb{Z}_9^*$?

Die Erzeugnistafeln beider Gruppen sind:

$\mathbb{Z}_6$:

a	$\langle a \rangle$	$\mathrm{ord}(a)$
0	$\{0\}$	1
1	$\{1,2,3,4,5,0\}$	6
2	$\{2,4,0\}$	3
3	$\{3,0\}$	2
4	$\{4,2,0\}$	3
5	$\{5,4,3,2,1,0\}$	6

$\mathbb{Z}_9^*$:

a	$\langle a \rangle$	$\mathrm{ord}(a)$
1	$\{1\}$	1
2	$\{2,4,8,7,5,1\}$	6
4	$\{4,7,1\}$	3
5	$\{5,7,8,4,2,1\}$	6
7	$\{7,4,1\}$	3
8	$\{8,1\}$	2

Dies ergibt, analog zum Beispiel auf Folie 1249, folgende Isomorphismen $h_1, h_2 : \mathbb{Z}_6 \to \mathbb{Z}_9^*$:

$$h_1(0) = 1, h_1(1) = 2, h_1(2) = 4, h_1(3) = 8, h_1(4) = 7, h_1(5) = 5.$$

und

$$h_2(0) = 1, h_2(1) = 5, h_2(2) = 7, h_2(3) = 8, h_2(4) = 4, h_2(5) = 2.$$

Gegeben seien folgende Gruppen:

$$\mathbb{Z}_4, \quad \mathbb{Z}_6, \quad \mathbb{Z}_5^*, \quad \mathbb{Z}_7^*, \quad \mathbb{Z}_8^*, \quad S_3.$$

1. Wie viele Elemente besitzt jede Gruppe?
2. Welche Gruppen sind zyklisch?
3. Welche Gruppen sind isomorph zueinander und welche nicht?

1. Es gilt $\mathbb{Z}_5^* = \{1,2,3,4\}$, $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ und $\mathbb{Z}_8^* = \{1,3,5,7\}$. Daraus folgt:

$$|\mathbb{Z}_4| = 4, \quad |\mathbb{Z}_6| = 6, \quad |\mathbb{Z}_5^*| = 4, \quad |\mathbb{Z}_7^*| = 6, \quad |\mathbb{Z}_8^*| = 4, \quad |S_3| = 3! = 6.$$

2. $\mathbb{Z}_n$ ist für jedes $n \in \mathbb{N}$ zyklisch. S_n ist nur für $n \leq 2$ zyklisch. Für $\mathbb{Z}_5^*$, $\mathbb{Z}_7^*$ und $\mathbb{Z}_8^*$ gilt:

$\mathbb{Z}_5^*$:

a	ord(a)
1	1
2	4
3	4
4	2

$\mathbb{Z}_7^*$:

a	ord(a)
1	1
2	3
3	6
4	3
5	6
6	2

$\mathbb{Z}_8^*$:

a	ord(a)
1	1
3	2
5	2
7	2

Somit sind nur $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_5^*$ und $\mathbb{Z}_7^*$ zyklisch und $\mathbb{Z}_8^*$ und S_3 nicht.

3. Für die Gruppen mit 4 Elementen gilt

$$\mathbb{Z}_4 \cong \mathbb{Z}_5^* \ncong \mathbb{Z}_8^*,$$

da $\mathbb{Z}_4$ und $\mathbb{Z}_5^*$ zyklisch sind und $\mathbb{Z}_8^*$ nicht.

Für die Gruppen mit 6 Elementen gilt:

$$\mathbb{Z}_6 \cong \mathbb{Z}_7^* \ncong S_3,$$

da $\mathbb{Z}_6$ und $\mathbb{Z}_7^*$ zyklisch sind und S_3 nicht.

Keine der 4-elementigen Gruppen ist isomorph zu einer der 6-elementigen Gruppen, weil isomorphe Gruppen gleich viele Elemente besitzen müssen.

Wichtige Aussagen zur Isomoprhie von Gruppen

1. Jede zyklische Gruppe $(G, \circ)$ mit $|G| = \infty$ ist isomorph zu $(\mathbb{Z}, +)$.
2. Jede zyklische Gruppe $(G, \circ)$ mit $|G| = n$ ist isomorph zu $(\mathbb{Z}_n, +_n)$.
3. Zwei zyklische Gruppen mit gleich vielen Elementen sind isomorph zueinander.
4. Alle zyklischen Gruppen sind automatisch auch kommutativ, da $(\mathbb{Z}, +)$ und $(\mathbb{Z}_n, +_n)$ beide abelsch (kommutativ) sind.
5. Sind $(G, \circ)$ und $(H, \bullet)$ zwei isomorphe Gruppen und $h : G \to H$ ein Isomorphismus, dann gilt:

$$\begin{array}{lcl} h(a) = b & \Longrightarrow & \text{ord}(a) = \text{ord}(b), \\ h(a) = b & \Longrightarrow & h(a^{-1}) = b^{-1}, \\ (G, \circ) \text{ abelsch} & \Longrightarrow & (H, \bullet) \text{ abelsch}, \\ (G, \circ) \text{ zyklisch} & \Longrightarrow & (H, \bullet) \text{ zyklisch}. \end{array}$$

Quizfragen

1. Gibt es eine Gruppe mit 724 Elementen?
2. Gibt es eine kommutative Gruppe mit 535 Elementen?
3. Gibt es eine nicht-kommutative Gruppe mit 6 Elementen?
4. Gibt es eine nicht-kommutative Gruppe mit 7 Elementen?
5. Gibt es eine nicht-kommutative Gruppe mit 12 Elementen?
6. Gibt es eine zyklische Gruppe mit 793 Elementen?
7. Gibt es eine nicht-zyklische Gruppe mit 24 Elementen?
8. Gibt es eine zyklische Gruppe, die nicht kommutativ ist?
9. Gibt es nicht-isomorphe Gruppen mit 23 Elementen?
10. Gibt es nicht-isomorphe Gruppen mit 24 Elementen?
11. Gibt es eine Gruppe mit 21 Elementen, die ein Element mit Ordnung 5 enthält?
12. Gibt es eine Gruppe mit 36 Elementen, die eine Untergruppe mit 8 Elementen besitzt?

1. Ja! $\mathbb{Z}_{724}$. Erinnerung: $\mathbb{Z}_n$ ist für alle $n \in \mathbb{N}$ eine Gruppe.
2. Ja! $\mathbb{Z}_{535}$. Erinnerung: $\mathbb{Z}_n$ ist für alle $n \in \mathbb{N}$ eine kommutative Gruppe.
3. Ja! S_3.
4. Nein! 7 ist prim und somit ist jede Gruppe mit 7 Elementen zyklisch und kommutativ.
5. Ja! Das innere Produkt $S_3 \times \mathbb{Z}_2$ besitzt $|S_3 \times \mathbb{Z}_2| = 6 \cdot 2 = 12$ Elemente und ist nicht kommutativ, da S_3 es nicht ist.
6. Ja! $\mathbb{Z}_{793}$. Erinnerung: $\mathbb{Z}_n$ ist für alle $n \in \mathbb{N}$ eine zyklische Gruppe.

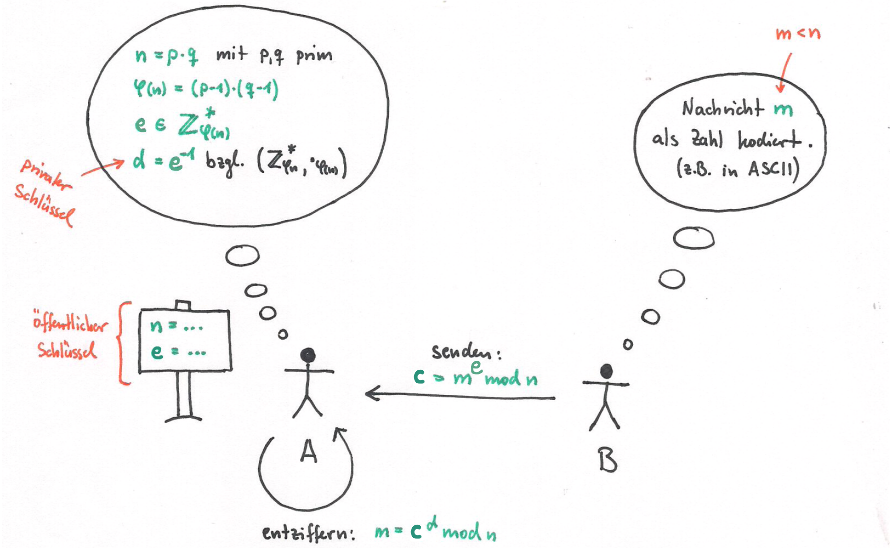
7. Ja! S_4. Erinnerung: S_n besitzt $n!$ Elemente und ist nur für $n \leq 2$ zyklisch und kommutativ. Für $n \geq 3$ ist S_n weder kommutativ noch zyklisch.
8. Nein! Jede Zyklische Gruppe ist kommutativ.
9. Nein! 23 ist prim, d.h. alle Gruppen mit 23 Elementen sind zyklisch und somit isomorph zueinander.
10. Ja! $\mathbb{Z}_{24}$ und S_4 haben beide 24 Elemente, aber sind sind nicht isomorph zueinander, weil $\mathbb{Z}_{24}$ zyklisch ist und S_4 nicht.
11. Nein! 5 teilt nicht die 21.
12. Nein! 8 teilt nicht 36.

Themenübersicht

RSA Kryptoverfahren

Ziel: Bob (B) möchte Alice (A) eine geheime Nachricht m senden.

RSA Kryptoverfahren



Infos

- Die Nachricht m (engl. *message*) stellt in der Regel ein einziges Zeichen dar, welches als Zahl kodiert wurde (z.B. mit ASCII, ANSI, Unicode oder UTF-8).
- Die verschlüsselte Nachricht c (engl. *cypher text*) wird Geheimtext oder Chiffrat genannt.
- (n, e) ist der öffentliche Schlüssel von Alice.
- d ist der private Schlüssel von Alice.
- $f_e : \mathbb{Z}_n \to \mathbb{Z}_n$ mit $f_e(x) = x^e \bmod n$ ist die Verschlüsselungsfunktion.
- $f_d : \mathbb{Z}_n \to \mathbb{Z}_n$ mit $f_d(x) = x^d \bmod n$ ist die Entschlüsselungsfunktion.
- e und d heißen auf Englisch *encryption key* und *decryption key*.

Infos

- Die Werte von n und e stehen Alice, Bob und allen anderen Gesprächsteilnehmern zur Verfügung.
- Wer die Primfaktoren p und q von n kennt, kann sehr leicht $\varphi(n) = (p-1)(q-1)$ berechnen. Mit φ und e kommt man mithilfe des erweiterten euklidischen Algorithmus sehr einfach auf d.
- Jeder, der den Wert von d kennt, könnte die Nachrichten entziffern, die an Alice addressiert worden sind.
- Jeder Teilnehmer hat verschiedene Werte für n, e und d. Möchte Alice also auf Bobs Nachricht antworten, so muss sie dafür den öffentlichen Schlüssel von Bob benutzen.
- Dieses Verfahren ist sicher, solange man die Zahl n so gigantisch groß wählt, dass man aus n nicht so einfach auf die Primfaktoren p und q schließen kann.

Beispiel

Sei $(n, e) = (22, 7)$ der öffentliche Schlüssel von Alice und $d = 3$ ihr privater Schlüssel. Bob möchte ihr eine als Zahl $m = 13$ kodierte Nachricht schicken. Folgende Fragen sind wichtig:

1. Ist $n = 22$ zulässig?
2. Ist $e = 7$ zulässig?
3. Ist $d = 3$ zulässig?
4. Wie verschlüsselt Bob seine Nachricht m?
5. Wie entschlüsselt Alice den Geheimtext c?

Beispiel

1. $n = 22$ ist zulässig, weil 22 aus genau zwei Primfaktoren besteht: $p = 2$ und $q = 11$. Es folgt:
$$\varphi(22) = (2-1)(11-1) = 10.$$
2. $e = 7$ ist zulässig, weil 10 und 7 teilerfremd sind. Es gilt also $\mathrm{ggT}(10, 7) = 1$ und somit $7 \in \mathbb{Z}_{10}^*$ (s. nächste Folie).
3. $d = 3$ ist zulässig, weil 3 das multiplikative inverse Element von 7 in $(\mathbb{Z}_{10}^*, \cdot_{10})$ ist (s. nächste Folie).
4. Bob verschlüsselt seine Nachricht $m = 13$ wie folgt:
$$c = m^e \bmod n = 13^7 \bmod 22 = 7.$$
5. Alice entschlüsselt die Nachricht $c = 7$ wie folgt:
$$m = c^d \bmod n = 7^3 \bmod 22 = 13.$$

Beispiel

Für die Beantwortung der Fragen 2. und 3. sind der euklidische Algorithmus und seine Erweiterung hilfreich:

r_i	s_i	t_i
10	-	3
7	1	-2
3	2	1
1	3	0
0	-	-

Dann gilt $10 \cdot (-2) + 7 \cdot 3 = 1$ und daher

$$7^{-1} = 3 \bmod 10 = 3.$$

Quizfrage

Alice benutzt den öffentlichen Schlüssel $(n, e) = (85, 43)$ und empfängt von Bob den Geheimtext $c = 5$.

Was war die ursprüngliche Nachricht m?

85 enthält die Primfaktoren $p = 5$ und $q = 17$. Daraus folgt:

$$\varphi(85) = (5-1)(17-1) = 4 \cdot 16 = 64.$$

Wir benutzen den erweiterten euklidischen Algorithmus, um den privaten Schlüssel $d = e^{-1}$ zu bestimmen:

r_i	s_i	t_i
64	-	3
43	1	-2
21	2	1
1	21	0
0	-	-

Das inverse Element zu $e = 43$ ist somit $d = 3 \bmod 64 = 3$ und die ursprüngliche Nachricht lautet: $m = c^d \bmod n = 5^3 \bmod 85 = 125 \bmod 85 = 40$.

Eindeutigkeit der Verschlüsselung

Die Verschlüsselungsfunktion f_e ist bijektiv und somit eine Permutation über $\mathbb{Z}_n$. Dies ist sehr wichtig für das Verfahren, denn nur so kann eine Entschlüsselungsfunktion f_d mit $f_d = f_e^{-1}$ überhaupt existieren. Wäre f_e nicht bijektiv, dann wäre die Entschlüsselung m einer verschlüsselten Nachricht c nicht eindeutig.

Beispiel (nochmal)

Sei $(22, 7)$ wieder der öffentliche Schlüssel von Alice und $d = 3$ ihr privater Schlüssel. Wir wollen überprüfen, dass $f_e(x) = x^e \bmod n$ tatsächlich eine Permutation ist und dass $f_d(x) = x^d \bmod n$ die Umkehrfunktion von f_e ist.

Beispiel (nochmal)

Für $f_e(x) = x^e \bmod n$ erhält man:

$$
\begin{array}{lcrcr}
f(0) & = & 0^7 \bmod 22 & = & 0 \\
f(1) & = & 1^7 \bmod 22 & = & 1 \\
f(2) & = & 2^7 \bmod 22 & = & 18 \\
f(3) & = & 3^7 \bmod 22 & = & 9 \\
f(4) & = & 4^7 \bmod 22 & = & 16 \\
f(5) & = & 5^7 \bmod 22 & = & 3 \\
f(6) & = & 6^7 \bmod 22 & = & 8 \\
f(7) & = & 7^7 \bmod 22 & = & 17 \\
f(8) & = & 8^7 \bmod 22 & = & 2 \\
f(9) & = & 9^7 \bmod 22 & = & 15 \\
f(10) & = & 10^7 \bmod 22 & = & 10
\end{array}
\qquad
\begin{array}{lcrcr}
f(11) & = & 11^7 \bmod 22 & = & 11 \\
f(12) & = & 12^7 \bmod 22 & = & 12 \\
f(13) & = & 13^7 \bmod 22 & = & 7 \\
f(14) & = & 14^7 \bmod 22 & = & 20 \\
f(15) & = & 15^7 \bmod 22 & = & 5 \\
f(16) & = & 16^7 \bmod 22 & = & 14 \\
f(17) & = & 17^7 \bmod 22 & = & 19 \\
f(18) & = & 18^7 \bmod 22 & = & 6 \\
f(19) & = & 19^7 \bmod 22 & = & 13 \\
f(20) & = & 20^7 \bmod 22 & = & 4 \\
f(21) & = & 21^7 \bmod 22 & = & 21
\end{array}
$$

Beispiel (nochmal)

Als Permutation:

$$f_e = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 0 & 1 & 18 & 9 & 16 & 3 & 8 & 17 & 2 & 15 & 10 & 11 & 12 & 7 & 20 & 5 & 14 & 19 & 6 & 13 & 4 & 21 \end{pmatrix}$$

Beispiel (nochmal)

Für $f_d(x) = x^d \bmod n$ erhält man:

$$
\begin{array}{lcrcr}
f(0) & = & 0^3 \bmod 22 & = & 0 \\
f(1) & = & 1^3 \bmod 22 & = & 1 \\
f(2) & = & 2^3 \bmod 22 & = & 8 \\
f(3) & = & 3^3 \bmod 22 & = & 5 \\
f(4) & = & 4^3 \bmod 22 & = & 20 \\
f(5) & = & 5^3 \bmod 22 & = & 15 \\
f(6) & = & 6^3 \bmod 22 & = & 18 \\
f(7) & = & 7^3 \bmod 22 & = & 13 \\
f(8) & = & 8^3 \bmod 22 & = & 6 \\
f(9) & = & 9^3 \bmod 22 & = & 3 \\
f(10) & = & 10^3 \bmod 22 & = & 10
\end{array}
\qquad
\begin{array}{lcrcr}
f(11) & = & 11^3 \bmod 22 & = & 11 \\
f(12) & = & 12^3 \bmod 22 & = & 12 \\
f(13) & = & 13^3 \bmod 22 & = & 19 \\
f(14) & = & 14^3 \bmod 22 & = & 16 \\
f(15) & = & 15^3 \bmod 22 & = & 9 \\
f(16) & = & 16^3 \bmod 22 & = & 4 \\
f(17) & = & 17^3 \bmod 22 & = & 7 \\
f(18) & = & 18^3 \bmod 22 & = & 2 \\
f(19) & = & 19^3 \bmod 22 & = & 17 \\
f(20) & = & 20^3 \bmod 22 & = & 15 \\
f(21) & = & 21^3 \bmod 22 & = & 21
\end{array}
$$

Beispiel (nochmal)

Als Permutation:

$$f_d = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 0 & 1 & 8 & 5 & 20 & 15 & 18 & 13 & 6 & 3 & 10 & 11 & 12 & 19 & 16 & 9 & 4 & 7 & 2 & 17 & 14 & 21 \end{pmatrix}$$

Beispiel (nochmal)

f_d ist tatsächlich die Umkehrfunktion von f_e:

$$f_e = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 0 & 1 & 18 & 9 & 16 & 3 & 8 & 17 & 2 & 15 & 10 & 11 & 12 & 7 & 20 & 5 & 14 & 19 & 6 & 13 & 4 & 21 \end{pmatrix}$$

$$f_d = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 0 & 1 & 8 & 5 & 20 & 15 & 18 & 13 & 6 & 3 & 10 & 11 & 12 & 19 & 16 & 9 & 4 & 7 & 2 & 17 & 14 & 21 \end{pmatrix}$$

Themenübersicht

Ringe

Eine Algebra $(A, \oplus, \odot)$ mit zwei Operatoren heißt Ring, falls folgendes gilt:

1. $(A, \oplus)$ ist eine kommutative Gruppe mit neutralem Element $0 \in A$ (additive Gruppe)
2. $(A, \odot)$ ist ein Monoid mit neutralem Element $1 \in A$ (multiplikatives Monoid)
3. $\oplus$ und $\odot$ sind distributiv, d.h. für alle $a, b, c \in A$ gilt:

$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$$
$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

Falls $(A, \odot)$ ein kommutatives Monoid ist, dann nennt man $(A, \oplus, \odot)$ einen kommutativen Ring.

Körper

Eine Algebra $(A, \oplus, \odot)$ mit zwei Operatoren heißt Körper, falls folgendes gilt:

1. $(A, \oplus)$ ist eine kommutative Gruppe mit neutralem Element $0 \in A$ (additive Gruppe)
2. $(A \setminus \{0\}, \odot)$ ist eine kommutative Gruppe mit neutralem Element $1 \in A$ (multiplikative Gruppe)
3. $\oplus$ und $\odot$ sind distributiv, d.h. für alle $a, b, c \in A$ gilt:

$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$$

Info

Weil $\odot$ kommutativ ist, braucht man bei Körpern nur eine Distributivität. Die andere folgt aus ihr ;-)

Hierarchie

Es gilt:

$$(A, \oplus, \odot) \text{ Körper} \implies (A, \oplus, \odot) \text{ Ring} \implies (A, \oplus, \odot) \text{ Algebra}$$

d.h. jeder Körper ist ein Ring und jeder Ring ist eine Algebra.

Infos

- A kann eine beliebige Menge sein, endlich oder unendlich
- $\oplus$ und $\odot$ können beliebige Operatoren sein.
- 0 und 1 sind nicht unbedingt die Zahlen 0 und 1.
- Man nennt die 0 Nullelement und die 1 Einselement.
- $-a$ ist das additive Inverse von a, entsprechend ist a^{-1} das multiplikative Inverse von a.
- Möchte man verdeutlichen, welche Elemente neutrale Elemente sind, dann kann man auch $(A, \oplus, \odot, 0, 1)$ statt $(A, \oplus, \odot)$ schreiben.

Beispiele

- Der bekannteste unendliche Ring ist:

$$(\mathbb{Z}, +, \cdot).$$

- Die bekanntesten unendlichen Körper sind:

$$(\mathbb{Q}, +, \cdot), \quad (\mathbb{R}, +, \cdot), \quad (\mathbb{C}, +, \cdot).$$

Quizfrage

Wieso ist $(\mathbb{Z}, +, \cdot)$ kein Körper?

$(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe, weil nur 1 und -1 multiplikative Inverse besitzen.

Restklassenringe

Für eine beliebige natürliche Zahl $n \in \mathbb{N}$ ist $(\mathbb{Z}_n, +_n, \cdot_n)$ ein kommutativer, endlicher Ring und wird Restklassenring $\mathbb{Z}$ modulo n genannt. Zusätzlich gilt:

$$(\mathbb{Z}_n, +_n, \cdot_n) \text{ ist ein Körper} \iff n \text{ ist prim} .$$

Infos

- Da $(\mathbb{Z}_n^*, \cdot_n)$ für alle $n \in \mathbb{N}$ eine kommutative Gruppe ist und $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$ gilt, falls n prim ist, ist $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ für alle Primzahlen n eine kommutative Gruppe.
- Auch hier ist es üblich, dass man nur $\mathbb{Z}_n$ statt $(\mathbb{Z}_n, +_n, \cdot_n)$ schreibt.

Beispiele

- $(\mathbb{Z}_1, +_1, \cdot_1)$ ist ein kommutativer, endlicher Ring, aber kein Körper, da $\mathbb{Z}_1 \setminus \{0\} = \emptyset$ gilt und jeder Körper mindestens ein Element braucht.

$+_1$	0
0	0

$\cdot_1$	0
0	0

- $(\mathbb{Z}_2, +_2, \cdot_2)$ ist ein endlicher Körper.

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

Beispiele

- $(\mathbb{Z}_3, +_3, \cdot_3)$ ist ein endlicher Körper.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- $(\mathbb{Z}_4, +_4, \cdot_4)$ ist ein kommutativer, endlicher Ring, aber kein Körper.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Beispiele

- $(\mathbb{Z}_5, +_5, \cdot_5)$ ist ein endlicher Körper.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Beispiele

- $(\mathbb{Z}_6, +_6, \cdot_6)$ ist ein kommutativer, endlicher Ring, aber kein Körper.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Gegeben seien folgende endlichen Ringe:

1. $(\mathbb{Z}_7, +_7, \cdot_7)$,
2. $(\mathbb{Z}_9, +_9, \cdot_9)$,
3. $(\mathbb{Z}_{11}, +_{11}, \cdot_{11})$,
4. $(\mathbb{Z}_{13}, +_{13}, \cdot_{13})$,
5. $(\mathbb{Z}_{15}, +_{15}, \cdot_{15})$,
6. $(\mathbb{Z}_{17}, +_{17}, \cdot_{17})$,
7. $(\mathbb{Z}_{19}, +_{19}, \cdot_{19})$,
8. $(\mathbb{Z}_{21}, +_{21}, \cdot_{21})$,
9. $(\mathbb{Z}_{23}, +_{23}, \cdot_{23})$,
10. $(\mathbb{Z}_{1624}, +_{1624}, \cdot_{1624})$.

Welche davon sind auch Körper?

Erinnerung:

$$n \text{ prim} \iff (\mathbb{Z}_n, +_n, \cdot_n) \text{ Körper} .$$

1. Körper.
2. Kein Körper.
3. Körper.
4. Körper.
5. Kein Körper.
6. Körper.
7. Körper.
8. Kein Körper.

9. Körper.
10. Kein Körper.

Nullteiler

Sei $(R, \oplus, \odot)$ ein Ring. Ein Element $x \in R$ mit $x \neq 0$ heißt Nullteiler, falls ein $y \in R$ mit $y \neq 0$ existiert mit:

$$x \odot y = 0$$

Infos

- y ist dann auch ein Nullteiler.
- Falls R keine Nullteiler besitzt, nennt man R nullteilerfrei.

Beispiele

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind nullteilerfrei.
- $(\mathbb{Z}_3, +_3, \cdot_3)$ ist nullteilerfrei.
- $(\mathbb{Z}_4, +_4, \cdot_4)$ besitzt den Nullteiler 2:

$$2 \cdot_2 2 = 0.$$

- Der Körper $(\mathbb{Z}_5, +_5, \cdot_5)$ ist nullteilerfrei.
- Der Ring $(\mathbb{Z}_6, +_6, \cdot_6)$ besitzt die Nullteiler 2, 3 und 4:

$$2 \cdot_6 3 = 0 \qquad 3 \cdot_6 2 = 0 \qquad 3 \cdot_6 4 = 0 \qquad 4 \cdot_6 3 = 0$$

Quizfrage

Ist jeder kommutative, nullteilerfreie Ring ein Körper?

Nö! $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer, nullteilerfreie Ring, aber kein Körper.

Ringe vs. Körper

Für jeden Ring (also auch für jeden Körper) $(R, \oplus, \odot)$ gilt:

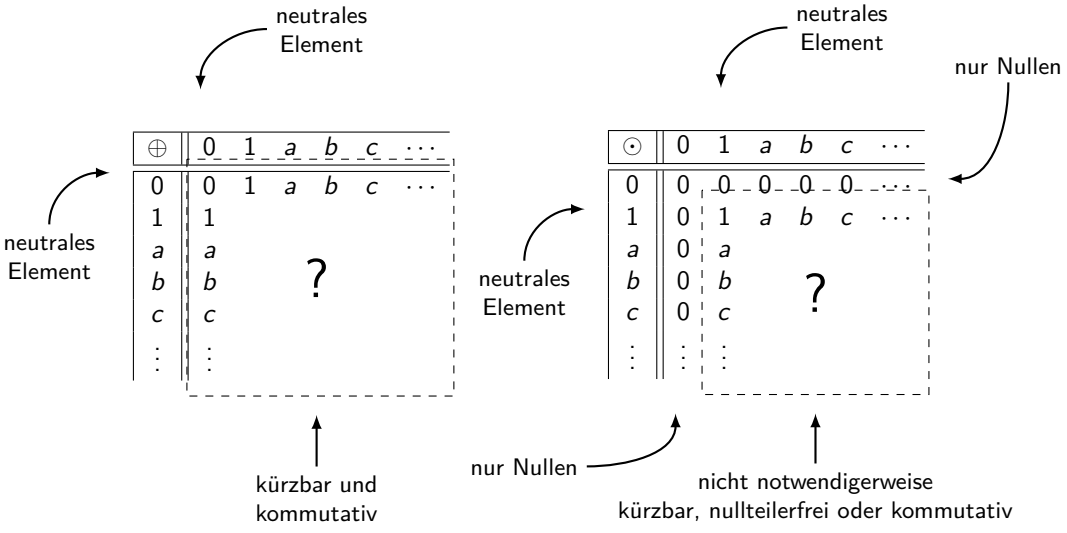
$$\forall a \in R : a \odot 0 = 0 = 0 \odot a$$

Die wesentlichen Unterschiede zwischen Ringen und Körpern sind:

1. Alle Elemente eines Körpers (außer die 0) haben Inverse bzgl. $\odot$, die eines Ringes nur manchmal.
2. $\odot$ ist bei Körpern immer kommutativ, bei Ringen nur manchmal.
3. Körper sind immer nullteilerfrei, Ringe nur manchmal.

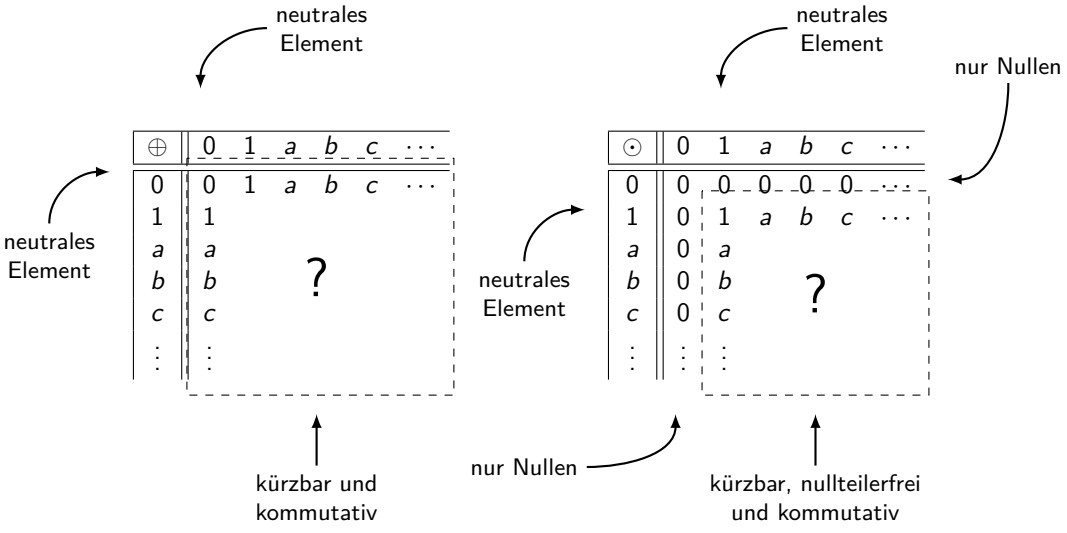
Verknüpfungstafeln von Ringen

Verknüpfungstafeln von Ringen



Verknüpfungstafeln von Körpern

Verknüpfungstafeln von Körpern



Infos

- Bei Algebren mit einem Operator kann man die Assoziativität leider nicht an der Verknüpfungstafel ablesen.
- Bei Algebren mit zwei Operatoren kann man die Distributivitäten leider nicht an den Verknüpfungstafeln ablesen.

D.h. entweder man weiß, dass der Operator (bzw. die Operatoren) assoziativ (bzw. distributiv) sind (z.B. $+$ und $\cdot$ oder $+_n$ und $\cdot_n$) oder man muss es extra beweisen :-(

Monoide vs. Gruppen vs. Ringe vs. Körper

Was kann man in jeder der Strukturen machen?

1. Monoide: addieren
2. Gruppen: addieren und subtrahieren
3. Ringe: addieren, subtrahieren und multiplizieren
4. Körper: addieren, subtrahieren, multiplizieren und dividieren

Deswegen sind Körper so schön zum Rechnen! :-)

Infos

- „subtrahieren “ heißt nichts anderes als „addieren mit dem additiven Inversen“.
- „dividieren“ heißt nichts anderes als „multiplizieren mit dem multiplikativen Inversen“.

Primitive Elemente

Sei $(K, \oplus, \odot)$ ein Körper. Ein Element $a \in K$ heißt primitiv, falls es ein Erzeuger der multiplikativen Gruppe $(K \setminus \{0\}, \odot)$ ist.

Erinnerung

Für jede endliche Gruppe $(G, \circ)$ und jedes $x \in G$ gilt:

$$x \text{ ist Erzeuger von } G \iff \operatorname{ord}(x) = |G| \ .$$

Beispiele

- 2 ist primitiv in $(\mathbb{Z}_3, +_3, \cdot_3)$, da $\text{ord}_{\cdot_3}(2) = 2$.
- 2 und 3 sind primitiv in $(\mathbb{Z}_5, +_5, \cdot_5)$, da $\text{ord}_{\cdot_5}(2) = 4$ und $\text{ord}_{\cdot_5}(3) = 4$.
- 3 und 5 sind primitiv in $(\mathbb{Z}_7, +_7, \cdot_7)$, da $\text{ord}_{\cdot_7}(3) = 6$ und $\text{ord}_{\cdot_7}(5) = 6$.

Isomorphie

Seien $(A, \oplus, \odot)$ und $(B, \boxplus, \boxdot)$ zwei Algebren mit jeweils zwei Operatoren. A und B sind isomorph zueinander, falls folgendes gilt:

- Es gibt eine Funktion $h : A \to B$ mit:

$$\forall x, y \in A : h(x \oplus y) = h(x) \boxplus h(y),$$
$$\forall x, y \in A : h(x \odot y) = h(x) \boxdot h(y),$$

- h ist bijektiv.

Info

Die Isomorphie von Algebren mit zwei Operatoren funktioniert analog zu der von Algebren mit nur einem Operator (s. Folie 1237).

Beispiel

Seien $(A, \oplus, \odot)$ und $(B, \boxplus, \boxdot)$ zwei Algebren mit $A = \{0, 1, 2, 3\}$, $B = \{\clubsuit, \spadesuit, \heartsuit, \diamondsuit\}$ und folgenden Verknüpfungstafeln:

A :

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

B :

$\boxplus$	$\clubsuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$
$\clubsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$
$\spadesuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\diamondsuit$	$\clubsuit$	$\spadesuit$
$\diamondsuit$	$\diamondsuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$

$\boxdot$	$\clubsuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$
$\clubsuit$	$\clubsuit$	$\clubsuit$	$\clubsuit$	$\clubsuit$
$\spadesuit$	$\clubsuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$
$\heartsuit$	$\clubsuit$	$\heartsuit$	$\clubsuit$	$\heartsuit$
$\diamondsuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$

Ein Isomorphismus $h : A \to B$ ist:

$$h(0) = \clubsuit \qquad h(1) = \spadesuit \qquad h(2) = \heartsuit \qquad h(3) = \diamondsuit$$

Themenübersicht

Polynomdivision

Für gegebene Polynome $p, q \in K[x]$ über einem Körper K liefert die Polynomdivision von p durch q eindeutige Polynome r und s mit

$$\frac{p(x)}{q(x)} = s(x) + \frac{r(x)}{q(x)} \qquad (\forall x \in K \setminus q^{-1}(0))$$

und $0 \leq \deg(r) < \deg(q)$.

Erinnerungen

- Körper sind z.B. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ und $\mathbb{Z}_n$ für $n \in \mathbb{P}$ (n prim). Keine Körper sind dagegen $\mathbb{Z}$, $\mathbb{N}$ und $\mathbb{Z}_n$ für $n \notin \mathbb{P}$ (n nicht prim).
- $K[x]$ ist die Menge aller Polynome über K. Beispielsweise gilt für $\mathbb{Z}_2 = \{0, 1\}$:

$$\mathbb{Z}_2[x] = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, \ldots\}$$

- Für eine Funktion $f\colon D \to W$ und ein Element $y \in W$ der Zielmenge ist

$$f^{-1}(y) = \{x \in D \mid f(x) = y\}$$

  Die Urbildmenge von y in f. Entsprechend ist $f^{-1}(0)$ die Menge aller Nullstellen von f. Beispielsweise gilt für $f\colon \mathbb{C} \to \mathbb{C}$ mit $f(x) = x^2 - 1$: $f^{-1}(0) = \{-1, 1\}$.
- Der Grad $\deg(p)$ eines Polynoms p ist der höchste Exponent von x in $p(x)$, z.B.:

$$\deg(3x^4 - 2x^3 + x - 5) = 4.$$

Beispiel

Für $p(x) = 3x^4 - 7x^3 - 6x^2 + 8x - 1$ und $q(x) = x^2 - 3x + 1$ gilt:

$$
\begin{array}{rrrrrcrcl}
(3x^4 & -7x^3 & -6x^2 & +8x & -1) & : & (x^2-3x+1) & = & 3x^2+2x-3. \\
-(3x^4 & -9x^3 & +3x^2) & & & & & & \\
\hline
 & 2x^3 & -9x^2 & +8x & & & & & \\
 & -(2x^3 & -6x^2 & +2x) & & & & & \\
\hline
 & & -3x^2 & +6x & -1 & & & & \\
 & & -(-3x^2 & +9x & -3) & & & & \\
\hline
 & & & -3x & +2 & & & &
\end{array}
$$

Daraus folgt:

$$\frac{3x^4 - 7x^3 - 6x^2 + 8x - 1}{x^2 - 3x + 1} = 3x^2 + 2x - 3 + \frac{-3x + 2}{x^2 - 3x + 1},$$

d.h. $r(x) = -3x + 2$ und $s(x) = 3x^2 + 2x - 3$.

Themenübersicht

Faktorisierung von Polynomen

Analog zur Faktorisierung ganzer Zahlen, wie z.B. in

$$600 = 2^3 \cdot 3 \cdot 5^2,$$

können auch Polynome faktorisiert werden.

Das Ziel der Faktorisierung von Polynomen ist es zu einem gegebenen Polynom $p \in K[x]$ über einem Körper K Polynome $p_1, \ldots, p_n \in K[x]$ zu finden mit

$$p = p_1 \cdot \ldots \cdot p_n.$$

Eine hilfreiche Aussage hierfür ist:

$$\begin{aligned} x_i \text{ ist Nullstelle von } p. &\iff (x - x_i) \text{ ist ein Faktor von } p. \\ &\iff \text{Es gibt ein Polynom } p' \text{ mit } p(x) = (x - x_i) \cdot p'(x). \end{aligned}$$

Das heißt, dass Polynome p_i mit $\deg(p_i) = 1$ sehr leicht abgespaltet werden können, indem man eine Nullstelle x_i von p durch „scharfes Hinschauen“ (d.h. durch Ausprobieren) errät und dann p mit Polynomdivision durch $(x - x_i)$ teilt.

Infos

- Die Faktorisierung von Polynomen über einem Körper ist, wie die Primfaktorzerlegung ganzer Zahlen, eindeutig.
- Für Polynome $p_1, \ldots, p_n$ über einem Ring (z.B. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ und $\mathbb{Z}_n$) gilt immer:

$$\deg(p_1 + \ldots + p_n) \leq \max\{\deg(p_1), \ldots, \deg(p_n)\},$$

$$\deg(p_1 \cdot \ldots \cdot p_n) \leq \deg(p_1) + \ldots + \deg(p_n).$$

- Weil Körper nullteilerfrei sind, gilt für Polynome $p_1, \ldots, p_n$ über einem Körper (z.B. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ und $\mathbb{Z}_n$ für n prim) sogar:

$$\deg(p_1 \cdot \ldots \cdot p_n) = \deg(p_1) + \ldots + \deg(p_n).$$

- Eine Faktorisierung

$$p = p_1 \cdot \ldots \cdot p_n$$

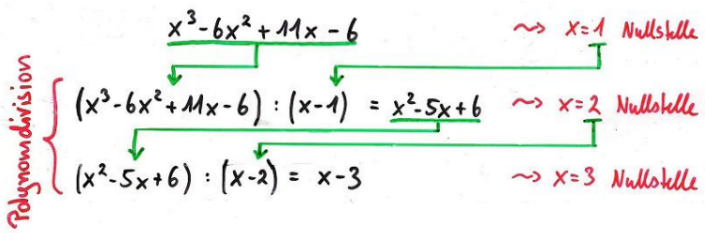
heißt vollständig, falls keines der Polynome $p_1, \ldots, p_n$ sich weiter faktorisieren lässt.

Beispiel

Sei p ein Polynom über $\mathbb{R}$ mit

$$p(x) = 2x^3 - 12x^2 + 22x - 12.$$

Aus $p(x) = 2(x^3 - 6x^2 + 11x - 6)$ und



folgt die vollständige Faktorisierung von p:

$$p(x) = 2(x-1)(x-2)(x-3).$$

Wie sieht die vollständige Faktorisierung der folgenden Polynome p aus?

1. $p(x) = 2x^3 + 10x^2 + 6x - 18$ mit $p \in \mathbb{R}[x]$,
2. $p(x) = 3x^3 + 6x^2 - 3x - 6$ mit $p \in \mathbb{R}[x]$,
3. $p(x) = x^4 - 1$ mit $p \in \mathbb{R}[x]$,
4. $p(x) = x^4 - 1$ mit $p \in \mathbb{C}[x]$.

Antworten

1. $p(x) = 2(x-1)(x+3)^2$.
2. $p(x) = 3(x-1)(x+1)(x+2)$.
3. $p(x) = (x^2+1)(x+1)(x-1)$.
4. $p(x) = (x+i)(x-i)(x+1)(x-1)$.

Themenübersicht

Polynome

Sei $(R, \oplus, \odot)$ ein beliebiger kommutativer Ring (endlich oder unendlich).

- Ein Polynom p über R in der Unbekannten x ist ein Ausdruck der Gestalt

$$p = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

  wobei $a_0, \ldots, a_n \in R$ gilt.
- $\deg(p) = n$ ist der Grad und $a_1, \ldots, a_n$ sind die Koeffizienten von p. Für alle $i > n$ definieren wir $a_i := 0$.
- $R[x]$ ist die Menge aller Polynome mit Koeffizienten aus R.
- Jedes Polynom p induziert eine Funktion $f_p : R \to R$ mit

$$f_p(x) = (a_n \odot x^n) \oplus (a_{n-1} \odot x^{n-1}) \oplus \ldots \oplus (a_1 \odot x) \oplus a_0$$

  für alle $x \in R$.
- Ein Element $x_0 \in R$ mit $f_p(x_0) = 0$ heißt Nullstelle von p.

Infos

- Für ein Polynom p kann man auch $p(x)$ schreiben und für die Unkenannte x auch X.
- In einem Polynom werden Teilasudrücke der Form $1x^i$ durch x^i ersetzt und Teilausdrücke der Form $0x^i$ werden weggelassen.
- Das Polynom $p = 0$ hat per Definition den Grad $\deg(p) = -\infty$.
- $R[x]$ wird „R *adjungiert* x“ gelesen.
- Polynome aus $R[x]$ kann man sich als Wörter über dem Alphabet $\Sigma = R \cup \{+, x, ^2, ^3, ^4, \ldots\}$ vorstellen. Zwei Polynome sind also gleich, wenn sie identisch aussehen.
- Ein Polynom induziert zwar eine Funktion, ist aber selber keine. Insbesondere können zwei verschiedene Polynome dieselbe Funktion induzieren!
- Weil Jeder Körper ein Ring ist, können die Koeffizienten des Polynoms auch aus einem Körper stammen.

Infos

- Polynome könnten auch als Tupel $(a_0, a_1, \ldots, a_d)$ bzw. Folgen $(a_0, a_1, \ldots)$ definiert werden, aber das würde das Rechnen mit ihnen viel weniger intuitiv machen.

Beispiel

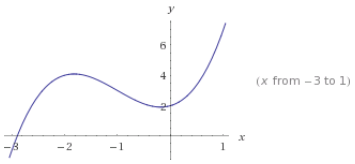
Sei $p \in \mathbb{R}[x]$ ein Polynom über dem Körper $(\mathbb{R}, +, \cdot)$ mit

$$p = x^3 + 3x^2 + x + 2.$$

Für ein beliebiges $x \in \mathbb{R}$ gilt dann:

$$f_p(x) = x^3 + 3 \cdot x^2 + x + 2.$$

Weil f_p in diesem Fall eine Funktion $f_p : \mathbb{R} \to \mathbb{R}$ ist, kann sie als Kurve in einem Koordinatensystem dargestellt werden:



Noch ein Beispiel

Sei $p \in \mathbb{R}[x]$ ein Polynom über dem endlichen Ring $(\mathbb{Z}_6, +_6, \cdot_6)$ mit

$$p = x^3 + 3x^2 + x + 2.$$

Für ein beliebiges $x \in \mathbb{Z}_6$ gilt dann:

$$f_p(x) = x^3 +_6 3 \cdot_6 x^2 +_6 x +_6 2$$

Daraus folgt:

x	0	1	2	3	4	5
$f_p(x)$	2	1	0	5	5	3

Diesmal ist f_p keine Funktion $f_p : \mathbb{R} \to \mathbb{R}$. D.h. sie kann nicht als Kurve in einem Koordinatensystem dargestellt werden!

Quizfrage

Quizfrage

Welche Nullstellen besitzen folgende Polynome aus $\mathbb{Z}_2[x]$?

0	1	x	$x+1$
x^2	x^2+1	x^2+x	x^2+x+1
x^3	x^3+1	x^3+x	x^3+x+1
x^3+x^2	x^3+x^2+1	x^3+x^2+x	x^3+x^2+x+1
x^4	x^4+1	x^4+x	x^4+x+1
x^4+x^2	x^4+x^2+1	x^4+x^2+x	x^4+x^2+x+1
x^4+x^3	x^4+x^3+1	x^4+x^3+x	x^4+x^3+x+1
$x^4+x^3+x^2$	$x^4+x^3+x^2+1$	$x^4+x^3+x^2+x$	$x^4+x^3+x^2+x+1$
x^5	x^5+1	x^5+x	x^5+x+1
x^5+x^2	x^5+x^2+1	x^5+x^2+x	x^5+x^2+x+1
x^5+x^3	x^5+x^3+1	x^5+x^3+x	x^5+x^3+x+1
$x^5+x^3+x^2$	$x^5+x^3+x^2+1$	$x^5+x^3+x^2+x$	$x^5+x^3+x^2+x+1$
x^5+x^4	x^5+x^4+1	x^5+x^4+x	x^5+x^4+x+1
$x^5+x^4+x^2$	$x^5+x^4+x^2+1$	$x^5+x^4+x^2+x$	$x^5+x^4+x^2+x+1$
$x^5+x^4+x^3$	$x^5+x^4+x^3+1$	$x^5+x^4+x^3+x$	$x^5+x^4+x^3+x+1$
$x^5+x^4+x^3+x^2$	$x^5+x^4+x^3+x^2+1$	$x^5+x^4+x^3+x^2+x$	$x^5+x^4+x^3+x^2+x+1$

Antwort

Antwort

Für die Nullstellen (NS) kommen nur Elemente aus $\mathbb{Z}_2$ infrage und es wird in $\mathbb{Z}_2$ gerechnet.

0 (NS: $0, 1$)	1 (NS: $-$)	x (NS: 0)	$x+1$ (NS: 1)
x^2 (NS: 0)	x^2+1 (NS: 1)	x^2+x (NS: 0)	x^2+x+1 (NS: $-$)
x^3 (NS: 0)	x^3+1 (NS: 1)	x^3+x (NS: $0, 1$)	x^3+x+1 (NS: $-$)
x^3+x^2 (NS: $0, 1$)	x^3+x^2+1 (NS: $-$)	x^3+x^2+x (NS: 0)	x^3+x^2+x+1 (NS: 1)
x^4 (NS: 0)	x^4+1 (NS: 1)	x^4+x (NS: $0, 1$)	x^4+x+1 (NS: $-$)
x^4+x^2 (NS: $0, 1$)	x^4+x^2+1 (NS: $-$)	x^4+x^2+x (NS: 0)	x^4+x^2+x+1 (NS: 1)
x^4+x^3 (NS: $0, 1$)	x^4+x^3+1 (NS: $-$)	x^4+x^3+x (NS: 0)	x^4+x^3+x+1 (NS: 1)
$x^4+x^3+x^2$ (NS: 0)	$x^4+x^3+x^2+1$ (NS: 1)	$x^4+x^3+x^2+x$ (NS: $0, 1$)	$x^4+x^3+x^2+x+1$ (NS: $-$)
x^5 (NS: 0)	x^5+1 (NS: 1)	x^5+x (NS: $0, 1$)	x^5+x+1 (NS: $-$)
x^5+x^2 (NS: $0, 1$)	x^5+x^2+1 (NS: $-$)	x^5+x^2+x (NS: 0)	x^5+x^2+x+1 (NS: 1)
x^5+x^3 (NS: $0, 1$)	x^5+x^3+1 (NS: $-$)	x^5+x^3+x (NS: 0)	x^5+x^3+x+1 (NS: 1)
$x^5+x^3+x^2$ (NS: 0)	$x^5+x^3+x^2+1$ (NS: 1)	$x^5+x^3+x^2+x$ (NS: $0, 1$)	$x^5+x^3+x^2+x+1$ (NS: $-$)
x^5+x^4 (NS: $0, 1$)	x^5+x^4+1 (NS: $-$)	x^5+x^4+x (NS: 0)	x^5+x^4+x+1 (NS: 1)
$x^5+x^4+x^2$ (NS: 0)	$x^5+x^4+x^2+1$ (NS: 1)	$x^5+x^4+x^2+x$ (NS: $0, 1$)	$x^5+x^4+x^2+x+1$ (NS: $-$)
$x^5+x^4+x^3$ (NS: 0)	$x^5+x^4+x^3+1$ (NS: 1)	$x^5+x^4+x^3+x$ (NS: $0, 1$)	$x^5+x^4+x^3+x+1$ (NS: $-$)
$x^5+x^4+x^3+x^2$ (NS: $0, 1$)	$x^5+x^4+x^3+x^2+1$ (NS: $-$)	$x^5+x^4+x^3+x^2+x$ (NS: 0)	$x^5+x^4+x^3+x^2+x+1$ (NS: 1)

Polynomaddition

Für zwei Polynome $a, b \in R[x]$ über einem kommutativen Ring $(R, \oplus, \odot)$ mit

$$a = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$
$$b = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

definieren wir:

$$a + b := c_r x^r + c_{r-1} x^{r-1} + \ldots + c_1 x + c_0$$

mit $r = \max(n, m)$ und $c_i := a_i \oplus b_i$ für alle $i = 0, \ldots, r$.

Erinnerung

Wir hatten $a_i = 0$ für $i > n$ und $b_i = 0$ für $i > m$ definiert.

Beispiele

- Seien $a, b \in \mathbb{Z}[x]$ folgende Polynome über dem Ring $(\mathbb{Z}, +, \cdot)$:

$$a = 2x^3 + x^2 - 3x + 3,$$
$$b = -3x^2 + 4x + 2.$$

  Dann gilt: $a + b = 2x^3 - 2x^2 + x + 5$.

- Seien $a, b \in \mathbb{Z}_4[x]$ folgende Polynome über dem Ring $(\mathbb{Z}_4, +_4, \cdot_4)$:

$$a = x^3 + x^2 + 1,$$
$$b = 3x^3 + x^2 + 3x + 2.$$

  Dann gilt: $a + b = 2x^2 + 3x + 3$.

Polynomsubtraktion

Für zwei Polynome $a, b \in R[x]$ über einem kommutativen Ring $(R, \oplus, \odot)$ mit

$$a = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$
$$b = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

definieren wir:

$$a - b := c_r x^r + c_{r-1} x^{r-1} + \ldots + c_1 x + c_0$$

mit $r = \max(n, m)$ und $c_i := a_i \oplus (-b_i)$ für alle $i = 0, \ldots, r$.

Erinnerungen

- $-b_i$ ist das additive Inverse von b_i in $(R, \oplus, \odot)$.
- Wir hatten $a_i = 0$ für $i > n$ und $b_i = 0$ für $i > m$ definiert.

Beispiele

- Seien $a, b \in \mathbb{Z}[x]$ folgende Polynome über dem Ring $(\mathbb{Z}, +, \cdot)$:

$$a = 2x^3 + x^2 - 3x + 3,$$
$$b = -3x^2 + 4x + 2.$$

  Dann gilt: $a - b = 2x^3 + 4x^2 - 7x + 1$.

- Seien $a, b \in \mathbb{Z}_4[x]$ folgende Polynome über dem Ring $(\mathbb{Z}_4, +_4, \cdot_4)$:

$$a = x^3 + x^2 + 1,$$
$$b = 3x^3 + x^2 + 3x + 2.$$

  Dann gilt: $a - b = 2x^3 + x + 3$.

Polynommultiplikation

Für zwei Polynome $a, b \in R[x]$ über einem kommutativen Ring $(R, \oplus, \odot)$ mit

$$a = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$
$$b = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

definieren wir:

$$a \cdot b := c_r x^r + c_{r-1} x^{r-1} + \ldots + c_1 x + c_0$$

mit $r = n + m$ und $c_i = \bigoplus_{j=0}^{i} (a_j \odot b_{i-j})$ für alle $i = 0, \ldots, r$.

Der Ausdruck

$$\bigoplus_{j=0}^{i}(a_j \odot b_{i-j}) = (a_0 \odot b_i) \oplus (a_1 \odot b_{i-1}) \oplus (a_2 \odot b_{i-2}) \oplus \ldots \oplus (a_i \odot b_0)$$

entsteht durch das Ausmultiplizieren, Sortieren und Zusammenfassen der Koeffizienten.

Beispiele

- Seien $a, b \in \mathbb{Z}[x]$ folgende Polynome über dem Ring $(\mathbb{Z}, +, \cdot)$:

$$a = x^2 - 2x + 3,$$
$$b = 3x + 1.$$

  Dann gilt: $a \cdot b = 3x^3 - 5x^2 + 7x + 3$.

- Seien $a, b \in \mathbb{Z}_4[x]$ folgende Polynome über dem Ring $(\mathbb{Z}_4, +_4, \cdot_4)$:

$$a = x^2 + 3x + 2,$$
$$b = 2x + 3.$$

  Dann gilt: $a \cdot b = 2x^3 + x^2 + x + 2$.

Info

Mit Polynomen aus $\mathbb{Z}_n[x]$ rechnet man einfach wie mit Polynomen aus $\mathbb{Z}[x]$, mit dem Unterschied, dass am Schluss alle Koeffizienten modulo n genommen werden. Kein Koeffizient darf negativ oder größer oder gleich n sein!

Polynomdivision

Für gegebene Polynome $a, b \in K[x]$ über einem Körper $(K, \oplus, \odot)$ liefert die Polynomdivision von a durch b eindeutige Polynome r und s, so dass gilt:

$$a = b \cdot s + r \quad \text{und} \quad 0 \leq \deg(r) < \deg(b)$$

Analog zur ganzzahligen Division in $\mathbb{Z}$ definieren wir

$$s := a \div b \quad \text{und} \quad r := a \bmod b$$

Auf diese Weise können wir den Euklidischen Algorithmus und seine Erweiterung auch auf Polynome anwenden!

Beispiel

Seien $a, b \in \mathbb{Q}[x]$ mit $a = 3x^4 - 7x^3 - 6x^2 + 8x - 1$ und $b = x^2 - 3x + 1$:

$$
\begin{array}{rrrrr}
(3x^4 & -7x^3 & -6x^2 & +8x & -1) \\
-(3x^4 & -9x^3 & +3x^2) & & \\
\hline
 & 2x^3 & -9x^2 & +8x & \\
 & -(2x^3 & -6x^2 & +2x) & \\
\hline
 & & -3x^2 & +6x & -1 \\
 & & -(-3x^2 & +9x & -3) \\
\hline
 & & & -3x & +2
\end{array}
\quad : \quad (x^2 - 3x + 1) \quad = \quad 3x^2 + 2x - 3
$$

Es gilt dann $a = b \cdot s + r$ mit:

$$s = 3x^2 + 2x - 3 \quad \text{und} \quad r = -3x + 2.$$

Seien $p, q \in \mathbb{Q}[x]$ zwei Polynome mit $p = x^4 - 7x^2 + 6x$ und $q = x^3 - 8x + 3$.

1. Was ist $\mathrm{ggT}(p, q)$?
2. Für welche Polynome $a, b \in \mathbb{Q}[x]$ gilt die Gleichung $a \cdot q + b \cdot p = \mathrm{ggT}(p, q)$?

Hinweis: Führe den erweiterten Euklidischen Algorithmus mithilfe der Polynomdivision mit p und q durch.

Die Tabelle des erweiterten Euklidischen Algorithmus sieht wie folgt aus:

r_i	s_i	t_i
$x^4 - 7x^2 + 6x$	$-$	$x^2 - 3x + 1$
$x^3 - 8x + 3$	x	$-x + 3$
$x^2 + 3x$	$x - 3$	1
$x + 3$	x	0
0	$-$	$-$

Daraus folgt:

1. $\mathrm{ggT}(p, q) = x + 3$.
2. $a = x^2 - 3x + 1$, $b = -x + 3$.

Polynomdivision über $\mathbb{Z}_n$

Sei n eine Primzahl, d.h. $\mathbb{Z}_n$ ein Körper. Eine Polynomdivision mit Polynomen über $\mathbb{Z}_n$ (d.h. mit Koeffizienten aus $\mathbb{Z}_n$) funktioniert analog zu einer Polynomdivision über $\mathbb{Q}$ oder $\mathbb{R}$ mit zwei wesentlichen Unterschieden:

- statt Zahlen zu dividieren, multipliziert man mit Inversen
- nach jeder Multiplikation und Subtraktion nimmt man das Ergebnis, falls es nicht in $\mathbb{Z}_n$ ist, modulo p

Beispiel

Seien $a, b \in \mathbb{Z}_5[x]$ mit $a = 3x^4 + x^3 + 3x^2 + 4x + 1$ und $b = 2x^2 + x + 4$.

$$
\begin{array}{rrrrrcll}
(3x^4 & +x^3 & +3x^2 & +4x & +1) & : & (2x^2 + x + 4) & = & 4x^2 + x + 3 \\
-(3x^4 & +4x^3 & +x^2) & & & & & & \\
\hline
 & 2x^3 & +2x^2 & +4x & & & & & \\
 & -(2x^3 & +x^2 & +4x) & & & & & \\
\hline
 & & x^2 & & +1 & & & & \\
 & & -(x^2 & +3x & +2) & & & & \\
\hline
 & & & 2x & +4 & & & &
\end{array}
$$

In $\mathbb{Z}_5$ gilt $2^{-1} = 3$, da $2 \cdot_5 3 = 6 \bmod 5 = 1$. Anstatt also jedesmal durch $2x^2$ zu dividieren multipliziert man (modulo 5) mit $(2x^2)^{-1} = 3x^{-2}$, d.h.:

$$3x^4 \cdot 3x^{-2} = (3 \cdot_5 3)x^2 = 4x^2, \qquad 2x^3 \cdot 3x^{-2} = (2 \cdot_5 3)x = x, \qquad x^2 \cdot 3x^{-2} = 1 \cdot_5 3 = 3.$$

Sei n eine Primzahl und $a, b \in \mathbb{Z}_n[x]$ zwei Polynome über $\mathbb{Z}_n$. Welche Polynome $r, s \in \mathbb{Z}_p[x]$ mit $0 \leq \deg(r) < \deg(b)$ erfüllen für folgende a, b und n die Gleichung $a = b \cdot s + r$?

1. $a = x^3 + 1$, $b = x^2 + x$, $n = 2$,
2. $a = x^3 + x^2 + 1$, $b = x^2 + x + 1$, $n = 2$,
3. $a = x^3 + x^2 + x$, $b = x^2 + 1$, $n = 2$,
4. $a = x^3 + x^2 + 2$, $b = 2x^2 + 1$, $n = 3$,
5. $a = x^3 + x + 2$, $b = x^2 + 2x + 2$, $n = 3$,
6. $a = 2x^3 + 3x + 1$, $b = 3x^2 + x + 2$, $n = 5$,
7. $a = x^3 + 2x^2 + 4$, $b = 4x^2 + 3x + 1$, $n = 5$,
8. $a = 3x^3 + 4x + 5$, $b = 4x^2 + 5x$, $n = 7$.

Hinweis: Benutze Polynomdivision!

1.

$$\begin{array}{rrrrcrrcrr} & (x^3 & & & +1) & : & (x^2 & +x) & = & x & +1 \\ - & (x^3 & +x^2) & & & & & & & & \\ & & x^2 & & +1 & & & & & & \\ & - & (x^2 & +x) & & & & & & & \\ & & & x & +1 & & & & & & \end{array}$$

Daraus folgt: $r = x + 1$ und $s = x + 1$.

2.

$$\begin{array}{rrrrcrrrcr} & (x^3 & +x^2 & & +1) & : & (x^2 & +x & +1) & = & x \\ - & (x^3 & +x^2 & +x) & & & & & & & \\ & & & x & +1 & & & & & & \end{array}$$

Daraus folgt: $r = x + 1$ und $s = x$.

3.

$$\begin{array}{rrrrcrrcrr} & (x^3 & +x^2 & +x &) & : & (x^2 & +1) & = & x & +1 \\ - & (x^3 & & +x) & & & & & & & \\ & & x^2 & & & & & & & & \\ & - & (x^2 & & +1) & & & & & & \\ & & & & 1 & & & & & & \end{array}$$

Daraus folgt: $r = 1$ und $s = x + 1$.

4.

$$\begin{array}{rrrrcrrcrr} & (x^3 & +x^2 & & +2) & : & (2x^2 & +1) & = & 2x & +2 \\ - & (x^3 & & +2x) & & & & & & & \\ & & x^2 & +x & +2 & & & & & & \\ & - & (x^2 & & +2) & & & & & & \\ & & & x & & & & & & & \end{array}$$

Daraus folgt: $r = x$ und $s = 2x + 2$.

5.

$$\begin{array}{rrrrcrrrcrr}
 & (x^3 & & +x & +2) & : & (x^2 & +2x & +2) & = & x & +1 \\
- & (x^3 & +2x^2 & +2x) & & & & & & & & \\
 & & x^2 & 2x & +2 & & & & & & & \\
 & - & (x^2 & +2x & +2) & & & & & & & \\
 & & & & 0 & & & & & & &
\end{array}$$

Daraus folgt: $r = 0$ und $s = x + 1$.

6.

$$\begin{array}{rrrrcrrrcrr}
 & (2x^3 & & +3x & +1) & : & (3x^2 & +x & +2) & = & 4x & +2 \\
- & (2x^3 & +4x^2 & +3x) & & & & & & & & \\
 & & x^2 & & +1 & & & & & & & \\
 & - & (x^2 & +2x & +4) & & & & & & & \\
 & & & 3x & +2 & & & & & & &
\end{array}$$

Daraus folgt: $r = 3x + 2$ und $s = 4x + 2$.

7.

$$\begin{array}{rrrrcrrcl} & (x^3 & +2x^2 & +4) & : & (4x^2 & +3x & +1) & = & 4x \\ - & (x^3 & +2x^2 & +4x) & & & & & & \\ & & & x & +4 & & & & \end{array}$$

Daraus folgt: $r = x + 4$ und $s = 4x$.

8.

$$\begin{array}{rrrrcrrcl} & (3x^3 & & +4x & +5) & : & (4x^2 & +5x) & = & 6x & +3 \\ - & (3x^3 & +2x^2) & & & & & & & & \\ & & (5x^2 & +4x & +5) & & & & & & \\ & - & (5x^2 & +x) & & & & & & & \\ & & & 3x & +5 & & & & & & \end{array}$$

Daraus folgt: $r = 3x + 5$ und $s = 6x + 3$.

Polynomringe

Für jeden kommutativen Ring R bildet $R[x]$ mit der Polynomaddition und -multiplikation aus den Folien 1341 und 1347 wieder einen kommutativen Ring. Polynome können aber auch benutzt werden, um das Konzept von Restklassenringen zu verallgemeinern.

Sei K ein Körper und $p \in K[x]$ ein Polynom mit Grad $\deg(p) = n$. Dann bildet die Menge

$$K[x]_p = \{q \in K[x]\} \deg(q) < \deg(p)$$

aller Polynome aus $K[x]$ mit kleinerem Grad als p zusammen mit den Operationen

$$a +_p b := (a + b) \bmod p \quad \text{und} \quad a \cdot_p b := (a \cdot b) \bmod p.$$

einen kommutativen Ring. Dieser wird Restklassenring $K[x]$ modulo p genannt.

Info

Für jeden endlichen Körper gilt: $|K[x]_p| = |K|^{\deg(p)}$, z.B.: $|\mathbb{Z}_3[x]_{x^4+1}| = 3^4 = 81$

Beispiel

Sei $p \in \mathbb{Z}_2[x]$ mit $p = x^2 + 1$. Dann bildet $\mathbb{Z}_2[x]_p = \{0, 1, x, x+1\}$ mit $+_p$ und $\cdot_p$ einen kommutativen Ring mit folgenden Verknüpfungstafeln:

$+_p$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot_p$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

Es gilt z.B.:

- $(x+1) +_p x = ((x+1) + x) \bmod p = 1$
- $(x+1) \cdot_p x = ((x+1) \cdot x) \bmod p = (x^2 + x) \bmod p = x + 1$

Infos

Man benutzt bei Restklassenringen oft verschiedene Schreibweisen:

- Bei Restklassenringen $\mathbb{Z}$ modulo n schreibt man oft $(\mathbb{Z}/(n), +, \cdot)$ bzw. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ statt $(\mathbb{Z}_n, +_n, \cdot_n)$, weil die zwei Ringe zueinander isomorph sind.
- Bei Restklassenringen $K[x]$ modulo p schreibt man analog auch $(K/(q), +, \cdot)$ oder auch $(K[x]_{\deg(p)}, +_p, \cdot_p)$ statt $(K[x]_p, +_p, \cdot_p)$.

Erinnerung: Isomorphie heißt nicht Gleichheit! Dass zwei Algebren isomorph sind heißt nur, dass sie dieselbe Struktur besitzen. In DS machen wir aber ein Auge zu und dürfen sorglos das eine durch das andere ersetzen ;-)

Welche Elemente sind in folgenden Mengen enthalten?

1. $\mathbb{Z}_2[x]_{x^2+1}$,
2. $\mathbb{Z}_5[x]_{x+4}$,
3. $\mathbb{Z}_2[x]_{x^3+x}$,
4. $\mathbb{Z}_3[x]_{x^2+2}$,
5. $\mathbb{Z}_2[x]_{x^4+x+1}$.

Hinweis: $|\mathbb{Z}_n[x]_p| = |\mathbb{Z}_n|^{\deg(p)} = n^{\deg(p)}$.

1. $\mathbb{Z}_2[x]_{x^2+1} = \{0, 1, x, x+1\}$.
2. $\mathbb{Z}_5[x]_{x+4} = \{0, 1, 2, 3, 4\}$.
3. $\mathbb{Z}_2[x]_{x^3+x} = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.
4. $\mathbb{Z}_3[x]_{x^2+2} = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$.
5. $\mathbb{Z}_2[x]_{x^4+x+1} =$
   $\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1,$

Sei $p = x^2 + 1$ ein Polynom über $\mathbb{Z}_2$ und $R = (\mathbb{Z}_2[x]_p, +_p, \cdot_p)$ ein Restklassenring modulo p.

1. Wie sieht der folgende Ausschnitt der multiplikativen Verknüpfungstafel von R aus?

$\cdot_p$	0	1	x	$x+1$
$x+1$				

2. Woran erkennt man, dass R kein Körper ist?

1. Es gilt:

$\cdot_p$	0	1	x	$x+1$
$x+1$	0	$x+1$	$x+1$	0

2. R ist nicht nullteilerfrei, da $(x+1) \cdot_p (x+1) = 0$. Außerdem gilt die Kürzungsregel nicht, da $(x+1) \cdot_p 1 = (x+1) \cdot_p x$.

Sei $p = x^2 + x$ ein Polynom über $\mathbb{Z}_2$ und $R = (\mathbb{Z}_2[x]_p, +_p, \cdot_p)$ ein Restklassenring.

1. Wie sieht der folgende Ausschnitt der multiplikativen Verknüpfungstafel von R aus?

$\cdot_p$	0	1	x	$x+1$
$x+1$				

2. Woran erkennt man, dass R kein Körper ist?

1. Es gilt:

$\cdot_p$	0	1	x	$x+1$
$x+1$	0	$x+1$	0	$x+1$

2. R ist nicht nullteilerfrei, da $(x+1) \cdot_p x = 0$. Außerdem gilt die Kürzungsregel nicht, da $(x+1) \cdot_p 1 = (x+1) \cdot_p (x+1)$.

Sei $p = 2x^2 + x$ ein Polynom über $\mathbb{Z}_3$ und $R = (\mathbb{Z}_3[x]_p, +_p, \cdot_p)$ ein Restklassenring.

1. Wie sieht der folgende Ausschnitt der multiplikativen Verknüpfungstafel von R aus?

$\cdot_p$	0	1	x	$x+1$
x				

2. Wie sieht der folgende Ausschnitt der multiplikativen Verknüpfungstafel von R aus?

$\cdot_p$	$x+1$	$x+2$
$2x$		
$2x+1$		

3. Woran erkennt man, dass R kein Körper ist?

1. Es gilt:

$\cdot_p$	0	1	x	$x+1$
x	0	x	x	$2x$

2. Es gilt:

$\cdot_p$	$x+1$	$x+2$
$2x$	x	0
$2x+1$	$2x+1$	$x+2$

3. R ist nicht nullteilerfrei, da $2x \cdot_p (x+2) = 0$. Außerdem gilt die Kürzungsregel nicht, da $x \cdot_p 1 = x \cdot_p x$.

Endliche Körper

Wir wissen nun, dass $(\mathbb{Z}_n[x]_p, +_p, \cdot_p)$ für jede natürliche Zahl $n \in \mathbb{N}$ und jedes Polynom $p \in \mathbb{Z}_n[x]$ mit Grad $\deg(p) = d$ ein kommutativer endlicher Ring mit n^d Elementen ist.

Zusätzlich gilt:

$$(\mathbb{Z}_n[x]_p, +_p, \cdot_p) \text{ ist ein Körper} \iff p \text{ ist irreduzibel und } n \text{ prim} .$$

Man nennt solche Körper Galois-Körper (engl. *Galois Field*) und bezeichnet sie mit $\mathrm{GF}(n^d)$.

Beispiel

Sei $p = x^2 + x + 1$ ein Polynom aus $\mathbb{Z}_2[x]$. Da p keine Nullstellen in $\mathbb{Z}_2$ besitzt, ist es irreduzibel. $\mathbb{Z}_2[x]_2 = \{0, 1, x, x+1\}$ bildet also mit $+_p$ und $\cdot_p$ einen Galois-Körper mit folgenden Verknüpfungstafeln:

$+_p$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot_p$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Es gilt z.B.:

- $(x+1) +_p x = ((x+1) + x) \bmod p = 1$
- $(x+1) \cdot_p x = ((x+1) \cdot x) \bmod p = (x^2 + x) \bmod p = 1$

1. Ist $(\mathbb{Z}_3[x]_p, +_p, \cdot_p)$ mit $p = x^4 + x^2 + 1$ ein Körper?
2. Ist $(\mathbb{Z}_9[x]_p, +_p, \cdot_p)$ mit $p = 8x^2 + 3x + 6$ ein Körper?
3. Ist $(\mathbb{Z}_3[x]_p, +_p, \cdot_p)$ mit $p = 2x^2 + 2$ ein Körper?
4. Ist $(\mathbb{Z}_4[x]_p, +_p, \cdot_p)$ mit $p = x^2 + x + 3$ ein Körper?
5. Ist $(\mathbb{Z}_3[x]_p, +_p, \cdot_p)$ mit $p = x^3 + 2x + 1$ ein Körper?
6. Ist $(\mathbb{Z}_2[x]_p, +_p, \cdot_p)$ mit $p = x^3 + x + 1$ ein Körper?
7. Ist $(\mathbb{Z}_6[x]_p, +_p, \cdot_p)$ mit $p = x^2 + 3x + 2$ ein Körper?
8. Ist $(\mathbb{Z}_2[x]_p, +_p, \cdot_p)$ mit $p = x^3 + x^2 + x + 1$ ein Körper?

Erinnerung: Damit $(\mathbb{Z}_n[x]_p, +_p, \cdot_p)$ ein Körper ist, müssen n prim und p irreduzibel sein.

1. Nein! p ist reduzibel, weil es die Nullstelle 2 besitzt.
2. Nein! 9 ist nicht prim.
3. Ja!
4. Nein! 4 ist nicht prim.
5. Ja!
6. Ja!
7. Nein! 6 ist nicht prim.
8. Nein! p ist reduzibel, weil es die Nullstelle 1 besitzt.

Infos

- Eine natürliche Zahl k für die natürliche Zahlen $d, n \in \mathbb{N}$ mit n prim und $k = n^d$ existieren, nennt man eine Primzahlpotenz.
- Für jede Primzahlpotenz n^d prim gibt es einen Galois-Körper $\mathrm{GF}(n^d)$ mit n^d Elementen.
- Alle endlichen Körper sind Galois-Körper und je zwei Galois-Körper mit gleich vielen Elementen sind isomorph zueinander
- Die Körper der Form $(\mathbb{Z}_n, +_n, \cdot_n)$ sind Spezialfälle der Körper $(\mathbb{Z}_n[x]_p, +_p, \cdot_p)$ für $\deg(p) = 1$.
- Falls $\deg(p) = 0$, dann gilt $\mathbb{Z}_n[x]_p = \{0\}$, da 0 das einzige Polynom mit negativem Grad ist (s. Folie 1333).
- Wäre $p = p_1 \cdot p_2$ reduzibel, dann sind alle Polynome, die p_1 oder p_2 als Faktor besitzen, Nullteiler in $(\mathbb{Z}_n[x]_p, +_p, \cdot_p)$.

Quizfragen

1. Gibt es einen Körper mit 5 Elementen?
2. Gibt es einen Körper mit 8 Elementen?
3. Gibt es einen Körper mit 9 Elementen?
4. Gibt es einen Körper mit 15 Elementen?
5. Gibt es einen Körper mit 21 Elementen?
6. Gibt es einen Körper mit 27 Elementen?
7. Gibt es einen Körper mit 32 Elementen?
8. Gibt es einen Körper mit 48 Elementen?
9. Gibt es einen Körper mit 100 Elementen?
10. Gibt es einen Körper mit 121 Elementen?
11. Gibt es einen Körper mit 124 Elementen?

Quizfragen

1. Ja! 5 ist eine Primzahl und somit eine Primzahlpotenz: $5 = 5^1$.
2. Ja! 8 ist eine Primzahlpotenz: $8 = 2^3$.
3. Ja! 9 ist eine Primzahlpotenz: $9 = 3^2$.
4. Nein! 15 ist keine Primzahlpotenz: $15 = 3 \cdot 5$.
5. Nein! 21 ist keine Primzahlpotenz: $21 = 3 \cdot 7$.
6. Ja! 27 ist eine Primzahlpotenz: $27 = 3^3$.
7. Ja! 32 ist eine Primzahlpotenz: $32 = 2^5$.
8. Nein! 48 ist keine Primzahlpotenz: $48 = 3 \cdot 2^4$.
9. Nein! 100 ist keine Primzahlpotenz: $100 = 2^2 \cdot 5^2$.
10. Ja! 121 ist eine Primzahlpotenz: $121 = 11^2$.
11. Nein! 124 ist keine Primzahlpotenz: $124 = 2^2 \cdot 31$.

Quizfragen

1. Ist GF(11) isomorph zu $(\mathbb{Z}_{11}, +_{11}, \cdot_{11})$?
2. Ist GF(27) isomorph zu $(\mathbb{Z}_{27}, +_{27}, \cdot_{27})$?
3. Ist GF(13) isomorph zu $(\mathbb{Z}_{13}, +_{13}, \cdot_{13})$?
4. Ist GF(9) isomorph zu $(\mathbb{Z}_{9}, +_{9}, \cdot_{9})$?
5. Ist GF(5) isomorph zu $(\mathbb{Z}_{5}, +_{5}, \cdot_{5})$?
6. Ist GF(16) isomorph zu $(\mathbb{Z}_{16}, +_{16}, \cdot_{16})$?
7. Ist GF(7) isomorph zu $(\mathbb{Z}_{7}, +_{7}, \cdot_{7})$?
8. Ist GF(25) isomorph zu $(\mathbb{Z}_{25}, +_{25}, \cdot_{25})$?

Antworten

GF(n) ist für jede Primzahlpotenz n ein Körper und ist ansonsten nicht definiert. GF(n) ist isomorph zu $(\mathbb{Z}_n, +_n, \cdot_n)$ genau dann, wenn n prim ist. Wenn n keine Primzahl ist, dann ist $(\mathbb{Z}_n, +_n, \cdot_n)$ kein Körper und kann demnach nicht isomorph zu GF(n) sein.

1. Ja! 11 ist prim.
2. Nein! $27 = 3^3$ ist nicht prim.
3. Ja! 13 ist prim.
4. Nein! $9 = 3^2$ ist nicht prim.
5. Ja! 5 ist prim.
6. Nein! $16 = 2^4$ ist nicht prim.
7. Ja! 7 ist prim.
8. Nein! $25 = 5^2$ ist nicht prim.

Sei $p \in \mathbb{Z}_5[x]$ ein Polynom mit $p = x^3 + 4x^2 + 3x + 2$.

1. Wie viele Elemente enthält $\mathbb{Z}_5[x]_p$?
2. Wie sieht die eindeutige Faktorisierung von p aus?
3. Welche der folgenden Polynomen $a, b, c \in \mathbb{Z}_5[x]$ sind Nullteiler in $(\mathbb{Z}_5[x]_p, +_p, \cdot_p)$?

$$a = 2x^2 + 1,$$
$$b = x^2 + 3x + 2,$$
$$c = x^2 + x + 3.$$

1. $|\mathbb{Z}_5[x]_3| = 5^3 = 125$.
2. Nullstelle 1 raten und p durch $(x+4)$ dividieren ($x - 1 = x + 4$ in $\mathbb{Z}_5$). Wir erhalten $p : (x+4) = x^2 + 3$, was nicht weiter faktorisierbar ist, weil es keine Nullstellen besitzt. Es folgt:
$$p = (x+4)(x^2+3).$$
3. Es gilt:
$$\begin{aligned} a &= 2x^2 + 1 = 2(x^2+3), \\ b &= x^2 + 3x + 2 = (x+1)(x+2), \\ c &= x^2 + x + 3 = (x+2)(x+4). \end{aligned}$$
Die Polynome a und c haben einen gemeinsamen Faktor mit p und sind somit Nullteiler in $(\mathbb{Z}_5[x]_p, +_p, \cdot_p)$.

Charakteristik

Die Charakteristik $\text{char}(K)$ eines Körpers $K = (S, \oplus, \odot)$ ist die additive Ordnung des multiplikativen neutralen Elements:

$$\text{char}(K) := \text{ord}_{\oplus}(1).$$

Die Charakteristik eines endlichen Körpers ist immer eine Primzahl!

Info

Die Notation „$\mathrm{ord}_{\oplus}$“ dient dazu, die Ordnung eines Elements in $(S, \oplus)$ von der in $(S \setminus \{0\}, \odot)$ zu unterscheiden. Beispielsweise gilt:

- $\mathrm{ord}_{\oplus}(0) = 1$, da 0 das neutrale Element bezüglich $\oplus$ ist,
- $\mathrm{ord}_{\odot}(1) = 1$, da 1 das neutrale Element bezüglich $\odot$ ist, und
- $\mathrm{ord}_{\odot}(0) = \infty$, weil kein $n \in \mathbb{N}$ mit $0^n = 1$ existiert (s. Folie 1108).

Beispiele

Seien $d, n \in \mathbb{N}$ mit n prim.

- Die Charakteristik von $(\mathbb{Z}_n, +_n, \cdot_n)$ ist n.
- Die Charakteristik von $\mathrm{GF}(n^d)$ ist ebenfalls n.

Welche Charakteristik besitzen folgende Körper?

1. GF(4).
2. GF(9).
3. GF(25).
4. GF(8).
5. GF(27).
6. GF(7).
7. GF(3).
8. GF(16).
9. GF(5).
10. GF(32).

11. GF(2).

Quizfragen

1. $\mathrm{char}(\mathrm{GF}(4)) = \mathrm{char}(\mathrm{GF}(2^2)) = 2$.
2. $\mathrm{char}(\mathrm{GF}(9)) = \mathrm{char}(\mathrm{GF}(3^2)) = 3$.
3. $\mathrm{char}(\mathrm{GF}(25)) = \mathrm{char}(\mathrm{GF}(5^2)) = 5$.
4. $\mathrm{char}(\mathrm{GF}(8)) = \mathrm{char}(\mathrm{GF}(2^3)) = 2$.
5. $\mathrm{char}(\mathrm{GF}(27)) = \mathrm{char}(\mathrm{GF}(3^3)) = 3$.
6. $\mathrm{char}(\mathrm{GF}(7)) = \mathrm{char}(\mathrm{GF}(7^1)) = 7$.
7. $\mathrm{char}(\mathrm{GF}(3)) = \mathrm{char}(\mathrm{GF}(3^1)) = 3$.
8. $\mathrm{char}(\mathrm{GF}(16)) = \mathrm{char}(\mathrm{GF}(2^4)) = 2$.
9. $\mathrm{char}(\mathrm{GF}(5)) = \mathrm{char}(\mathrm{GF}(5^1)) = 5$.
10. $\mathrm{char}(\mathrm{GF}(32)) = \mathrm{char}(\mathrm{GF}(2^5)) = 2$.
11. $\mathrm{char}(\mathrm{GF}(2)) = \mathrm{char}(\mathrm{GF}(2^1)) = 2$.

Themenübersicht

Irreduzibilität von Polynomen

Sei K ein Körper. Ein Polynom $p \in K[x]$ heißt reduzibel wenn zwei Polynome $p_1, p_2 \in K[x]$ existieren mit $\deg(p_1), \deg(p_2) \geq 1$ und $p = p_1 \cdot p_2$. Polynome, die nicht reduzibel sind, nennt man irreduzibel.

Info

Die Irreduzibilität von Polynomen ist das Analogon zur Primheit von Zahlen.

Beispiel

Das Polynom $p = x^2 + 1$ ist irreduzibel über $\mathbb{R}$, $\mathbb{Q}$ oder $\mathbb{Z}_3$, da keine Polynome aus $\mathbb{R}[x]$, $\mathbb{Q}[x]$ oder $\mathbb{Z}_3[x]$ existieren in denen sich p zerlegen lässt. Dagegen lässt sich p über andere Körper zerlegen, z.B.:

- Falls $p \in \mathbb{C}[x]$:
$$(x + i)(x - i) = x^2 - i^2 = x^2 - (-1) = x^2 + 1$$
- Falls $p \in \mathbb{Z}_2[x]$:
$$(x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1$$
- Falls $p \in \mathbb{Z}_5[x]$:
$$(x + 2)(x + 3) = x^2 + 5x + 6 = x^2 + 1$$

Quizfrage

Sei K ein Körper. Wieso sind Polynome $p \in K[x]$ mit Grad 0 oder 1 immer irreduzibel?

Aus

$$\deg(p_1 \cdot p_2) = \deg(p_1) + \deg(p_2)$$

(s. Folie 1326), können keine zwei Polynome $p_1, p_2 \in K[x]$ mit $\deg(p_1), \deg(p_2) \geq 1$ gefunden werden mit $p = p_1 \cdot p_2$.

Quizfrage

Sei K ein Körper. Wieso sind Polynome $p \in K[x]$ mit Grad 2 oder 3 genau dann irreduzibel, wenn sie keine Nullstellen besitzen?

Antwort

Aus Folie 1326 wissen wir:

$$\deg(p_1 \cdot p_2) = \deg(p_1) + \deg(p_2).$$

Außerdem gilt:

- Falls $\deg(p) = 2$, dann kann p nur in zwei Polynome $p_1, p_2 \in K[x]$ zerfallen mit $\deg(p_1), \deg(p_2) = 1$.
- Falls $\deg(p) = 3$, dann kann p nur in zwei Polynome $p_1, p_2 \in K[x]$ zerfallen mit $\deg(p_1) = 1$ und $\deg(p_2) = 2$ oder $\deg(p_1) = 2$ und $\deg(p_2) = 1$.

In beiden Fällen enthält p ein Faktor von Grad 1. Aus

$$x_0 \text{ ist Nullstele von } p \iff (x - x_0) \text{ ist ein Faktor von } p$$

folgt die Aussage.

Quizfrage

Sei K ein Körper. Wieso kann ein Polynom $p \in K[x]$ mit $\deg(p) \geq 4$ reduzibel sein, obwohl es keine Nullstellen besitzt?

p könnte beispielsweise in nullstellenfreie Faktoren $p_1, \ldots, p_n$ mit $\deg(p_1), \ldots, \deg(p_n) \geq 2$ zerfallen. Beispielsweise gilt für $p \in \mathbb{Q}[x]$ mit $p = x^4 + 2x^2 + 1$:

$$p = (x^2 + 1) \cdot (x^2 + 1).$$

Somit ist p reduzibel, obwohl es keine Nullstellen besitzt.

Wichtige Aussagen zur Irreduzibilität von Polynomen

Für alle Polynome $p \in K[x]$ gilt:

1. Falls $\deg(p) = 0$ oder $\deg(p) = 1$, dann ist p immer irreduzibel.
2. Falls $\deg(p) = 2$ oder $\deg(p) = 3$, dann gilt:

$$p \text{ irreduzibel} \iff p \text{ besitzt keine Nullstelle} .$$

3. Falls $\deg(p) \geq 4$, dann gilt:

$$p \text{ irreduzibel} \implies p \text{ besitzt keine Nullstelle} .$$

Welche der folgenden Polynome sind irreduzibel?

1. $x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$,
2. $x^3 + 2x + 2 \in \mathbb{Z}_5[x]$,
3. $x^3 + 2x + 2 \in \mathbb{Z}_3[x]$,
4. $x^3 + x + 1 \in \mathbb{Z}_2[x]$,
5. $x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$,
6. $x^3 + 2x + 1 \in \mathbb{Z}_3[x]$,
7. $x^3 + x^2 + x \in \mathbb{Z}_5[x]$,
8. $x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Antworten

Erinnerung: Ein Polynom von Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstellen hat.

1. Irreduzibel (keine Nullstellen).
2. Reduzibel (Nullstellen: 1 und 3).
3. Irreduzibel (keine Nullstellen).
4. Irreduzibel (keine Nullstellen).
5. Reduzibel (Nullstelle: 1).
6. Irreduzibel (keine Nullstellen).
7. Reduzibel (Nullstelle: 0).
8. Irreduzibel (keine Nullstellen).

Aus der Quizfrage auf Folie 1337 wissen wir, dass folgende Polynome $p \in \mathbb{Z}_2[x]$, die einzigen mit $2 \leq \deg(p) \leq 5$ sind, die keine Nullstellen besitzen:

Grad 2:	$x^2 + x + 1$,			
Grad 3:	$x^3 + x + 1$,	$x^3 + x^2 + 1$,		
Grad 4:	$x^4 + x + 1$,	$x^4 + x^2 + 1$,	$x^4 + x^3 + 1$,	
Grad 5:	$x^5 + x + 1$,	$x^5 + x^2 + 1$,	$x^5 + x^3 + 1$.	$x^5 + x^4 + 1$

Welche davon sind irreduzibel?

$x^2 + x + 1$, $x^3 + x + 1$ und $x^3 + x^2 + 1$ sind alle irreduzibel, weil sie Grad 2 oder 3 haben und keine Nullstellen besitzen.

Damit ein Polynom von Grad 4 reduzibel ist, obwohl es keine Nullstellen besitzt, muss es in zwei nullstellenfreie Polynome von jeweils Grad 2 zerfallen. Die einzige Kombination hierfür ist:

$$(x^2 + x + 1) \cdot (x^2 + x + 1) = x^4 + x^2 + 1.$$

D.h., dass $x^4 + x^2 + 1$ reduzibel ist und $x^4 + x + 1$ und $x^4 + x^3 + 1$ irreduzibel.

(Fortsetzung)

Damit ein Polynom von Grad 5 reduzibel ist, obwohl es keine Nullstellen besitzt, muss es in zwei nullstellenfreie Polynome mit Graden 2 und 3 zerfallen. Die einzigen Kombinationen hierfür sind:

$$(x^2 + x + 1) \cdot (x^3 + x + 1) = x^5 + x^4 + 1,$$
$$(x^2 + x + 1) \cdot (x^3 + x^2 + 1) = x^5 + x + 1.$$

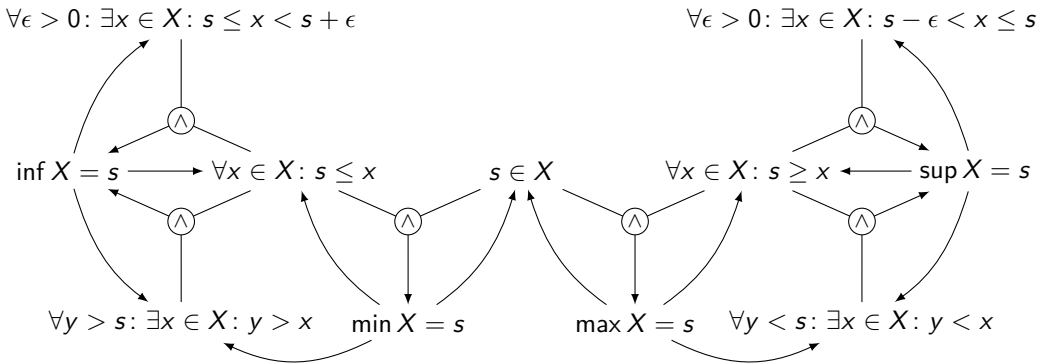
D.h., dass $x^5 + x^4 + 1$ und $x^5 + x + 1$ reduzibel sind und $x^5 + x^2 + 1$ und $x^5 + x^3 + 1$ irreduzibel.

Themenübersicht

Themenübersicht

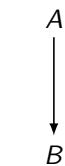
Implikationsgraph für inf, min, sup und max

Für einen angeordneten Körper K, eine nichtleere Teilmenge $X \subset K$ und ein $s \in K$ gelten folgende Implikationen.

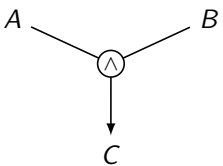


Infos

- Die Pfeile der letzten zwei Implikationsgraphen haben folgende Bedeutungen:



$A \Longrightarrow B$



$(A \wedge B) \Longrightarrow C$

- Als angeordnete Körper kommen bei uns nur $\mathbb{Q}$ und $\mathbb{R}$ infrage!
- Für jede beschränkte Teilmenge $X \subset \mathbb{R}$ gilt $\sup, \inf \in \mathbb{R}$.

Infos

- $\mathbb{Q}$ besitzt beschränkte Teilmengen, die kein Supremum oder Infimum in $\mathbb{Q}$ haben. Beispielsweise besitzt die Menge $\left\{x \in \mathbb{Q} \,\middle|\, x^2 \leq 2\right\}$ kein Supremum in $\mathbb{Q}$, da das Supremum $\sqrt{2}$ nicht in $\mathbb{Q}$ enthalten ist.
- Aus der ϵ-Charakterisierung des Supremums folgt

$$\forall \epsilon > 0 \colon \exists x \in X \colon \sup X - \epsilon < x \leq \sup X$$

für eine nichtleere Teilmenge $X \subset K$ eines angeordneten Körpers K, denn für $s := \sup X$ sind die Bedingungen $\forall x \in X \colon s \geq x$ und $\sup X = s$ trivialerweise erfüllt.

- Analog gilt:

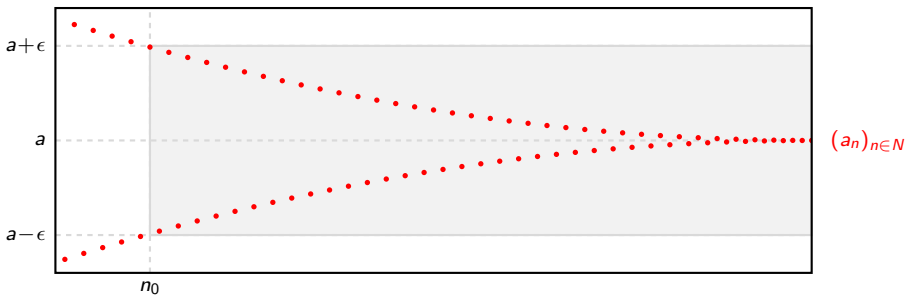
$$\forall \epsilon > 0 \colon \exists x \in X \colon \inf X \leq x < \inf X + \epsilon.$$

Themenübersicht

Grenzwert einer Folge

Eine Folge $(a_n)_{n\in\mathbb{N}}$ hat den Grenzwert $a \in \mathbb{R}$, falls gilt:

$$\forall \epsilon > 0 \colon \exists n_0 \in \mathbb{N} \colon \forall n \geq n_0 \colon \underbrace{|a_n - a| < \epsilon}_{a-\epsilon<a_n<a+\epsilon}$$

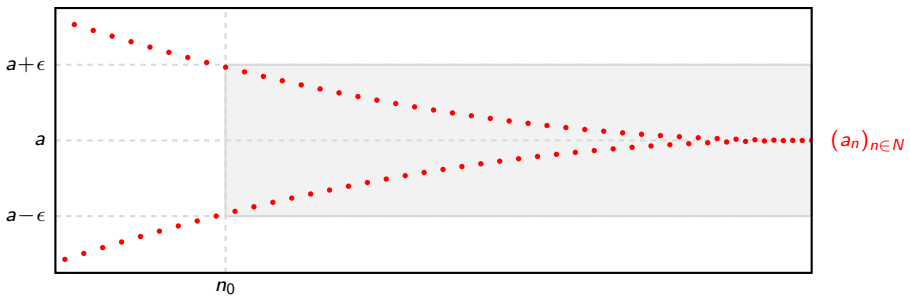


Man schreibt $\lim_{n\to\infty} a_n = a$ oder $a_n \xrightarrow{n\to\infty} a$.

Grenzwert einer Folge

Eine Folge $(a_n)_{n\in\mathbb{N}}$ hat den Grenzwert $a \in \mathbb{R}$, falls gilt:

$$\forall \epsilon > 0 \colon \exists n_0 \in \mathbb{N} \colon \forall n \geq n_0 \colon \underbrace{|a_n - a| < \epsilon}_{a-\epsilon < a_n < a+\epsilon}$$

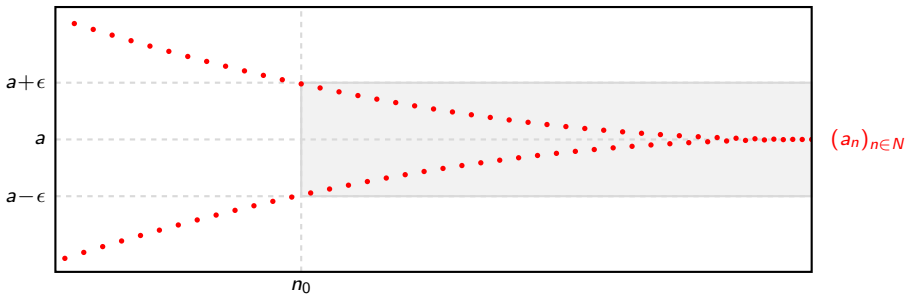


Man schreibt $\lim_{n\to\infty} a_n = a$ oder $a_n \xrightarrow{n\to\infty} a$.

Grenzwert einer Folge

Eine Folge $(a_n)_{n\in\mathbb{N}}$ hat den Grenzwert $a \in \mathbb{R}$, falls gilt:

$$\forall \epsilon > 0 \colon \exists n_0 \in \mathbb{N} \colon \forall n \geq n_0 \colon \underbrace{|a_n - a| < \epsilon}_{a-\epsilon < a_n < a+\epsilon}$$

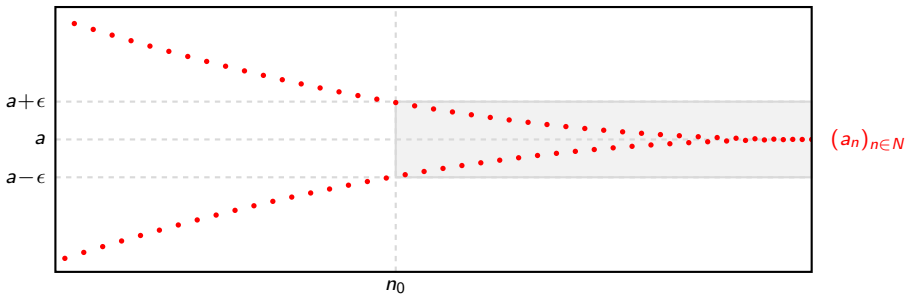


Man schreibt $\lim_{n\to\infty} a_n = a$ oder $a_n \xrightarrow{n\to\infty} a$.

Grenzwert einer Folge

Eine Folge $(a_n)_{n\in\mathbb{N}}$ hat den Grenzwert $a \in \mathbb{R}$, falls gilt:

$$\forall \epsilon > 0 \colon \exists n_0 \in \mathbb{N} \colon \forall n \geq n_0 \colon \underbrace{|a_n - a| < \epsilon}_{a-\epsilon<a_n<a+\epsilon}$$

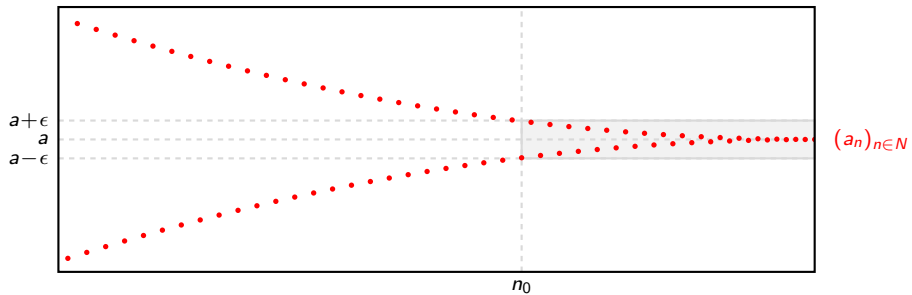


Man schreibt $\lim_{n\to\infty} a_n = a$ oder $a_n \xrightarrow{n\to\infty} a$.

Grenzwert einer Folge

Eine Folge $(a_n)_{n\in\mathbb{N}}$ hat den Grenzwert $a \in \mathbb{R}$, falls gilt:

$$\forall \epsilon > 0 \colon \exists n_0 \in \mathbb{N} \colon \forall n \geq n_0 \colon \underbrace{|a_n - a| < \epsilon}_{a-\epsilon<a_n<a+\epsilon}$$



Man schreibt $\lim_{n\to\infty} a_n = a$ oder $a_n \xrightarrow{n\to\infty} a$.

Beweisen von Konvergenz und Divergenz

Eine Folge, die nicht konvergiert, heißt divergent. Eine *divergente* Folge kann uneigentlich gegen ∞ oder $-\infty$ konvergieren oder auch nicht. Folgende Aussagen helfen bei Beweisen:

1. $(a_n)_{n\in\mathbb{N}}$ konvergiert gegen a ($\lim_{n\to\infty} a_n = a$), falls:

$$\forall \epsilon > 0 \colon \exists n_0 \in \mathbb{N} \colon \forall n \geq n_0 \colon \underbrace{|a_n - a| < \epsilon}_{a-\epsilon<a_n<a+\epsilon}.$$

2. $(a_n)_{n\in\mathbb{N}}$ konvergiert uneigentlich gegen ∞ ($\lim_{n\to\infty} a_n = \infty$), falls:

$$\forall K > 0 \colon \exists n_0 \in \mathbb{N} \colon \forall n \geq n_0 \colon a_n > K.$$

3. $(a_n)_{n\in\mathbb{N}}$ konvergiert uneigentlich gegen $-\infty$ ($\lim_{n\to\infty} a_n = -\infty$), falls:

$$\forall K > 0 \colon \exists n_0 \in \mathbb{N} \colon \forall n \geq n_0 \colon \underbrace{-a_n > K}_{a_n<-K}.$$

Widerlegen von Konvergenz und Divergenz

Durch Negieren der Formeln auf der letzten Folie erhält man:

1. $(a_n)_{n\in\mathbb{N}}$ divergiert, falls:

$$\forall a \in \mathbb{R}\colon \exists \epsilon > 0\colon \forall n_0 \in \mathbb{N}\colon \exists n \geq n_0\colon \underbrace{|a_n - a| \geq \epsilon}_{a_n \leq a-\epsilon \text{ oder } a_n \geq a+\epsilon}.$$

2. $(a_n)_{n\in\mathbb{N}}$ konvergiert nicht uneigentlich gegen ∞, falls:

$$\exists K > 0\colon \forall n_0 \in \mathbb{N}\colon \exists n \geq n_0\colon a_n \leq K.$$

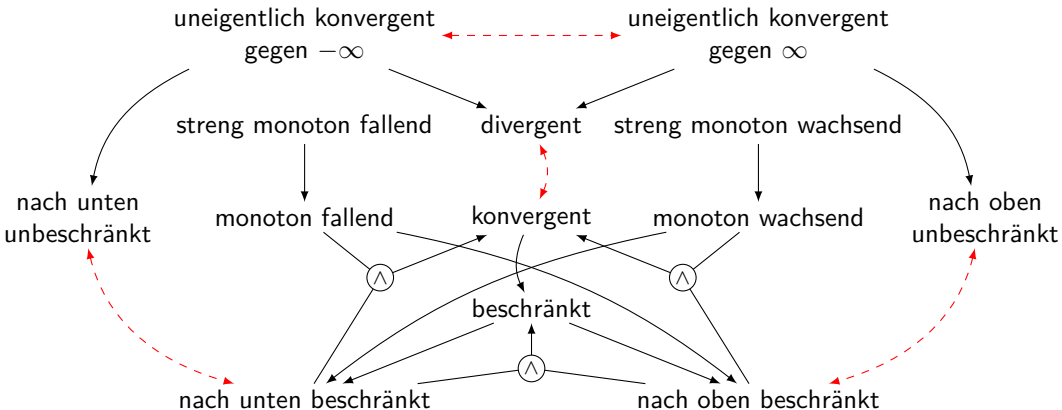
3. $(a_n)_{n\in\mathbb{N}}$ konvergiert nicht uneigentlich gegen $-\infty$, falls:

$$\exists K > 0\colon \forall n_0 \in \mathbb{N}\colon \exists n \geq n_0\colon \underbrace{-a_n < K}_{a_n > -K}.$$

Die Aussagen $\lim_{n\to\infty} a_n = a$, $\lim_{n\to\infty} a_n = \infty$ und $\lim_{n\to\infty} a_n = -\infty$ schließen sich gegenseitig aus, d.h. sobald eine von ihnen gilt kann man davon ausgehen, dass die anderen zwei nicht gelten können.

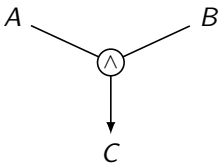
Implikationsgraph für reelle Zahlenfolgen

Für eine beliebige reelle Zahlenfolge $(a_n)_{n\in\mathbb{N}}$ gilt:



Die Pfeile im letzten Implikationsgraph haben folgende Bedeutungen:

$A \Longrightarrow B$



$(A \wedge B) \Longrightarrow C$

$\neg A \vee \neg B$

$\neg A \vee \neg B$ heißt, dass die Aussagen A und B nicht gleichzeitig gelten können, d.h. A und B schließen sich gegenseitig aus.

Themenübersicht

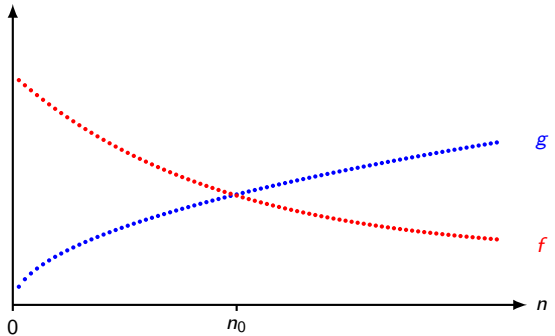
Dominante Funktionen

Seien $f, g : \mathbb{N} \to \mathbb{R}$ beliebige Funktionen. g dominiert f, wenn g an einer bestimmten Stelle f überholt und ab dann immer größer bzw. größer oder gleich f ist. D.h.:

$$\exists n_0 \in \mathbb{N} : \forall n \geq n_0 : f(n) < g(n) \qquad \text{bzw.} \qquad \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : f(n) \leq g(n).$$

Beispiel

f wird von g dominiert.



rot: f, blau: g.

Info

Es gibt auch Funktionen f und g bei denen keine die andere dominiert. Dies passiert z.B. bei Funktionen die „hin- und herschwingen“. Solche Funktionen sind typischerweise

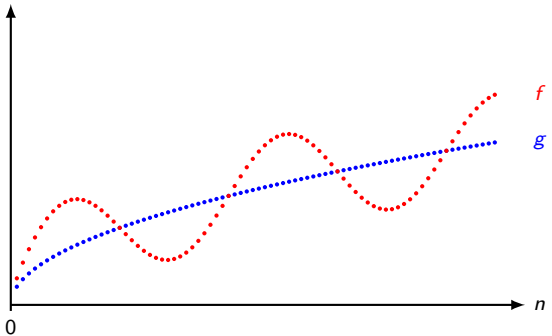
$$f(n) = (-1)^n, \qquad f(n) = \sin(n), \qquad f(n) = \cos(n)$$

oder Funktionen, die etwa so definiert sein könnten:

$$f(n) = \begin{cases} //\ldots, & \text{falls } n \text{ gerade} \\ \ldots, & \text{falls } n \text{ ungerade} \end{cases}$$

Beispiel

Keine der Funktionen f und g dominiert die andere.



rot: f, blau: g.

Konstante Faktoren

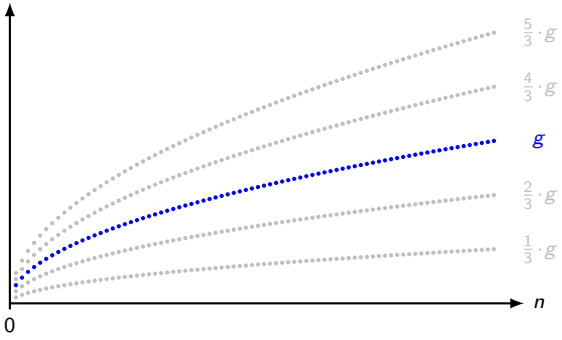
Sei $c \in \mathbb{R}^+$. Die Kurve von $c \cdot g(n)$ ist nichts anderes als die von $g(n)$, aber senkrecht gestreckt (falls $c > 1$) bzw. gestaucht (falls $c < 1$).

Erinnerung

$\mathbb{R}^+ = \{x \in \mathbb{R}\}\, x > 0$ ist die Menge aller positiven reellen Zahlen.

Beispiel

Funktionen g und $c \cdot g$ für $c \in \left\{\frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \frac{5}{3}\right\}$:



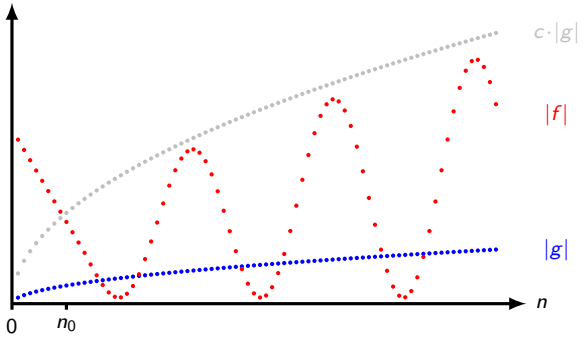
blau: g

Groß-O

Sei $g : \mathbb{N}^{\geq n_0} \to \mathbb{R}$ bzw. $(g_n)_{n \geq n_0}$ eine reelle Folge. $\mathcal{O}(g)$ enthält alle reelle Folgen $(f_n)_{n \geq n_0}$, die von $c \cdot g$ für einige $c \in \mathbb{R}^+$ dominiert werden. D.h.:

$$f \in \mathcal{O}(g) \quad :\iff \quad \exists c > 0 : \exists N \geq n_0 : \forall n \geq N : |f(n)| \leq c \cdot |g(n)| \ .$$

(TODO: considerar escribir las definiciones así)

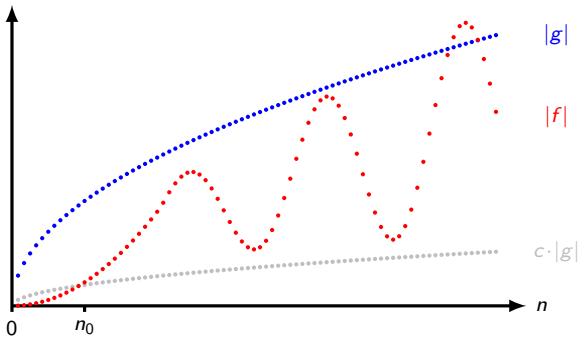


rot: $|f|$, blau: $c \cdot |g|$

Groß-Omega

Sei $g : \mathbb{N} \to \mathbb{R}$ eine beliebige Funktion. $\Omega(g)$ enthält alle Funktionen $f : \mathbb{N} \to \mathbb{R}$, die $c \cdot g(n)$ für einige $c \in \mathbb{R}^+$ dominieren. D.h.:

$$f \in \Omega(g) \quad :\Longleftrightarrow \quad \exists c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| \geq c \cdot |g(n)| \ .$$

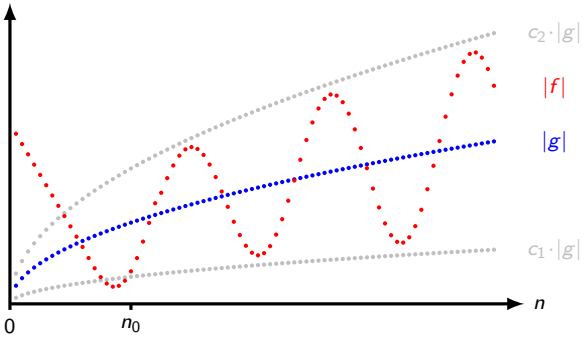


rot: $|f|$, blau: $c \cdot |g|$

Groß-Theta

Sei $g : \mathbb{N} \to \mathbb{R}$ eine beliebige Funktion. $\Theta(g)$ enthält alle Funktionen $f : \mathbb{N} \to \mathbb{R}$, die $c_1 \cdot g(n)$ dominieren und von $c_2 \cdot g(n)$ dominiert werden für einige $c_1, c_2 \in \mathbb{R}^+$. D.h.:

$$f \in \Theta(g) \quad :\Longleftrightarrow \quad \exists c_1, c_2 \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : c_1 \cdot |g(n)| \leq |f(n)| \leq c_2 \cdot |g(n)| \ .$$

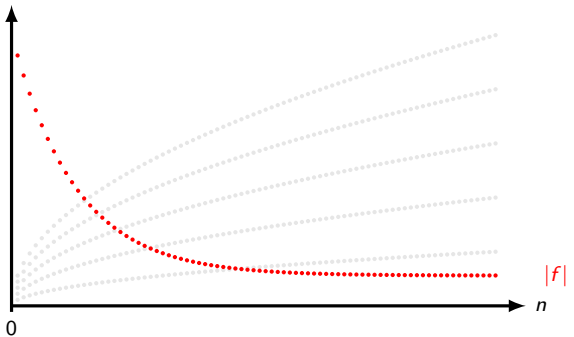


rot: $|f|$, blau: $c_1 \cdot |g|$ und $c_2 \cdot |g|$, grau: $c \cdot |g|$ für verschiedene $c \in \mathbb{R}^+$

Klein-O

Sei $g : \mathbb{N} \to \mathbb{R}$ eine beliebige Funktion. $o(g)$ enthält alle Funktionen $f : \mathbb{N} \to \mathbb{R}$, die von $c \cdot g(n)$ für alle $c \in \mathbb{R}^+$ dominiert werden. D.h.:

$$f \in o(g) \quad :\Longleftrightarrow \quad \forall c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| < c \cdot |g(n)| \ .$$

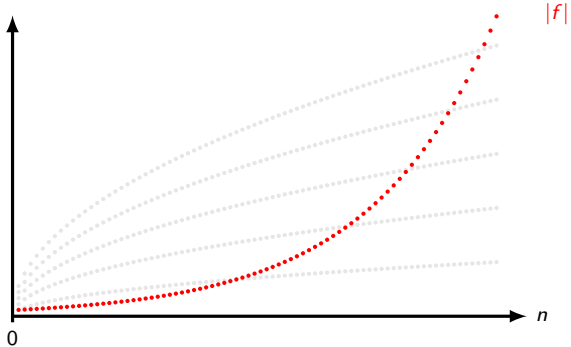


rot: $|f|$, grau: $c \cdot |g|$ für verschiedene $c \in \mathbb{R}^+$

Klein-Omega

Sei $g : \mathbb{N} \to \mathbb{R}$ eine beliebige Funktion. $\omega(g)$ enthält alle Funktionen $f : \mathbb{N} \to \mathbb{R}$, die $c \cdot g(n)$ für alle $c \in \mathbb{R}^+$ dominieren. D.h.:

$$f \in \omega(g) \quad :\Longleftrightarrow \quad \forall c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| > c \cdot |g(n)| \ .$$



rot: $|f|$, grau: $c \cdot |g|$ für verschiedene $c \in \mathbb{R}^+$

Infos

- Statt f und g schreiben wir öfter die Ausdrücke $f(n)$ und $g(n)$, z.B. in $n^2 \in \omega(\sqrt{n})$.
- Es kann auch passieren, dass zwei Funktionen $f(n)$ und $g(n)$ nicht vergleichbar sind!
- Statt

$$f \in o(g), \quad f \in \omega(g), \quad f \in \mathcal{O}(g), \quad f \in \Omega(g), \quad f \in \Theta(g)$$

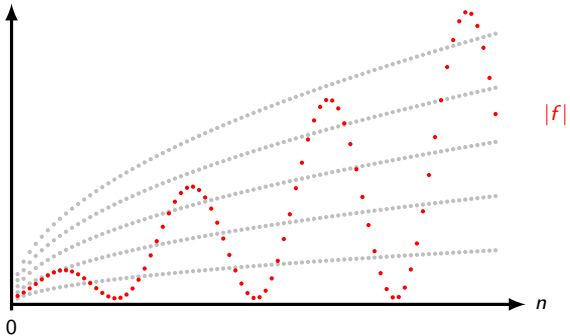
schreibt man leider auch

$$f = o(g), \quad f = \omega(g), \quad f = \mathcal{O}(g), \quad f = \Omega(g), \quad f = \Theta(g),$$

obwohl die zweite Variante formal keinen Sinn macht.

Beispiel

Folgende Funktionen f und g sind nicht vergleichbar.



rot: $|f|$, grau: $c \cdot |g|$ für verschiedene $c \in \mathbb{R}^+$

Quizfrage

$\prec$, $\succ$, $\preceq$, $\succeq$ und $\asymp$ sind homogene Relationen über Funktionen. Welche Eigenschaften besitzen sie?

Hinweis: Die Eigenschaften für diese Relationen zu beweisen kann sehr nervig sein. Versuch die Frage mit Bauchgefühl zu beantworten ;-)

Antwort

- $\prec$ und $\succ$ sind antisymmetrisch, asymmetrisch und transitiv.
- $\preceq$ und $\succeq$ sind reflexiv und transitiv.
- $\asymp$ ist reflexiv, symmetrisch und transitiv, also eine Äquivalenzrelation

Quizfragen

Seien $f, g : \mathbb{N} \to \mathbb{R}$ beliebige Funktionen.

1. Welche der folgenden Äquivalenzen sind richtig?

$$
\begin{aligned}
f \in o(g) &\iff f \in \mathcal{O}(g), \\
f \in \omega(g) &\iff f \in \Omega(g), \\
f \in \mathcal{O}(g) &\iff f \in \Theta(g), \\
f \in \Omega(g) &\iff f \in \Theta(g), \\
f \in o(|g|) &\iff g \in \omega(|f|), \\
f \in \mathcal{O}(|g|) &\iff g \in \Omega(|f|), \\
f \in \Theta(|g|) &\iff g \in \Theta(|f|).
\end{aligned}
$$

   Ersetze bei falschen Aussagen das Symbol „ $\iff$ “ durch „ $\implies$ “ oder „ $\impliedby$ “.

2. Kann gleichzeitig $f \in o(g)$ und $f \in \Omega(g)$ gelten?
3. Kann gleichzeitig $f \in \omega(g)$ und $f \in \mathcal{O}(g)$ gelten?

1.

$$
\begin{array}{lcl}
f \in o(g) & \Longrightarrow & f \in \mathcal{O}(g), \\
f \in \omega(g) & \Longrightarrow & f \in \Omega(g), \\
f \in \mathcal{O}(g) & \Longleftarrow & f \in \Theta(g), \\
f \in \Omega(g) & \Longleftarrow & f \in \Theta(g), \\
f \in o(|g|) & \Longleftrightarrow & g \in \omega(|f|), \\
f \in \mathcal{O}(|g|) & \Longleftrightarrow & g \in \Omega(|f|), \\
f \in \Theta(|g|) & \Longleftrightarrow & g \in \Theta(|f|).
\end{array}
$$

2. Nö! Wir wissen:

$$\begin{aligned} f \in o(g) &\iff \forall c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| < c \cdot g(n) \\ f \in \Omega(g) &\iff \exists c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| \geq c \cdot g(n) \end{aligned}$$

   $f(n)$ kann nicht für alle $c \in \mathbb{R}^+$ von $c \cdot g(n)$ dominiert werden und gleichzeitig $c \cdot g(n)$ für einige $c \in \mathbb{R}^+$ dominieren.

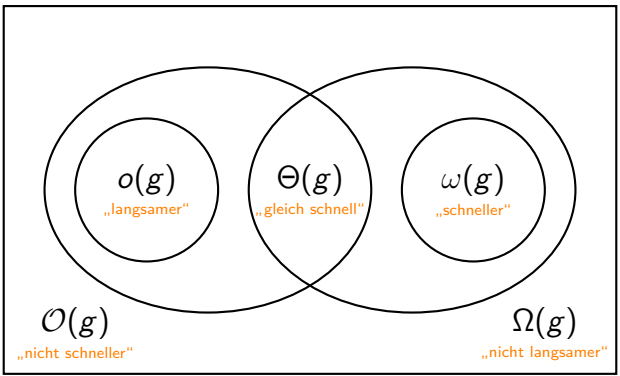
3. Genauso nö wie 2. Wir wissen:

$$\begin{aligned} f \in \omega(g) &\iff \forall c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| > c \cdot g(n) \\ f \in \mathcal{O}(g) &\iff \exists c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| \leq c \cdot g(n) \end{aligned}$$

   $f(n)$ kann nicht $c \cdot g(n)$ für alle $c \in \mathbb{R}^+$ dominieren und gleichzeitig für einige $c \in \mathbb{R}^+$ von $c \cdot g(n)$ dominiert werden.

Info

Viele Ergebnisse der letzten Quizfragen kann man an folgendem Euler-Diagramm erkennen:



Seien $f_1, \ldots, f_6 : \mathbb{N} \to \mathbb{R}$ Funktionen mit:

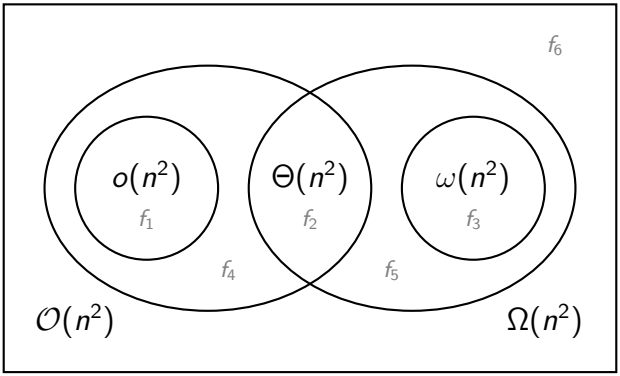
$$f_1(n) = n \qquad f_4(n) = \begin{cases} n, & \text{falls } n \text{ gerade} \\ n^2, & \text{sonst} \end{cases} \qquad f_2(n) \quad = n^2 f_5(n) \quad = \begin{cases} n^2, & \text{falls } n \text{ gerade} \\ n^3, & \text{sonst} \end{cases}$$

$$f_3(n) = n^3 \qquad f_6(n) = \begin{cases} n, & \text{falls } n \text{ gerade} \\ n^3, & \text{sonst} \end{cases}$$

Wie sieht das Euler-Diagramm über dem Universum $\{f_1, \ldots, f_6\}$ mit den Mengen

$$o(n^2) \qquad \omega(n^2) \qquad \mathcal{O}(n^2) \qquad \Omega(n^2) \qquad \Theta(n^2)$$

aus?


f_6
$o(n^2)$
f_1
$\Theta(n^2)$
f_2
$\omega(n^2)$
f_3
f_4
f_5
$\mathcal{O}(n^2)$
$\Omega(n^2)$

Überblick

Hier sind nochmal alle fünf Definitionen:

$$
\begin{array}{lcl}
f \in o(g) & \iff & \forall c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| < c \cdot g(n) \\
f \in \omega(g) & \iff & \forall c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| > c \cdot g(n) \\
f \in \mathcal{O}(g) & \iff & \exists c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| \leq c \cdot g(n) \\
f \in \Omega(g) & \iff & \exists c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |f(n)| \geq c \cdot g(n) \\
f \in \Theta(g) & \iff & f \in \mathcal{O}(g) \text{ und } f \in \Omega(g)
\end{array}
$$

Und ihre entsprechenden Negationen:

$$
\begin{array}{lcl}
f \notin o(g) & \iff & \exists c \in \mathbb{R}^+ : \forall n_0 \in \mathbb{N} : \exists n \geq n_0 : |f(n)| \geq c \cdot g(n) \\
f \notin \omega(g) & \iff & \exists c \in \mathbb{R}^+ : \forall n_0 \in \mathbb{N} : \exists n \geq n_0 : |f(n)| \leq c \cdot g(n) \\
f \notin \mathcal{O}(g) & \iff & \forall c \in \mathbb{R}^+ : \forall n_0 \in \mathbb{N} : \exists n \geq n_0 : |f(n)| > c \cdot g(n) \\
f \notin \Omega(g) & \iff & \forall c \in \mathbb{R}^+ : \forall n_0 \in \mathbb{N} : \exists n \geq n_0 : |f(n)| < c \cdot g(n) \\
f \notin \Theta(g) & \iff & f \notin \mathcal{O}(g) \text{ oder } f \notin \Omega(g)
\end{array}
$$

Rezept

Frage: Wie zeigt man, dass zwei gegebene Funktionen f und g in einer gegebenen Beziehung zueinander stehen? (z.B. $f \in o(g)$ oder $f \notin \Omega(g)$)
Methode:

1. Betrachte die Aussage, die bewiesen werden muss. Diese hat folgende Form:

$$Q_1\, c \in \mathbb{R}^+ : Q_2\, n_0 \in \mathbb{N} : Q_3\, n \geq n_0 : |f(n)|\, R\, c \cdot g(n),$$

   wobei $R \in \{<, >, \leq, \geq\}$ ein Vergleichsoperator und $Q_1, Q_2, Q_3 \in \{\exists, \forall\}$ Quantoren sind.

2. Finde einen konkreten Wert für jede Variable neben einem Existenzquantor $\exists$, in Abhängigkeit von allen Variablen links von ihr, die neben einem Allquantor $\forall$ stehen.

3. Die gewählten Werte sollen die Ungleichung $|f(n)|\, R\, c \cdot g(n)$ erfüllen.

Erstes Beispiel

Es soll $6n^2 \in o(2n^3)$ gezeigt werden, also:

$$\forall c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |6n^2| < c \cdot |2n^3|.$$

Gesucht ist ein $n_0 \in \mathbb{N}$ in Abhängigkeit von einem beliebigen $c \in \mathbb{R}^+$, so dass die Aussage in den Klammern erfüllt ist.

Lösen der Ungleichung nach n ergibt:

$$|6n^2| < c \cdot |2n^3| \iff 6n^2 < c \cdot 2n^3 \iff \frac{3}{c} < n \impliedby \frac{3}{c} + 1 \leq n.$$

Für $n_0 := \left\lceil \frac{3}{c} + 1 \right\rceil$ gilt dann:

$$n \geq n_0 \implies |6n^2| < c \cdot |2n^3|.$$

□

Info

In dem Beispiel haben wir $\frac{3}{c} + 1$ mit Gauß-Klammern $\lceil \dots \rceil$ aufgerundet, weil $\frac{3}{c} + 1$ nicht für jedes $c \in \mathbb{R}^+$ eine natürliche Zahl ist.

Zweites Beispiel

Es soll $4n^3 \in \omega(8n^2)$ gezeigt werden, also:

$$\forall c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |4n^3| > c \cdot |8n^2|.$$

Gesucht ist ein $n_0 \in \mathbb{N}$ in Abhängigkeit von einem beliebigen $c \in \mathbb{R}^+$, so dass die Aussage in den Klammern erfüllt ist.

Lösen der Ungleichung nach n ergibt:

$$|4n^3| > c \cdot |8n^2| \iff 4n^3 > c \cdot 8n^2 \iff n > 2c \impliedby n \geq 2c + 1.$$

Für $n_0 := \lceil 2c + 1 \rceil$ gilt dann:

$$n \geq n_0 \implies |4n^3| > c \cdot |8n^2|.$$

□

Drittes Beispiel

Es soll $n^2 + \frac{1}{10} \in \mathcal{O}(n^3 + 1)$ gezeigt werden, also:

$$\exists c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : \left| n^2 + \frac{1}{10} \right| \leq c \cdot |n^3 + 1|.$$

Wähle z.B. $c := \frac{1}{10}$.

Lösen der Ungleichung nach n ergibt:

$$\left| n^2 + \frac{1}{10} \right| \leq \frac{1}{10} \cdot |n^3 + 1| \iff n^2 + \frac{1}{10} \leq \frac{1}{10} n^3 + \frac{1}{10} \iff n^2 \leq \frac{1}{10} n^3 \iff 10 \leq n.$$

Für $n_0 := 10$ gilt dann:

$$n \geq n_0 \implies \left| n^2 + \frac{1}{10} \right| \leq c \cdot |n^3 + 1|.$$

□

Viertes Beispiel

Es soll $n^2 + 1 \in \Omega\left(n + \frac{1}{5}\right)$ gezeigt werden, also:

$$\exists c \in \mathbb{R}^+ : \exists n_0 \in \mathbb{N} : \forall n \geq n_0 : |n^2 + 1| \geq c \cdot \left|n + \frac{1}{5}\right|.$$

Wähle z.B. $c := 5$.

Lösen der Ungleichung nach n ergibt:

$$|n^2 + 1| \geq 5 \cdot \left|n + \frac{1}{5}\right| \iff n^2 + 1 \geq 5n + 1 \iff n^2 \geq 5n \iff n \geq 5.$$

Für $n_0 := 5$ gilt dann:

$$n \geq n_0 \implies |n^2 + 1| \geq c \cdot \left|n - \frac{1}{5}\right|.$$

□

Fünftes Beispiel

Es soll $3n^3 \notin o(n^2)$ gezeigt werden, also:

$$\exists c \in \mathbb{R}^+ : \forall n_0 \in \mathbb{N} : \exists n \geq n_0 : |3n^3| \geq c \cdot |n^2|.$$

Wähle z.B. $c := 3$.

Lösen der Ungleichung nach n ergibt:

$$|3n^3| \geq 3 \cdot |n^2| \iff 3n^3 \geq 3n^2 \iff n \geq 1.$$

Nun soll ein $n \in \mathbb{N}$ in Abhängigkeit von $n_0 \in \mathbb{N}$ gewählt werden, so dass $n \geq n_0$ und $n \geq 1$ gelten, z.B.

$$n := \max\{n_0, 1\}.$$

□

Sechstes Beispiel

Es soll $2^n \notin \omega(n^n)$ gezeigt werden, also:

$$\exists c \in \mathbb{R}^+ : \forall n_0 \in \mathbb{N} : \exists n \geq n_0 : |2^n| \leq c \cdot |n^n|.$$

Wähle z.B. $c := 1$.

Lösen der Ungleichung nach n ergibt:

$$|2^n| \leq 1 \cdot |n^n| \iff 2^n \leq n^n \iff \ln(2^n) \leq \ln(n^n) \iff n \ln 2 \leq n \ln n \iff 2 \leq n.$$

Nun soll ein $n \in \mathbb{N}$ in Abhängigkeit von $n_0 \in \mathbb{N}$ gewählt werden, so dass $n \geq n_0$ und $n \geq 2$ gelten, z.B.

$$n := \lceil \max\{n_0, 2\} \rceil.$$

□

Siebtes Beispiel

Es soll $5n^2 \notin \mathcal{O}(n)$ gezeigt werden, also:

$$\forall c \in \mathbb{R}^+ : \forall n_0 \in \mathbb{N} : \exists n \geq n_0 : |5n^2| > c \cdot |n|.$$

Lösen der Ungleichung nach n ergibt:

$$|5n^2| > c \cdot |n| \iff 5n^2 > c \cdot n \iff n > \frac{c}{5} \impliedby n \geq \frac{c}{5} + 1.$$

Nun soll ein $n \in \mathbb{N}$ in Abhängigkeit von $c \in \mathbb{R}^+$ und $n_0 \in \mathbb{N}$ gewählt werden, so dass $n \geq n_0$ und $n \geq \frac{c}{5} + 1$ gelten, z.B.

$$n := \left\lceil \max\left\{ n_0, \frac{c}{5} + 1 \right\} \right\rceil.$$

□

Achtes Beispiel

Es soll $n \notin \Omega(3n^2)$ gezeigt werden, also:

$$\forall c \in \mathbb{R}^+ : \forall n_0 \in \mathbb{N} : \exists n \geq n_0 : |n| < c \cdot |3n^2|.$$

Lösen der Ungleichung nach n ergibt:

$$|n| < c \cdot |3n^2| \iff n < 3cn^2 \iff \frac{1}{3c} < n \impliedby \frac{1}{3c} + 1 \leq n$$

Nun soll ein $n \in \mathbb{N}$ in Abhängigkeit von $c \in \mathbb{R}^+$ und $n_0 \in \mathbb{N}$ gewählt werden, so dass $n \geq n_0$ und $n \geq \frac{1}{3c} + 1$ gelten, z.B.

$$n := \left\lceil \max \left\{ n_0, \frac{1}{3c} + 1 \right\} \right\rceil.$$

□

Rechenregeln

Falls $\lim_{n\to\infty}\left|\frac{f(n)}{g(n)}\right|$ existiert, dann gilt:

$$
\begin{aligned}
f \in o(g) &\iff \lim_{n\to\infty}\left|\frac{f(n)}{g(n)}\right| = 0,\\
f \in \omega(g) &\iff \lim_{n\to\infty}\left|\frac{f(n)}{g(n)}\right| = \infty,\\
f \in \mathcal{O}(g) &\iff \lim_{n\to\infty}\left|\frac{f(n)}{g(n)}\right| < \infty,\\
f \in \Omega(g) &\iff \lim_{n\to\infty}\left|\frac{f(n)}{g(n)}\right| > 0,\\
f \in \Theta(g) &\iff \lim_{n\to\infty}\left|\frac{f(n)}{g(n)}\right| = c \text{ mit } 0 < c < \infty.
\end{aligned}
$$

Außerdem gilt für alle $k > 1$:

$$
n! \in \mathcal{O}(n^n), \quad 2^n \in \mathcal{O}\left(2^{2n}\right), \quad n! \in \Omega\left(\left(\tfrac{n}{e}\right)^n\right), \quad n! \in \mathcal{O}\left(n \cdot \left(\tfrac{n}{e}\right)^n\right), \quad \sum_{i=0}^{k} a_i n^i \in \mathcal{O}(n^k),
$$

Hierarchie

Hier sind übliche Folgen nach ihrem Wachstum sortiert.

$$
\begin{aligned}
1 \prec \log\log n \prec (\log\log n)^2 \prec (\log\log n)^3 \prec \ldots \\
\prec \log n \prec (\log n)^2 \prec (\log n)^3 \prec \ldots \\
\prec n \prec n^2 \prec n^3 \prec \ldots \\
\prec 2^n \prec 3^n \prec 4^n \prec \ldots \\
\prec n^{\frac{n}{2}} \prec \left(\frac{n}{3}\right)^n \prec n! \prec \left(\frac{n}{2}\right)^n \prec n^n \\
\prec 2^{n^2} \prec 2^{n^3} \prec 2^{n^4} \prec \ldots .
\end{aligned}
$$

Bitte schaut euch die Infos auf der nächsten Folie an.

Infos zur Hierarchie

- Erinnerungen: $f \prec g$ heißt $f \in o(g)$ und $f \asymp g$ heißt $f \in \Theta(g)$.
- Ich habe immer „log“ statt „$\log_b$“ für eine bestimmte Basis b geschrieben, weil alle Logarithmen, unabhängig von der Basis, gleich schnell wachsen. Für Folgen f und g, die keine Nullfolgen sind, und Konstanten $a, b \in \mathbb{R}^+ \setminus \{1\}$ gilt:

$$f \asymp g \quad \Longrightarrow \quad \log_a f \asymp \log_b g \ .$$

  Z.B.: $\log_2 n \asymp \log_3 n$ und $\log_4 \log_2 n \asymp \log_5 \log_3 n$.
- Möchte man zwei Funktionen der Form $\frac{1}{\dots}$ miteinander vergleichen, so benutzt man die Regeln:

$$f(n) \prec g(n) \iff \tfrac{1}{g(n)} \prec \tfrac{1}{f(n)} \quad \text{und} \quad f(n) \asymp g(n) \iff \tfrac{1}{f(n)} \asymp \tfrac{1}{g(n)}$$

- Multipliziert man eine Funktion mit einer positiven Konstante, so wird sie dadurch weder schneller noch langsamer, z.B.:

$$n^2 \asymp 2n^2 \asymp 3n^2 \asymp \dots$$

In welcher Beziehung stehen folgende Funktionen zueinander?

	$\ln n$	n	$2n$	$\ln \sqrt{n}$	$\sqrt{n}$	$\log_2 n$
$\ln n$						
n						
$2n$						
$\ln \sqrt{n}$						
$\sqrt{n}$						
$\log_2 n$						

Trage in die Zeile von $f(n)$ und Spalte von $g(n)$ ein o, ω bzw. Θ ein, falls $f \in o(g)$, $f \in \omega(g)$ bzw. $f \in \Theta(g)$ gilt.

	$\ln n$	n	$2n$	$\ln \sqrt{n}$	$\sqrt{n}$	$\log_2 n$
$\ln n$	Θ	o	o	Θ	o	Θ
n	ω	Θ	Θ	ω	ω	ω
$2n$	ω	Θ	Θ	ω	ω	ω
$\ln \sqrt{n}$	Θ	o	o	Θ	o	Θ
$\sqrt{n}$	ω	o	o	ω	Θ	ω
$\log_2 n$	Θ	o	o	Θ	o	Θ

In welcher Beziehung stehen folgende Funktionen zueinander?

	$n \ln n$	n^2	2^n	$n\sqrt{n}$	3^n	$5n^2$
$n \ln n$						
n^2						
2^n						
$n\sqrt{n}$						
3^n						
$5n^2$						

Trage in die Zeile von $f(n)$ und Spalte von $g(n)$ ein o, ω bzw. Θ ein, falls $f \in o(g)$, $f \in \omega(g)$ bzw. $f \in \Theta(g)$ gilt.

	$n \ln n$	n^2	2^n	$n\sqrt{n}$	3^n	$5n^2$
$n \ln n$	Θ	o	o	o	o	o
n^2	ω	Θ	o	ω	o	Θ
2^n	ω	ω	Θ	ω	o	ω
$n\sqrt{n}$	ω	o	o	Θ	o	o
3^n	ω	ω	ω	ω	Θ	ω
$5n^2$	ω	Θ	o	ω	o	Θ

Die Stirling'sche Formel

Es gilt:

$$n! = \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{12n} + \mathcal{O}\left(\frac{1}{n^2}\right)\right)$$

Das heißt insbesondere:

$$\lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n} = 1$$

Info

Der Teil „$+\mathcal{O}\left(\frac{1}{n^2}\right)$“ bedeutet nichts anderes als „$+f(n)$“ mit f eine bestimmte Funktion aus $\mathcal{O}\left(\frac{1}{n^2}\right)$.

Themenübersicht

Konvergenzkriterien

Sei $(a_n)_{n\in\mathbb{N}}$ eine komplexe (oder reelle) Zahlenfolge.

- Nullfolgenkriterium. Es gilt:

$$a_n \text{ konvergiert nicht gegen Null} \implies \sum_{k=1}^{\infty} a_k \text{ divergiert}$$

- Majoranten- und Minorantenkriterium. Sei $(b_n)_{n\in\mathbb{N}}$ eine reelle Zahlenfolge mit $\exists n_0 \in \mathbb{N}\colon \forall n \geq n_0\colon |a_n| \leq b_n$. Dann gilt:

$$\begin{array}{lll} \sum_{k=1}^{\infty} b_k \text{ konvergiert} & \implies & \sum_{k=1}^{\infty} a_k \text{ konvergiert absolut} \\ \sum_{k=1}^{\infty} a_k \text{ divergiert} & \implies & \sum_{k=1}^{\infty} b_k \text{ divergiert} \end{array}$$

  Man nennt dann $\sum_{k=1}^{\infty} b_k$ eine Majorante von $\sum_{k=1}^{\infty} a_k$ und $\sum_{k=1}^{\infty} a_k$ eine Minorante von $\sum_{k=1}^{\infty} b_k$. Auf dem nächsten Info-Block sind potentielle Majoranten und Minoranten aufgelistet.

Konvergenzkriterien

- Quotientenkriterium. Falls $\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right|$ existiert und $\exists n_0 \in \mathbb{N}\colon \forall n \geq n_0\colon a_n \neq 0$ erfüllt, dann gilt:

$$\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| < 1 \quad \Longrightarrow \quad \sum_{k=1}^{\infty} a_k \text{ konvergiert absolut}$$
$$\lim_{n\to\infty} \left|\frac{a_{n+1}}{a_n}\right| > 1 \quad \Longrightarrow \quad \sum_{k=1}^{\infty} a_k \text{ divergiert}$$

- Wurzelkriterium. Es gilt:

$$\limsup_{n\to\infty} \sqrt[n]{|a_n|} < 1 \quad \Longrightarrow \quad \sum_{k=1}^{\infty} a_k \text{ konvergiert absolut}$$
$$\limsup_{n\to\infty} \sqrt[n]{|a_n|} > 1 \quad \Longrightarrow \quad \sum_{k=1}^{\infty} a_k \text{ divergiert}$$

- Leibniz-Kriterium. Falls $(a_n)_{n\in\mathbb{N}}$ eine reelle, monoton fallende Zahlenfolge ist, dann gilt:

$$\lim_{n\to\infty} a_n = 0 \quad \Longrightarrow \quad \sum_{k=1}^{\infty} (-1)^k a_k \text{ konvergiert}$$

Info

Folgende Reihen konvergieren und können als Majoranten benutzt werden:

- $\sum_{k=0}^{\infty} z^k$ (konvergiert für $|z| < 1$),
- $\sum_{k=1}^{\infty} \frac{1}{k(k+1)}$,
- $\sum_{k=1}^{\infty} \frac{1}{k^s}$ (konvergiert für $s \in \mathbb{Q}, s \geq 2$),
- $\sum_{k=0}^{\infty} \frac{1}{k!}$ (konvergiert gegen e),
- $\sum_{k=0}^{\infty} \frac{z^k}{k!}$ (konvergiert für alle $z \in \mathbb{C}$ gegen e^z) und
- $\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k}$.

Folgende Reihen divergieren und können als Minoranten benutzt werden:

- $\sum_{k=0}^{\infty} z^k$ (divergiert für $|z| \geq 1$) und
- $\sum_{k=1}^{\infty} \frac{1}{k}$.

Themenübersicht

Wichtige Operatoren

Sei $\mathbb{C}^{\mathbb{Z}}$ die Menge aller Funktionen von $\mathbb{Z}$ nach $\mathbb{C}$. Die Operatoren

$$E, \Delta, \nabla, I : \mathbb{C}^{\mathbb{Z}} \to \mathbb{C}^{\mathbb{Z}}$$

operieren auf solche Funktionen, d.h. sie erwarten eine Funktion von $\mathbb{Z}$ nach $\mathbb{C}$ als Argument und liefern ebenfalls eine Funktion von $\mathbb{Z}$ nach $\mathbb{C}$. Für eine beliebige Funktion $f : \mathbb{Z} \to \mathbb{C}$ gilt:

$$\begin{aligned} Ef(x) &:= f(x+1), \\ If(x) &:= f(x), \\ \Delta f(x) &:= f(x+1) - f(x), \\ \nabla f(x) &:= f(x) - f(x-1). \end{aligned}$$

Infos

- Die Funktion f bildet nur auf $\mathbb{C}$ ab, damit sie möglichst allgemein gehalten wird. Das heißt nicht unbedingt, dass sie von diesen bösen imaginären Zahlen heimgesucht wird!
- Δ heißt „Delta“ und ∇ „Nabla“.
- E und I sind umkehrbar. Es gilt:

$$E^{-1}f(x) = f(x-1) \qquad \text{und} \qquad I^{-1}f(x) = f(x)$$

- Δ und ∇ sind nicht umkehrbar, weil sie nicht bijektiv sind. Es gilt z.B.:

$$\Delta 3x - 2 = (3(x+1) - 2) - (3x - 2) = 3$$
$$\Delta 3x + 5 = (3(x+1) + 5) - (3x + 5) = 3$$

Mehr Infos

Für beliebige Funktionen f, g und Zahlen $n \in \mathbb{N}_0$ und $a \in \mathbb{C}$ gibt es folgende Abkürzungen:

- $(f+g)(x) = f(x) + g(x)$
- $(f-g)(x) = f(x) - g(x)$
- $(af)(x) = a \cdot f(x)$
- $(fg)(x) = (f \circ g)(x) = f(g(x))$
- $f^n(x) = (\underbrace{f \circ f \circ \ldots \circ f}_{n \text{ mal}})(x)$

Weil Δ, ∇, E und I auch Funktionen sind, funktionieren diese Abkürzungen auch für sie.

Beispiele

- $\Delta x(x+1) = (x+1)(x+2) - x(x+1) = x^2 + 3x + 2 - x^2 - x = 2x + 2$
- $E^3\ 5^x = EEE5^x = EE5^{x+1} = E5^{x+2} = 5^{x+3}$
- $E\nabla x^2 = E(x^2 - (x-1)^2) = (x+1)^2 - x^2 = 2x + 1$
- $(3E^{-1} + I)(2x) = 3E^{-1}(2x) + I(2x) = 3(2(x-1)) + 2x = 8x - 6$

Erinnerung

$$
\begin{aligned}
Ef(x) &:= f(x+1), \\
If(x) &:= f(x), \\
\Delta f(x) &:= f(x+1) - f(x), \\
\nabla f(x) &:= f(x) - f(x-1).
\end{aligned}
$$

Was ergeben folgende Operationen?

1. $\Delta(2x + 1)$,
2. $\nabla(x + 3)$,
3. $\Delta(x^2 - x)$,
4. $\nabla(x^2 - x)$,
5. $\Delta(x^2 + x)$,
6. $\nabla(x^2 + x)$,
7. $E(x^2) - I(2x)$,
8. $E^3 1$.

1. $\Delta(2x+1) = (2(x+1)+1) - (2x+1) = 2$,
2. $\nabla(x+3) = (x+3) - ((x-1)+3) = 1$,
3. $\Delta(x^2 - x) = ((x+1)^2 - (x+1)) - (x^2 - x) = 2x$,
4. $\nabla(x^2 - x) = (x^2 - x) - ((x-1)^2 - (x-1)) = 2x - 2$,
5. $\Delta(x^2 - x) = ((x+1)^2 + (x+1)) - (x^2 + x) = 2x + 2$,
6. $\nabla(x^2 - x) = (x^2 + x) - ((x-1)^2 + (x-1)) = 2x$,
7. $E(x^2) - I(2x) = (x+1)^2 - 2x = x^2 + 1$,
8. $E^3 1 = E(E(E(1))) = E(E(1)) = E(1) = 1$.

Noch eine Quizfrage

Sei $f : \mathbb{Z} \to \mathbb{C}$ mit

$$f(x) = \begin{cases} 3 - x & \text{falls } x \text{ gerade} \\ x - 3 & \text{sonst.} \end{cases}$$

Was ist $\Delta f(x)$?

Falls x gerade, dann ist $x+1$ ungerade und es gilt

$$\Delta f(x) = f(x+1) - f(x) = (x+1) - 3 - (3-x) = 2x - 5.$$

Falls x ungerade, dann ist $x+1$ gerade und es gilt

$$\Delta f(x) = f(x+1) - f(x) = 3 - (x+1) - (x-3) = 5 - 2x.$$

Daraus folgt:

$$\Delta f(x) = \begin{cases} 2x-5 & \text{falls } x \text{ gerade} \\ 5-2x & \text{sonst.} \end{cases}$$

Alternativ kann man $f(x) = (-1)^x \cdot (3-x)$ schreiben. Daraus folgt:

$$\begin{aligned} \Delta f(x) &= f(x+1) - f(x) \\ &= (-1)^{x+1} \cdot (3-(x+1)) - (-1)^x \cdot (3-x) \\ &= (-1)^x \cdot (2x-5). \end{aligned}$$

Mehr Quizfragen

Sei $f : \mathbb{Z} \to \mathbb{C}$ eine beliebige Funktion.

1. Gilt $(E \circ \nabla)(f(x)) = \Delta(f(x))$?
2. Gilt $(E \circ \Delta)(f(x)) = \nabla(f(x))$?
3. Gilt $(E \circ \Delta)(f(x)) = (\Delta \circ E)(f(x))$?
4. Gilt $(E \circ \nabla)(f(x)) = (\nabla \circ E)(f(x))$?
5. Gilt $(\Delta \circ \nabla)(f(x)) = (\nabla \circ \Delta)(f(x))$?

Mehr Antworten

1. Ja.
2. Nein.
3. Ja.
4. Ja.
5. Ja.

Erinnerung aus der Schule

Die Ableitung $\frac{\mathrm{d}}{\mathrm{d}x} f(x)$ bzw. $f'(x)$ einer Funktion $f : \mathbb{R} \to \mathbb{C}$ war:

$$\frac{\mathrm{d}}{\mathrm{d}x} f(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}.$$

äquivalent dazu ist der Ausdruck

$$\frac{\mathrm{d}}{\mathrm{d}x} f(x) = \lim_{h \to 0} \frac{f(x) - f(x-h)}{h}.$$

Hier kann man h gegen 0 laufen lassen, weil der Abstand zwischen zwei reellen Zahlen beliebig klein sein kann. Man nennt $\frac{\mathrm{d}}{\mathrm{d}x}$ Differentialoperator.

Diskrete Ableitung

In $\mathbb{Z}$ ist der kleinste Abstand zwischen zwei Zahlen 1. Setzt man also $h = 1$ so bekommt man für $f : \mathbb{Z} \to \mathbb{C}$ zwei diskrete Analoga zur Ableitung, nämlich Δ und ∇:

$$\lim_{h \to 1} \frac{f(x+h) - f(x)}{h} = \frac{f(x+1) - f(x)}{1} = f(x+1) - f(x) = \Delta f(x),$$
$$\lim_{h \to 1} \frac{f(x) - f(x-h)}{h} = \frac{f(x) - f(x-1)}{1} = f(x) - f(x-1) = \nabla f(x).$$

Man nennt Δ Vorwärts- und ∇ Rückwärts-Differenzenoperator.

n-te Ableitung

Für eine beliebige Funktion $f : \mathbb{Z} \to \mathbb{C}$ gilt:

$$\Delta^n f(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k)$$

Beispiel

Für $f : \mathbb{Z} \to \mathbb{C}$ mit $f(x) = x^3$ gilt:

$$\begin{aligned}
\Delta^2 x^3 &= \sum_{k=0}^{2} (-1)^{2-k} \binom{2}{k} (x+k)^3 \\
&= (-1)^{2-0} \binom{2}{0} (x+0)^3 + (-1)^{2-1} \binom{2}{1} (x+1)^3 + (-1)^{2-2} \binom{2}{2} (x+2)^3 \\
&= x^3 - 2(x+1)^3 + (x+2)^3 \\
&= 6x + 6.
\end{aligned}$$

Fallende und steigende Faktorielle (ausführlicher)

Sei $n \in \mathbb{N}$ beliebig. Aus Folie 102 wissen wir:

$$x^{\underline{0}} := 1, \qquad x^{\underline{n}} := x \cdot (x-1) \cdot (x-2) \cdot \ldots \cdot (x-n+1),$$
$$x^{\overline{0}} := 1, \qquad x^{\overline{n}} := x \cdot (x+1) \cdot (x+2) \cdot \ldots \cdot (x+n-1).$$

D.h. es gelten folgende Zusammenhänge:

$$x^{\underline{n}} = (x-n+1)^{\overline{n}}, \qquad x^{\overline{n}} = (x+n-1)^{\underline{n}}.$$

Fallende und steigende Faktorielle (ausführlicher)

Für negative Exponenten gilt:

$$x^{\underline{-n}} := \frac{1}{(x+1)^{\overline{n}}} = \frac{1}{(x+n)^{\underline{n}}}, \qquad x^{\overline{-n}} := \frac{1}{(x-1)^{\underline{n}}} = \frac{1}{(x-n)^{\overline{n}}}.$$

Daraus folgt, dass für ein beliebiges $k \in \mathbb{Z}$ gilt:

$$(x-k) \cdot x^{\underline{k}} = x^{\underline{k+1}}, \qquad (x+k) \cdot x^{\overline{k}} = x^{\overline{k+1}}.$$

Das schöne hier ist: k kann (im Gegensatz zu n) auch negativ sein!

Erinnerung aus der Schule

Eine reellwertige Funktion F mit $\frac{\mathrm{d}}{\mathrm{d}x}F(x) = f(x)$ hieß Stammfunktion von f und wir schrieben immer:

$$F(x) = \int f(x)dx,$$

wobei oft auch ein $c \in \mathbb{C}$ dazu addiert wurde. Außerdem galt immer:

$$\int_a^b f(x)dx = F(b) - F(a).$$

Dies entsprach der Fläche unterhalb von $f(x)$ zwischen a und b.

Summation

Eine Funktion $F : \mathbb{Z} \to \mathbb{C}$ mit $\Delta F(x) = f(x)$ nennt man Summation (auch diskrete Stammfunktion) von $f(x)$ und wir schreiben analog zur normalen Stammfunktion:

$$F(x) = \sum f(x),$$

wobei oft auch ein $c \in \mathbb{C}$ dazu addiert wird. Außerdem gilt:

$$\sum_{x=a}^{b} f(x) = F(b+1) - F(a).$$

Dies entspricht einer gewöhnlichen Summe

$$f(a) + f(a+1) + f(a+2) + \ldots + f(b).$$

Info

Falls $\Delta F(x) = f(x)$ gilt, so ist $F(x)$ nicht *die* diskrete Stammfunktion von $f(x)$, sondern lediglich *eine* diskrete Stammfunktion, denn für jedes $c \in \mathbb{C}$ ist $F(x) + c$ eine mögliche diskrete Stammfunktion von $f(x)$.

Meistens ist es egal, welche diskrete Stammfunktion man verwendet. Deswegen dürfen wir das blöde c oft einfach weglassen!

Diskrete Ableitungs- und Stammfunktionsregeln

Für die Funktionen $x^{\underline{n}}$, $x^{\overline{n}}$, a^x und $\binom{x}{m}$ gibt es folgende Rechenregeln:

$$\Delta x^{\underline{n}} = n \cdot x^{\underline{n-1}} \qquad (n \in \mathbb{Z}), \qquad \sum x^{\underline{n}} = \frac{x^{\underline{n+1}}}{n+1} \qquad (n \in \mathbb{Z} \setminus \{-1\}),$$

$$\Delta x^{\overline{n}} = n \cdot (x+1)^{\overline{n-1}} \qquad (n \in \mathbb{Z}), \qquad \sum x^{\overline{n}} = \frac{(x-1)^{\overline{n+1}}}{n+1} \qquad (n \in \mathbb{Z} \setminus \{-1\}),$$

$$\Delta a^x = a^x(a-1) \qquad (a \in \mathbb{C}), \qquad \sum a^x = \frac{a^x}{a-1} \qquad (a \in \mathbb{C}),$$

$$\Delta \binom{x}{m} = \binom{x}{m-1} \qquad (m \in \mathbb{N}), \qquad \sum \binom{x}{m} = \binom{x}{m+1} \qquad (m \in \mathbb{N}).$$

Nicht vergessen

$\sum f(x)$ ist nicht die einzige diskrete Stammfunktion von $f(x)$, sondern nur eine mögliche!

Beispiel

Wir bestimmen die Lösung (in Abhängigkeit von n) der Summe

$$\sum_{x=1}^{n} x^{\overline{2}} = 2 + 6 + 12 + 20 + \ldots + n(n+1).$$

Zuerst bestimmen wir eine Stammfunktion $F(x)$ für $f(x) = x^{\overline{2}}$:

$$F(x) = \sum x^{\overline{2}} = \frac{(x-1)^{\overline{2+1}}}{2+1} = \frac{(x-1)^{\overline{3}}}{3}.$$

Dann setzen wir die Grenzen ein:

$$\sum_{x=1}^{n} x^{\overline{2}} = F(n+1) - F(1) = \frac{n^{\overline{3}}}{3} - \frac{0^{\overline{3}}}{3} = \frac{n(n+1)(n+2)}{3}.$$

Was sind die Ergebnisse folgender Summen in Abhängigkeit von n?

1. $\sum_{x=0}^{n+1} x(x-1)$,
2. $\sum_{x=0}^{n-1} 3^x$,
3. $\sum_{x=0}^{n} \binom{x}{9}$.

1. Info: $x(x-1) = x^{\underline{2}}$.
   $\sum x^{\underline{2}} = \frac{x^{\underline{3}}}{3}$
   $\rightsquigarrow \sum_{x=0}^{n+1} x(x-1) = \sum_{x=0}^{n+1} x^{\underline{2}} = \frac{(n+2)^{\underline{3}}}{3} - \frac{0^{\underline{3}}}{3} = \frac{(n+2)(n+1)n}{3}$.
2. $\sum 3^x = \frac{3^x}{3-1} = \frac{3^x}{2}$
   $\rightsquigarrow \sum_{x=0}^{n-1} 3^x = \frac{3^n}{2} - \frac{3^0}{2} = \frac{3^n-1}{2}$.
3. $\sum \binom{x}{9} = \binom{x}{9+1} = \binom{x}{10}$
   $\rightsquigarrow \sum_{x=0}^{n} \binom{x}{9} = \binom{n+1}{10} - \binom{0}{10} = \binom{n+1}{10}$.

Eine der beliebtesten Integrationsregeln war immer die partielle Integration:

$$\int u(x) \cdot v'(x) dx = u(x) \cdot v(x) - \int u'(x) \cdot v(x) dx.$$

Mit Grenzen:

$$\int_a^b u(x) \cdot v'(x) dx = [u(x) \cdot v(x)]_a^b - \int_a^b u'(x) \cdot v(x) dx,$$

wobei $[h(x)]_a^b = h(b) - h(a)$.

Partielle Summation

Unsere beliebteste Summationsregel wird die Partielle Summation sein:

$$\sum u(x) \cdot \Delta v(x) = u(x) \cdot v(x) - \sum Ev(x) \cdot \Delta u(x).$$

Mit Grenzen:

$$\sum_{x=a}^{b} u(x) \cdot \Delta v(x) = [u(x) \cdot v(x)]_a^{b+1} - \sum_{x=a}^{b} Ev(x) \cdot \Delta u(x).$$

wobei $[h(x)]_a^b = h(b) - h(a)$.

Tipp

Bei der partiellen Summation sollte man die Funktion $u(x)$ so wählen, dass sie nach dem Ableiten einfacher wird oder sogar komplett verschwindet.

Beispiel

Wir bestimmen mithilfe der partiellen Summation das Ergebnis der Summe

$$\sum_{x=1}^{n} x \cdot 2^x.$$

Dazu haben wir zwei Möglichkeiten. Entweder:

1. Wir definieren $u(x) := x$ und $\Delta v(x) := 2^x$ und bestimmen zuerst eine mögliche Stammfunktion von $f(x) = x \cdot 2^x$ mithilfe der partiellen Summation:

$$F(x) = \sum x \cdot 2^x = x \cdot \frac{2^x}{2-1} - \sum 2^{x+1} \cdot 1 = x \cdot 2^x - \frac{2^{x+1}}{2-1} = (x-2) \cdot 2^x.$$

Danach setzen wir die Grenzen ein und erhalten:

$$\sum_{x=1}^{n} x \cdot 2^x = F(n+1) - F(1) = (n-1) \cdot 2^{n+1} - (-1) \cdot 2^1 = (n-1) \cdot 2^{n+1} + 2.$$

Beispiel

Oder:

2. Wir definieren $u(x) := x$ und $\Delta v(x) := 2^x$ und bestimmen den Wert von $\sum_{x=1}^{n} x \cdot 2^x$ direkt mithilfe der partiellen Summation mit Grenzen:

$$\begin{aligned}\sum_{x=1}^{n} x \cdot 2^x &= [x \cdot 2^x]_1^{n+1} - \sum_{x=1}^{n} 2^{x+1} \cdot 1 \\ &= [x \cdot 2^x]_1^{n+1} - \left[\frac{2^{x+1}}{2-1}\right]_1^{n+1} \\ &= ((n+1)2^{n+1} - 2) - (2^{n+2} - 2^2) \\ &= (n-1) \cdot 2^{n+1} + 2.\end{aligned}$$

Was sind die Ergebnisse folgender Summen?

1. $\sum_{k=1}^{n} k2^k$,
2. $\sum_{k=1}^{n} 9k4^k$,
3. $\sum_{k=1}^{n} k(k-1)3^k$.

Benutze die partielle Summation.

1. $\sum k2^k = k\frac{2^k}{2-1} - \sum E(\frac{2^k}{2-1})((k+1)-k) = k2^k - \sum 2^{k+1}\cdot 1 = k2^k - 2\sum 2^k =$
   $k2^k - 2\cdot\frac{2^k}{2-1} = (k-2)2^k$
   $\rightsquigarrow \sum_{k=1}^{n} k2^k = (((n+1)-2)2^{n+1}) - ((1-2)2^1) = (n-1)2^{n+1} + 2.$

2. $\sum 9k4^k = 9k\frac{4^k}{4-1} - \sum E(\frac{4^k}{4-1})(9(k+1)-9k) = 3k4^k - \sum\frac{4^{k+1}}{3}\cdot 9 = 3k4^k - 3\frac{4^{k+1}}{4-1} =$
   $3k4^k - 4^{k+1} = (3k-4)4^k$
   $\rightsquigarrow \sum_{k=1}^{n} 9k4^k = ((3(n+1)-4)4^{n+1}) - ((3\cdot 1-4)4^1) = (3n-1)4^{n+1} + 4.$

3. $\sum k(k-1)3^k = k(k-1)\frac{3^k}{2} - \sum 2k\frac{3^{k+1}}{2} = k(k-1)\frac{3^k}{2} - \sum k3^{k+1}$
   $\sum k3^{k+1} = k\frac{3^{k+1}}{2} - \sum 1\frac{3^{k+2}}{2} = k\frac{3^{k+1}}{2} - \frac{3^{k+2}}{4}$
   $\rightsquigarrow \sum k(k-1)3^k = k(k-1)\frac{3^k}{2} - k\frac{3^{k+1}}{2} + \frac{3^{k+2}}{4} = \frac{1}{2}(k(k-4)+\frac{9}{2})3^k$
   $\rightsquigarrow \sum_{k=1}^{n} k(k-1)3^k = (\frac{1}{2}((n+1)(n-3)+\frac{9}{2})3^{n+1}) - (\frac{1}{2}(1(1-4)+\frac{9}{2})3^1) =$
   $\frac{1}{2}(n^2-2n+\frac{3}{2})3^{n+1} - \frac{9}{4}.$

Vektor-Matrix-Multiplikation

Seien $A \in \mathbb{R}^{m \times m}$ eine Matrix mit m Zeilen und m Spalten und $u, v \in \mathbb{R}^m$ zwei Vektoren der Länge m. Es gilt:

$$A \cdot u = v \iff \forall n \in [m] : v_n = \sum_{k=1}^{m} a_{n,k} \cdot u_k$$

Beispiel

Beispielsweise gilt für $m = 3$:

$$\underbrace{\begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}}_{A \in \mathbb{R}^{3\times 3}} \cdot \underbrace{\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}}_{u \in \mathbb{R}^3} = \underbrace{\begin{pmatrix} a_{1,1}u_1 + a_{1,2}u_2 + a_{1,3}u_3 \\ a_{2,1}u_1 + a_{2,2}u_2 + a_{2,3}u_3 \\ a_{3,1}u_1 + a_{3,2}u_2 + a_{3,3}u_3 \end{pmatrix}}_{v \in \mathbb{R}^3}.$$

Inverse Matrizen

Seien $A, B \in \mathbb{R}^{m \times m}$ zwei $m \times m$-Matrizen. Fall $A \cdot B = I_m$ gilt, nennt man B die Inverse Matrix von A und schreibt:

$$A^{-1} = B$$

Dabei ist $I_m \in \mathbb{R}^{m \times m}$ die Einheitsmatrix:

$$I_m = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

I_m ist sowas wie das Einselement der $m \times m$-Matrizen und A und B multiplikative inverse Elemente voneinander

Infos

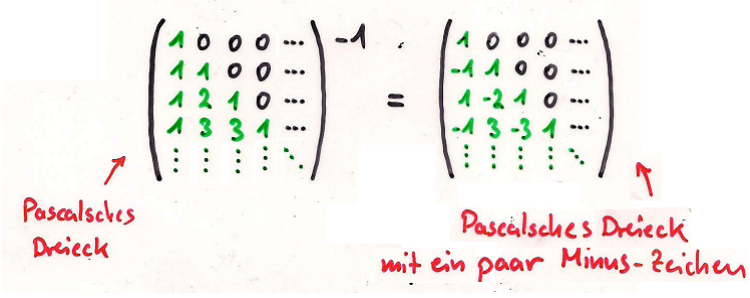
- Auch unendliche Matrizen können Inverse Matrizen besitzen. Die unendliche Einheitsmatrix wird durch das Kronecker-Delta dargestellt (s. Folie **??**).
- Ob man die Indizierung der Komponenten eines Vektors oder einer Matrix mit 1 oder mit 0 beginnt, ist völlig irrelevant. Die Formel wird entsprechend angepasst.

Bimomialinversion

Für beliebige Folgen $u = (u_0, u_1, u_2, \ldots)$ und $v = (v_0, v_1, v_2, \ldots)$, bzw. Vektoren unendlicher Länge, gilt:

$$\forall n \in \mathbb{N}_0 : v_n = \sum_{k=0}^{n} \binom{n}{k} \cdot u_k \iff \forall n \in \mathbb{N}_0 : u_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \cdot v_k.$$

Das heißt:



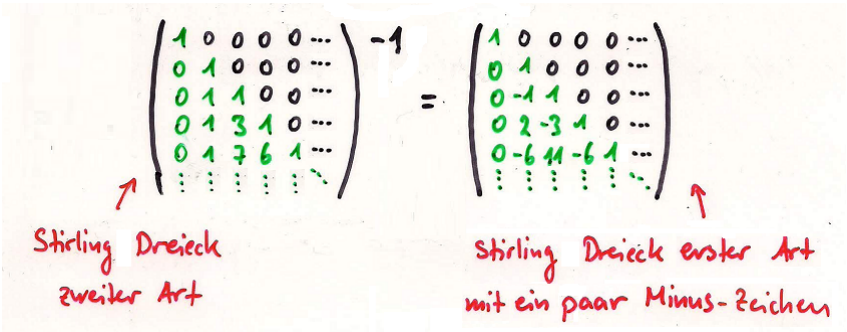
Stirling-Inversion

Für beliebige Folgen $u = (u_0, u_1, u_2, \ldots)$ und $v = (v_0, v_1, v_2, \ldots)$, bzw. Vektoren unendlicher Länge, gilt:

$$\forall n \in \mathbb{N}_0 : v_n = \sum_{k=0}^{n} S_{n,k} \cdot u_k \iff \forall n \in \mathbb{N}_0 : u_n = \sum_{k=0}^{n} (-1)^{n-k} s_{n,k} \cdot v_k.$$

Das heißt:

Stirling-Inversion



Themenübersicht

Folgen

Eine Funktion $f : \mathbb{N}_0 \to \mathbb{C}$ wird Folge genannt. Weil der Definitionsbereich von Folgen abzählbar ist, lassen sich Folgen als indizierte Listen darstellen. Man schreibt

$$(f_n)_{n\geq 0} = (f_0, f_1, f_2, f_3, \ldots)$$

mit $f_n = f(n)$ für alle $n \in \mathbb{N}_0$.

Beispiele

Einige (mehr oder weniger) bekannte Folgen sind:

- Fibonacci-Folge
$$(0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots),$$
- Merkwürdige Zahlen
$$(70, 836, 4030, 5830, 7192, 7912, \ldots),$$
- Superperfekte Zahlen
$$(2, 4, 16, 64, 4096, 65536, 262144, \ldots),$$
- Fröhliche Zahlen
$$(1, 7, 10, 13, 19, 23, 28, 31, 32, 44, \ldots),$$
- Glückliche Zahlen
$$(1, 3, 7, 9, 13, 15, 21, 25, 31, 33, \ldots).$$

Info

Die Folgen aus dem letzten Beispiel heißen wirklich so.

Geschlossene Ausdrücke

Oft lassen sich Folgen durch mathematische Ausdrücke vollständig beschreiben. Einen solchen Ausdruck nennen wir einen geschlossenen Ausdruck.

Beispiele

- $f_n = n^2$ ist ein geschlossener Ausdruck für die Folge

$$(f_n)_{n\geq 0} = (0, 1, 4, 9, 16, 25, 36, \ldots).$$

- $f_n = 2^n - 1$ ist ein geschlossener Ausdrsuck für die Folge

$$(f_n)_{n\geq 0} = (0, 1, 3, 7, 15, 31, 63, \ldots).$$

- $f_n = (-1)^n \cdot n$ ist ein geschlossener Ausdruck für die Folge

$$(f_n)_{n\geq 0} = (0, -1, 2 - 3, 4, -5, 6, -7, 8, \ldots).$$

Infos

- Es gibt Folgen, die man zwar mit einem Algorithmus berechnen kann, aber für die es keinen geschlossenen Ausdruck gibt. Tatsächlich gibt es auch Folgen, für die es nicht mal einen Algorithmus gibt!
- Im Abschnitt „Wachstum von Funktionen“ haben wir es ausschließlich mit solchen Folgen zu tun gehabt. Im Abschnitt „Beweismethoden“ (Teil Rekursionsgleichungen) haben wir die Korrektheit von gegebenen geschlossenen Ausdrücken bewiesen. In diesem Abschnitt werden wir Methoden kennenlernen, mit denen sich geschlossene Ausdrücke für bestimmte Arten von Rekursionsgleichungen finden lassen.

Welche geschlossenen Ausdrücke besitzen folgende Folgen $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0}$ und $(c_n)_{n\geq 0}$?

1. Für $(a_n)_{n\geq 0}$ gilt $a_0 = 0$ und $a_n = a_{n-1} + 1$ für alle $n \geq 1$.
2. Für $(b_n)_{n\geq 0}$ gilt $b_0 = 0$ und $b_n = b_{n-1} + 2n - 1$ für alle $n \geq 1$.
3. Für $(c_n)_{n\geq 0}$ gilt $c_0 = 0$, $c_1 = -2$ und $c_n = -4 \cdot (c_{n-1} + c_{n-2})$ für alle $n \geq 1$.

Wir berechnen die ersten Werte jeder Folge

n	0	1	2	3	4	5	6	$\cdots$
a_n	0	1	2	3	4	5	6	$\cdots$
b_n	0	1	4	9	16	25	36	$\cdots$
c_n	0	-2	8	-24	64	-160	384	$\cdots$

und erhalten folgende Vermutungen:

1. $a_n = n$
2. $b_n = n^2$
3. $c_n = n \cdot (-2)^n$

Natürlich ist das Ergebnis von c_n absolut trivial! ;-)

Lineare Rekursionsgleichungen

Wir betrachten in DS nur lineare Rekursionsgleichungen. Diese haben die Form:

$$f_{n+d} + q_1 f_{n+d-1} + q_2 f_{n+d-2} + \ldots + q_d f_n = s_n \qquad (\forall n \geq 0),$$

wobei $q_d \neq 0$ und s_n selbst eine Folge ist, z.B. $s_n = 5$, $s_n = 2^n$, etc.

Falls $s_n = 0$, dann ist die Rekursionsgleichung homogen. Ansonsten ist sie inhomogen.

Man nennt d den Grad, $q_1, q_2, \ldots, q_d$ die Koeffizienten und s_n das Störglied.

Werden die Anfangsbedingungen $f_0, f_1, \ldots, f_{d-1}$ explizit angegeben, so stellt die Rekursionsgleichung eine eindeutige Folge $(f_n)_{n \geq 0}$ dar.

Beispiele

Folgende Rekursionsgleichungen sind linear und homogen:

- Die Fibonacci-Folge kann geschrieben werden als:

$$f_{n+2} - f_{n+1} - f_n = 0 \qquad (\forall n \geq 0)$$

  mit $f_0 = 1$ und $f_1 = 1$.

- Die Folge $(c_n)_{n \geq 0}$ aus Folie 1518 kann definiert werden als:

$$c_{n+2} + 4c_{n+1} + 4c_n = 0 \qquad (\forall n \geq 0)$$

  mit $c_0 = 0$ und $c_1 = -2$.

Mehr Beispiele

Folgende Rekursionsgleichungen sind linear, aber nicht homogen:

- Die Folge $(a_n)_{n\geq 0}$ aus Folie 1518 kann definiert werden als:

$$a_{n+1} - a_n = 1 \qquad (\forall n \geq 0)$$

  mit $a_0 = 0$.

- Die Folge $(b_n)_{n\geq 0}$ aus Folie 1518 kann definiert werden als:

$$b_{n+1} - b_n = 2n + 1 \qquad (\forall n \geq 0)$$

  mit $b_0 = 0$.

Noch mehr Beispiele

Folgende Rekursionsgleichungen sind nicht linear und somit kein Teil von DS:

- Für die Fakultät $f_n = n!$ gilt:

$$f_{n+1} = (n+1) \cdot f_n \qquad (\forall n \geq 0)$$

  mit $f_0 = 1$.

- Für die Folge $(g_n)_{n \geq 0} = (2, 2, 4, 8, 32, 256, \ldots)$ gilt:

$$f_{n+2} = f_{n+1} \cdot f_n \qquad (\forall n \geq 0)$$

  mit $f_0 = 2$ und $f_1 = 2$.

Info

Einige inhomogene Rekursionsgleichungen lassen sich „homogenisieren“, d.h. in eine homogene Rekursionsgleichung überbringen. Leider funktioniert das nicht bei allen.

Charakteristisches Polynom

Zu einer gegebenen linearen homogenen Rekursionsgleichung

$$f_{n+d} + q_1 f_{n+d-1} + q_2 f_{n+d-2} + \ldots + q_d f_n = 0 \qquad (\forall n \geq 0)$$

ist das charakteristische Polynom $q^R(z)$ definiert als:

$$q^R(z) = z^d + q_1 z^{d-1} + q_2 z^{d-2} + \ldots + q_d$$

Beispiel

Die Rekursionsgleichung

$$f_{n+4} + 5f_{n+3} - 3f_{n+2} + 2f_{n+1} - f_n = 0 \qquad (\forall n \geq 0)$$

besitzt das charakteristische Polynom

$$q^R(z) = z^4 + 5z^3 - 3z^2 + 2z - 1.$$

Allgemeine Lösung

Zu einem gegebenen (faktorisierten) charakteristischen Polynom einer Rekursionsgleichung f mit Nullstellen $\alpha_1, \alpha_2, \ldots, \alpha_k$ und Vielfachheiten $d_1, d_2, \ldots, d_k$

$$\begin{aligned} q^R(z) &= z^d + q_1 z^{d-1} + q_2 z^{d-2} + \ldots + q_d \\ &= (z-\alpha_1)^{d_1}(z-\alpha_2)^{d_2}\ldots(z-\alpha_k)^{d_k} \end{aligned}$$

ist die allgemeine Lösung f_n der Rekursionsgleichung f

$$f_n = p_1(n)\alpha_1^n + p_2(n)\alpha_2^n + \ldots + p_k(n)\alpha_k^n \ ,$$

wobei die $p_i(n)$ Polynome über n sind mit Konstanten $c_0, c_1, \ldots, c_{d-1}$ und Grad $\text{grad}(p_i) \leq d_i - 1$.

Beispiel

Die zum charakteristischen Polynom

$$\begin{aligned} q^R(z) &= z^7 - 9z^6 + 27z^5 - 19z^4 - 48z^3 + 72z^2 + 16z - 48 \\ &= (z+1)^2(z-2)^4(z-3) \end{aligned}$$

gehörende allgemeine Lösung ist

$$f_n = \underbrace{(c_0 + c_1 n)}_{p_1(n)}(-1)^n + \underbrace{(c_2 + c_3 n + c_4 n^2 + c_5 n^3)}_{p_2(n)} 2^n + \underbrace{c_6}_{p_3(n)} 3^n.$$

Es gilt:

- $\text{grad}(p_1) = d_1 - 1 = 2 - 1 = 1$
- $\text{grad}(p_2) = d_2 - 1 = 4 - 1 = 3$
- $\text{grad}(p_3) = d_3 - 1 = 1 - 1 = 0$

Erinnerung

Man kann ein Polynom mit Unbekannter z faktorisieren, indem man eine Nullstelle α_i errät und dann das Polynom durch $(z - \alpha_i)$ teilt. Somit wird der Grad des Polynoms um 1 verringert. Das wiederholt man bis das Polynom Grad 2 hat. Dann kann man die fehlenden zwei Nullstellen beispielsweise mit der Mitternachtsformel bestimmen.

Nicht vergessen

Ein Polynom von Grad d über einem Körper K hat immer höchstens d Nullstellen in K. Falls $K = \mathbb{C}$, dann sind es immer genau d.

Methode 1

Frage: Wie löst man lineare homogene Rekursionsgleichungen?
Methode: Gegeben sei die Rekursionsgleichung:

$$f_{n+d} + q_1 f_{n+d-1} + q_2 f_{n+d-2} + \ldots + q_d f_n = 0 \qquad (\forall n \geq 0)$$

mit Anfangsbedingungen $f_0, f_1, \ldots, f_{d-1}$.

1. Charakteristisches Polynom aufstellen und über $\mathbb{C}$ faktorisieren:

$$\begin{aligned} q^R(z) &= z^d + q_1 z^{d-1} + q_2 z^{d-2} + \ldots + q_d \\ &= (z-\alpha_1)^{d_1} \cdot (z-\alpha_2)^{d_2} \cdot \ldots \cdot (z-\alpha_k)^{d_k}. \end{aligned}$$

2. Allgemeine Lösung aufstellen:

$$f_n = p_1(n)\alpha_1^n + p_2(n)\alpha_2^n + \ldots + p_k(n)\alpha_k^n$$

   mit $p_i(n)$ Polynome über n mit Konstanten $c_0, c_1, \ldots, c_{d-1}$ und $\operatorname{grad}(p_i) = d_i - 1$.

3. Allgemeine Lösung f_n für $n = 0, \ldots, d-1$ mit der jeweiligen Anfangsbedingung gleichsetzen und Gleichungssystem nach $c_0, \ldots, c_{d-1}$ lösen.

4. Die allgemeine Lösung mit eingesetzten c_i nennt man spezielle Lösung.

Beispiel

Aufgabe: Löse die lineare homogene Rekursionsgleichung

$$f_{n+3} - 4f_{n+2} + 5f_{n+1} - 2f_n = 0 \qquad (\forall n \geq 0)$$

mit Anfangsbedingungen $f_0 = 2$, $f_1 = 4$ und $f_2 = 7$.

Beispiel

Lösung:

1. Das charakteristisches Polynom ist:

$$q^R(z) = z^3 - 4z^2 + 5z - 2 = (z-2)(z-1)^2.$$

2. Die allgemeine Lösung ist:

$$f_n = c_0 2^n + (c_1 + c_2 n)1^n = c_0 2^n + c_1 + c_2 n.$$

3. Einsetzen von 0, 1 und 2 in f_n und Gleichsetzen mit den Anfangsbedingungen liefert:

$$\begin{array}{rcrcrcrcl} f_0 & = & c_0 & + & c_1 & & & \stackrel{!}{=} & 2 \\ f_1 & = & 2c_0 & + & c_1 & + & c_2 & \stackrel{!}{=} & 4 \\ f_2 & = & 4c_0 & + & c_1 & + & 2c_2 & \stackrel{!}{=} & 7 \end{array}$$

   mit eindeutiger Lösung $c_0 = 1, c_1 = 1, c_2 = 1$.

4. Die spezielle Lösung ist dann:

$$f_n = 2^n + 1 + n.$$

Welche Lösung besitzen folgende homogene Rekursionsgleichungen?

1. $f_0 = 2$ und $f_{n+1} - 2f_n = 0$ für alle $n \geq 0$,
2. $f_0 = 1$ und $f_{n+1} + 5f_n = 0$ für alle $n \geq 0$,
3. $f_0 = 4$, $f_1 = 0$ und $f_{n+2} - 4f_{n+1} + 4f_n = 0$ für alle $n \geq 0$,
4. $f_0 = 3$, $f_1 = 0$ und $f_{n+2} + f_{n+1} - 2f_n = 0$ für alle $n \geq 0$,
5. $f_0 = 2$, $f_1 = 4$, $f_2 = 7$ und $f_{n+3} - 4f_{n+2} + 5f_{n+1} - 2f_n = 0$ für alle $n \geq 0$,
6. $f_0 = 3$, $f_1 = 6$, $f_2 = -4$ und $f_{n+3} + 2f_{n+2} - 4f_{n+1} - 8f_n = 0$ für alle $n \geq 0$,
7. $f_0 = 1$, $f_1 = 0$, $f_2 = 3$, $f_3 = 4$ und $f_{n+4} - 4f_{n+3} + 6f_{n+2} - 4f_{n+1} + f_n = 0$ für alle $n \geq 0$.

Benutze die Methode aus Folie 1531.

Antworten (kompakt)

1. $q^R = z - 2$
   $\rightsquigarrow f_n = c_0 \cdot 2^n = 2 \cdot 2^n = 2^{n+1}$,
2. $q^R = z + 5$
   $\rightsquigarrow f_n = c_0 \cdot (-5)^n = (-5)^n$,
3. $q^R = z^2 - 4z + 4 = (z-2)^2$
   $\rightsquigarrow f_n = (c_0 + c_2 n) \cdot 2^n = (4 - 4n) \cdot 2^n = (1-n) \cdot 2^{n+2}$,
4. $q^R = z^2 + z - 2 = (z-1) \cdot (z+2)$
   $\rightsquigarrow f_n = c_0 \cdot 1^n + c_1 \cdot (-2)^n = 2 + (-2)^n$,
5. $q^R = z^3 - 4z^2 + 5z - 2 = (z-1)^2 \cdot (z-2)$
   $\rightsquigarrow f_n = (c_0 + c_1 n) \cdot 1^n + c_2 \cdot 2^n = 1 + n + 2^n$,
6. $q^R = z^3 + 2z^2 - 4z - 8 = (z-2) \cdot (z+2)^2$
   $\rightsquigarrow f_n = c_0 \cdot 2^n + (c_1 + c_2 n) \cdot (-2)^n = 2 \cdot 2^n + (1 - 2n) \cdot (-2)^n = 2^{n+1} + (1-2n) \cdot (-2)^n$,

7. $q^R(z) = z^4 - 4z^3 + 6z^2 - 4z + 1 = (z-1)^4$
   $\rightsquigarrow f_n = (c_0 + c_1 n + c_2 n^2 + c_3 n^3) \cdot 1^n = 1 - 5n + 5n^2 - n^3.$

Gegeben seien die durch die Rekursionsgleichungen

$$f_{n+1} - 3f_n = g_n \qquad (\forall n \geq 0) \qquad \text{und} \qquad g_{n+1} - 2g_n = 2f_n \qquad (\forall n \geq 0)$$

mit Anfangsbedingungen $f_0 = 1$ und $g_0 = 2$ beschrieben Folgen $(f_n)_{n\geq 0}$ und $(g_n)_{n\geq 0}$.

Welchen geschlossenen Ausdruck besitzt f_n?

Einsetzen von $g_n = f_{n+1} - 3f_n$ in $g_{n+1} - 2g_n = 2f_n$ liefert:

$$(f_{n+2} - 3f_{n+1}) - 2(f_{n+1} - 3f_n) = 2f_n \qquad (\forall n \geq 0) \ .$$

Durch Umformen erhält man die Rekursionsgleichung

$$f_{n+2} - 5f_{n+1} + 4f_n = 0 \qquad (\forall n \geq 0)$$

mit Anfangsbedingungen $f_0 = 1$ und $f_1 = g_0 + 3f_0 = 2 + 3 \cdot 1 = 5$. Es folgt:

$$q^R(z) = z^2 - 5z + 4 = (z-1)(z-4)$$

$$\rightsquigarrow \ f_n = c_0 \cdot 1^n + c_1 \cdot 4^n = -\tfrac{1}{3} \cdot 1^n + \tfrac{4}{3} \cdot 4^n = \tfrac{1}{3}(4^{n+1} - 1)$$

Methode 2

Frage: Wie homogenisiert man eine lineare inhomogene Rekursionsgleichung?
Methode: Gegeben sei die Rekursionsgleichung:

$$f_{n+d} + q_1 f_{n+d-1} + q_2 f_{n+d-2} + \ldots + q_d f_n = s_n \qquad (\forall n \geq 0) \tag{5}$$

mit Anfangsbedingungen $f_0, f_1, \ldots, f_{d-1}$.

1. s_n als lineare homogene Rekursionsgleichung mit Grad e darstellen:

   $$s_{n+e} + r_1 s_{n+e-1} + r_2 s_{n+e-2} + \ldots + r_e s_n = 0 \qquad (\forall n \geq 0) \tag{6}$$

   (Methode 1 rückwärts!)
2. Die Gleichung (1) für $s_n, s_{n+1}, \ldots, s_{n+e}$ in (2) einsetzen und eine lineare homogene Rekursionsgleichung mit Grad $d + e$ für f bekommen:

   $$f_{n+d+e} + t_1 f_{n+d+e-1} + t_2 f_{n+d+e-2} + \ldots + t_{d+e} f_n = 0 \qquad (\forall n \geq 0)$$

3. Die fehlenden e Anfangsbedingungen $f_d, f_{d+1}, \ldots, f_{d+e-1}$ mit Gleichung (1) berechnen.

Beispiel

Aufgabe: Homogenisiere die Rekursionsgleichung

$$f_{n+1} + f_n = n \cdot 3^n \qquad (\forall n \geq 0) \tag{1}$$

mit Anfangsbedingung $f_0 = 1$.

Beispiel

Lösung:

1. Das Störglied $s_n = n \cdot 3^n$ hat die Form $s_n = p_1(n) \cdot 3^n$ mit $\text{grad}(p_1) = 1$. Daraus folgt: $\alpha_1 = 3, d_1 = \text{grad}(p_1) + 1 = 2$. Das charakteristische Polynom von s_n lautet also:

$$q^R(z) = (z-3)^2 = z^2 - 6z + 9$$

und somit ist die gesuchte Rekursionsgleichung:

$$s_{n+2} - 6s_{n+1} + 9s_n = 0 \qquad (\forall n \geq 0) \tag{2}$$

2. Durch Einsetzen von $s_n = f_{n+1} + f_n$ aus (1) in (2) bekommt man:

$$\underbrace{(f_{n+3} + f_{n+2})}_{s_{n+2}} - 6\underbrace{(f_{n+2} + f_{n+1})}_{s_{n+1}} + 9\underbrace{(f_{n+1} + f_n)}_{s_n} = 0 \qquad (\forall n \geq 0)$$

und durch Umformen:

$$f_{n+3} - 5f_{n+2} + 3f_{n+1} + 9f_n = 0 \qquad (\forall n \geq 0)$$

3. Einsetzen von $n = 0$ und $n = 1$ in (1) liefert $f_1 = -1$ und $f_2 = 4$.

Wie kann man folgende inhomogene Rekursionsgleichungen homogenisieren?

1. $f_0 = 0$ und $f_{n+1} + 2f_n = 2^n$ für alle $n \geq 0$,
2. $f_0 = 1$ und $f_{n+1} - 3f_n = 3^n$ für alle $n \geq 0$,
3. $f_0 = 2$ und $f_{n+1} + f_n = 5^n$ für alle $n \geq 0$,
4. $f_0 = 1$ und $f_{n+1} - 4f_n = 5$ für alle $n \geq 0$,
5. $f_0 = 1$ und $f_{n+1} + f_n = n \cdot 3^n$ für alle $n \geq 0$,
6. $f_0 = 1$, $f_1 = 2$ und $f_{n+2} - 2f_{n+1} + f_n = 3^n + (-2)^n$ für alle $n \geq 0$,
7. $f_0 = 1$ und $f_{n+1} + f_n = n \cdot 3^n + 2^n$ für alle $n \geq 0$.

Benutze die Methode aus Folie 1539.

Antworten (kompakt)

1. $f_0 = 0$, $f_1 = 1$ und $f_{n+2} - 4f_n = 0$ für alle $n \geq 0$,
2. $f_0 = 1$, $f_1 = 4$ und $f_{n+2} - 6f_{n+1} + 9f_n = 0$ für alle $n \geq 0$,
3. $f_0 = 2$, $f_1 = -1$ und $f_{n+2} - 4f_{n+1} - 5f_n = 0$ für alle $n \geq 0$,
4. $f_0 = 1$, $f_1 = 9$ und $f_{n+2} - 5f_{n+1} + 4f_n = 0$ für alle $n \geq 0$,
5. $f_0 = 1$, $f_1 = -1$, $f_2 = 4$ und $f_{n+3} - 5f_{n+2} + 3f_{n+1} + 9f_n = 0$ für alle $n \geq 0$,
6. $f_0 = 1$, $f_1 = 2$, $f_2 = 5$, $f_3 = 9$ und $f_{n+4} - 3f_{n+3} - 3f_{n+2} + 11f_{n+1} - 6f_n = 0$ für alle $n \geq 0$,
7. $f_0 = 1$, $f_1 = 0$, $f_2 = 5$, $f_3 = 17$ und $f_{n+4} - 7f_{n+3} + 13f_{n+2} + 3f_{n+1} - 18f_n = 0$ für alle $n \geq 0$.

Erzeugende Funktionen

Zu einer Folge $(f_n)_{n\geq 0} = (f_0, f_1, f_2, \ldots)$ ist die erzeugende Funktion $F(z)$ definiert als:

$$F(z) := \sum_{n=0}^{\infty} f_n \cdot z^n.$$

Infos

- Man benutzt für die erzeugende Funktion denselben Buchstaben wie für die Folge, aber in Großschrift, z.B.:

$$A(z) := \sum_{n=0}^{\infty} a_n \cdot z^n, \qquad B(z) := \sum_{n=0}^{\infty} b_n \cdot z^n, \qquad C(z) := \sum_{n=0}^{\infty} c_n \cdot z^n \ , \qquad \dots$$

- Das war Definition 219 im Skript vom Wintersemester 2012/13 (Prof. Mayr)

Schön. Aber wozu erzeugende Funktionen?

Kommt gleich!

Erzeugende Funktionen für lineare homogene Rekursionsgleichungen

Zu einer gegebenen linearen homogenen Rekursionsgleichung

$$f_{n+d} + q_1 f_{n+d-1} + q_2 f_{n+d-2} + \ldots + q_d f_n = 0$$

mit Anfangsbedingungen $f_0, f_1, \ldots, f_{d-1}$ ist die erzeugende Funktion:

$$F(z) = \frac{e_0 + e_1 z + e_2 z^2 + \ldots + e_{d-1} z^{d-1}}{1 + q_1 z + q_2 z^2 + q_3 z^3 + \ldots + q_d z^d}$$

mit

$$e_i = f_i + q_1 f_{i-1} + q_2 f_{i-2} + \ldots + q_i f_0$$

für alle $i = 0, \ldots, d-1$.

Beispiel

Zur Rekursionsgleichung

$$f_{n+4} + 5f_{n+3} - 3f_{n+2} + 2f_{n+1} - f_n = 0$$

mit $f_0 = 1, f_1 = 3, f_2 = 5, f_3 = 7$ ist die erzeugende Funktion:

$$\begin{aligned}
F(z) &= \frac{e_0 + e_1 z + e_2 z^2 + e_3 z^3}{1 + q_1 z + q_2 z^2 + q_3 z^3 + q_4 z^4} \\
&= \frac{f_0 + (f_1 + q_1 f_0)z + (f_2 + q_1 f_1 + q_2 f_0)z^2 + (f_3 + q_1 f_2 + q_2 f_1 + q_3 f_0)z^3}{1 + q_1 z + q_2 z^2 + q_3 z^3 + q_4 z^4} \\
&= \frac{1 + (3 + 5 \cdot 1)z + (5 + 5 \cdot 3 + (-3) \cdot 1)z^2 + (7 + 5 \cdot 5 + (-3) \cdot 3 + 2 \cdot 1)z^3}{1 + 5z + (-3)z^2 + 2z^3 + (-1)z^4} \\
&= \frac{1 + 8z + 17z^2 + 25z^3}{1 + 5z - 3z^2 + 2z^3 - z^4}
\end{aligned}$$

Info

Diese Formel erlaubt uns eine äquivalente Darstellung für die erzeugende Funktion $F(z) = \sum_{n=0}^{\infty} f_n \cdot z^n$ zu finden. Bevor wir die allgemeine Methode kennenlernen, kommt als nächstes ein kleines Beispiel, damit ihr euch davon überzeugen könnt, dass beide Darstellungen äquivalent sind.

Beispiel

Betrachten wir die homogene Rekursionsgleichung

$$f_{n+1} - f_n = 0 \qquad (\forall n \geq 0)$$

mit Anfangsbedingung $f_0 = 1$. Diese Rekursionsgleichung hat Lösung $f_n = 1$ und somit die erzeugende Funktion

$$F(z) = \sum_{n=0}^{\infty} 1 \cdot z^n = \sum_{n=0}^{\infty} z^n.$$

Die äquivalente Darstellung wäre:

$$F(z) = \frac{e_0}{1 + q_1 z} = \frac{1}{1 - z}.$$

Tatsächlich gilt $\sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$, denn:

$$(1 - z) \cdot \sum_{n=0}^{\infty} z^n = \sum_{n=0}^{\infty} z^n - \sum_{n=0}^{\infty} z^{n+1} = (1 + z + z^2 + z^3 + \ldots) - (z + z^2 + z^3 + \ldots) = 1.$$

Die ultimative Rechenregel für erzeugende Funktionen

Für beliebige $d \in \mathbb{N}$, $\alpha \in \mathbb{C}$ und $i \in \mathbb{N}_0$ mit $0 \leq i < d$ gilt:

$$\frac{z^i}{(1-\alpha z)^d} = \sum_{n=0}^{\infty} \binom{d+n-i-1}{d-1} \alpha^{n-i} z^n.$$

Mit dieser Regel kann man so ziemlich alle für uns relevanten erzeugenden Funktionen von Summen in Brüche und von Brüchen in Summen umwandeln.

Beispiel

$$\begin{aligned}
\frac{3}{1-3z} + \frac{2z+5}{(1-2z)^2} &= 3 \cdot \frac{1}{1-3z} + 2 \cdot \frac{z}{(1-2z)^2} + 5 \cdot \frac{1}{(1-2z)^2} \\
&= 3 \cdot \sum_{n=0}^{\infty} 3^n z^n + 2 \cdot \sum_{n=0}^{\infty} n \cdot 2^{n-1} z^n + 5 \cdot \sum_{n=0}^{\infty} (n-1) \cdot 2^n z^n \\
&= \sum_{n=0}^{\infty} \left(3 \cdot 3^n + 2 \cdot n \cdot 2^{n-1} + 5 \cdot (n-1) \cdot 2^n\right) z^n \\
&= \sum_{n=0}^{\infty} \left(3^{n+1} + (6n-5) \cdot 2^n\right) z^n
\end{aligned}$$

Methode 3

Frage: Wie löst man lineare homogene Rekursionsgleichungen mit erzeugenden Funktionen?
Methode: Gegeben sei die Rekursionsgleichung

$$f_{n+d} + q_1 f_{n+d-1} + q_2 f_{n+d-2} + \ldots + q_d f_n = 0 \qquad (\forall n \geq 0)$$

mit Anfangsbedingungen $f_0, f_1, \ldots, f_{d-1}$.

1. Erzeugende Funktion $F(z)$ aufstellen:

$$F(z) = \frac{e_0 + e_1 z + e_2 z^2 + \ldots + e_{d-1} z^{d-1}}{1 + q_1 z + q_2 z^2 + q_3 z^3 + \ldots + q_d z^d}$$

   mit $e_i = f_i + q_1 f_{i-1} + q_2 f_{i-2} + \ldots + q_i f_0$ für alle $i = 0, \ldots, d-1$.

2. Seien $\alpha_1, \ldots, \alpha_k$ die Nullstellen des charakteristischen Polynoms und $d_1, \ldots, d_k$ ihre Vielfachheiten. Mit Partialbruchzerlegung (über $\mathbb{C}$) Polynome $g_1, \ldots, g_k$ mit $\text{grad}(g_i) < d_i$ finden, so dass gilt:

$$F(z) = \frac{g_1(z)}{(1-\alpha_1 z)^{d_1}} + \frac{g_2(z)}{(1-\alpha_2 z)^{d_2}} + \ldots + \frac{g_k(z)}{(1-\alpha_k z)^{d_k}}$$

Methode 3

3. Die einzelnen Brüchen, analog zum Beispiel auf Folie 1552, in Summen umwandeln und f_n rauslesen:

$$F(z) = \sum_{n=0}^{\infty} (\underbrace{p_1(n)\alpha_1^n + p_2(n)\alpha_2^n + \ldots + p_k(n)\alpha_k^n}_{f_n}) z^n.$$

Hierbei sind $p_1(n), \ldots, p_k(n)$ wieder Polynome mit Unbekannter n.

Beispiel

Aufgabe: Löse die lineare homogene Rekursionsgleichung

$$f_{n+2} - 5f_{n+1} + 6f_n = 0 \qquad (\forall n \geq 0)$$

mit Anfangsbedingungen $f_0 = 1$ und $f_1 = 4$.
Lösung:

1. Die erzeugende Funktion ist:
$$F(z) = \frac{1-z}{1-5z+6z^2}$$
2. Partialbruchzerlegung liefert:
$$F(z) = \frac{-1}{1-2z} + \frac{2}{1-3z}$$
3. Mit Folie 1551 bekommt man:
$$F(z) = (-1) \cdot \sum_{n=0}^{\infty} 2^n z^n + 2 \cdot 2 \cdot \sum_{k=0}^{\infty} 3^n z^n = \sum_{n=0}^{\infty} (-2^n + 2 \cdot 3^n) z^n$$

   Daraus folgt:
$$f_n = -2^n + 2 \cdot 3^n$$

Welche Lösung besitzen folgende homogene Rekursionsgleichungen?

1. $f_0 = 3$ und $f_{n+1} - f_n = 0$ für alle $n \geq 0$,
2. $f_0 = 1$ und $f_{n+1} - 2f_n = 0$ für alle $n \geq 0$,
3. $f_0 = -2$ und $f_{n+1} + 3f_n = 0$ für alle $n \geq 0$,
4. $f_0 = 0$, $f_1 = 1$ und $f_{n+2} - 3f_{n+1} + 2f_n = 0$ für alle $n \geq 0$,
5. $f_0 = 1$, $f_1 = 4$ und $f_{n+2} - 5f_{n+1} + 6f_n = 0$ für alle $n \geq 0$.

Benutze die Methode aus Folie 1553.

Antworten (kompakt)

1. $F(z) = \frac{3}{1-z} = \sum_{n=0}^{\infty} 3z^n$
   $\rightsquigarrow f_n = 3.$
2. $F(z) = \frac{1}{1-2z} = \sum_{n=0}^{\infty} (2z)^n = \sum_{n=0}^{\infty} 2^n z^n$
   $\rightsquigarrow f_n = 2^n.$
3. $F(z) = \frac{-2}{1+3z} = \sum_{n=0}^{\infty} -2 \cdot (-3)^n z^n$
   $\rightsquigarrow f_n = -2 \cdot (-3)^n.$
4. $F(z) = \frac{z}{1-3z+2z^2} = \frac{-1}{1-z} + \frac{1}{1-2z} = \sum_{n=0}^{\infty} (-1 + 2^n) z^n$
   $\rightsquigarrow f_n = -1 + 2^n.$
5. $F(z) = \frac{1-z}{1-5z+6z^2} = \frac{-1}{1-2z} + \frac{2}{1-3z} = \sum_{k=0}^{\infty} (-2^n + 2 \cdot 3^n) z^n$
   $\rightsquigarrow f_n = -2^n + 2 \cdot 3^n.$

Methode 4

Frage: Wie löst man lineare inhomogene Rekursionsgleichungen mit erzeugenden Funktionen?
Methode: Gegeben sei die Rekursionsgleichung

$$f_{n+d} + q_1 f_{n+d-1} + q_2 f_{n+d-2} + \ldots + q_d f_n = s_n \qquad (\forall n \geq 0)$$

mit Anfangsbedingungen $f_0, f_1, \ldots, f_{d-1}$

1. lineare homogene Rekursionsgleichung definieren mit:

   $$h_{n+d} + q_1 h_{n+d-1} + q_2 h_{n+d-2} + \ldots + q_d h_n = 0 \qquad (\forall n \geq 0)$$

   und Anfangsbedingungen $h_0 = f_0, h_1 = f_1, \ldots, h_{d-1} = f_{d-1}$ und h_n mit Methode 1 oder Methode 3 lösen.
2. Folge p_n mit folgender erzeugenden Funktion $P(z)$ definieren:

   $$P(z) = \frac{z^d \cdot \sum_{n=0}^{\infty} s_n z^n}{1 + q_1 z + q_2 z^2 + \ldots + q_d z^d}$$

3. Die Summe $\sum_{n=0}^{\infty} s_n z^n$ mit Folie 1551 in ein Bruch umwandeln und analog zur Methode 3 p_n mit $P(z)$ lösen.
4. $f_n = h_n + p_n$ setzen.

Beispiel

Aufgabe: Löse die lineare inhomogene Rekursionsgleichung

$$f_{n+1} + f_n = 3^n \qquad (\forall n \geq 0)$$

mit Anfangsbedingung $f_0 = 1$.

Beispiel

Lösung:

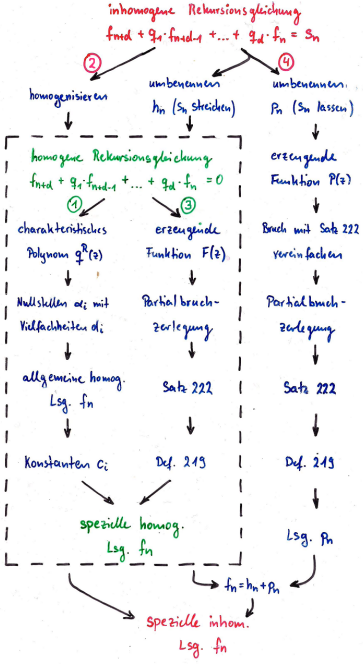
1. Man definiert
$$h_{n+1} + h_n = 0 \qquad (\forall n \geq 0)$$
mit Anfangsbedingung $h_0 = f_0 = 1$ und bekommt als Lösung: $h_n = (-1)^n$.
2. Die Erzeugende Funktion $P(z)$ von p ist:
$$P(z) = \frac{z \cdot \sum_{n=0}^{\infty} 3^n z^n}{1+z}$$
3. Mit Folie 1551, Partialbruchzerlegung und nochmal Folie 1551 bekommt man:
$$P(z) \overset{F.1551}{=} \frac{z \cdot \frac{1}{1-3z}}{1+z} = \frac{z}{(1-3z)(1+z)} \overset{\text{PBZ}}{=} \frac{\frac{1}{4}}{1-3z} + \frac{-\frac{1}{4}}{1+z}$$
$$\overset{F.1551}{=} \sum_{n=0}^{\infty} \frac{1}{4} \cdot 3^n z^n + \sum_{n=0}^{\infty} -\frac{1}{4} \cdot (-1)^n z^n = \sum_{n=0}^{\infty} \left(\frac{1}{4}(3^n - (-1)^n) \right) z^n$$
4. Daraus folgt: $f_n = h_n + p_n = (-1)^n + \frac{1}{4}(3^n - (-1)^n) = \frac{1}{4}\left(3(-1)^n + 3^n\right)$.

Überblick

Wir haben insgesamt 4 Methoden kennengelernt:

1. Mit Methode 1 lassen sich lineare homogene Rekursionsgleichungen lösen.
2. Mit Methode 2 kann man lineare inhomogene Rekursionsgleichungen in lineare homogene Rekursionsgleichungen überbringen.
3. Mit Methode 3 lassen sich auch lineare homogene Rekursionsgleichungen lösen. Sie ist aber nicht ganz so einfach wie die erste!
4. Mit Methode 4 lassen sich lineare inhomogene Rekursionsgleichungen lösen. Sie ist sehr schwierig, sogar schwieriger als die ersten zwei Methoden zusammen!

Graphisch:


inhomogene Rekursionsgleichung
$f_{n+d} + g_{d-1} \cdot f_{n+d-1} + \ldots + g_0 \cdot f_n = s_n$
2
4
homogenisieren
umbenennen
h_n (s_n streichen)
umbenennen
p_n (s_n lassen)
homogene Rekursionsgleichung
$f_{n+d} + g_{d-1} \cdot f_{n+d-1} + \ldots + g_0 \cdot f_n = 0$
1
3
erzeugende Funktion $P(z)$
charakteristisches Polynom $g^R(z)$
erzeugende Funktion $F(z)$
Bruch mit Satz 222 vereinfachen
Nullstellen α_i mit Vielfachheiten d_i
Partialbruchzerlegung
Partialbruchzerlegung
allgemeine homog. Lsg. f_n
Satz 222
Satz 222
Konstanten c_i
Def. 219
Def. 219
spezielle homog. Lsg. f_n
Lsg. p_n
$f_n = h_n + p_n$
spezielle inhom. Lsg. f_n

Gegeben sei folgende nichtlineare Rekursionsgleichung:

$$\frac{f_{n+2} \cdot f_{n+1}}{(f_n)^2} = 1 \qquad (\forall n \geq 0)$$

mit Anfangsbedingungen $f_0 = 8$ und $f_1 = 1$.

Welchen geschlossenen Ausdruck besitzt f_n?

Hinweis: Betrachte zunächste die Folge $(h_n)_{n \geq 0}$ mit $h_n := \log_2(f_n)$.

Wir rechnen:

$$\begin{aligned}\frac{f_{n+2}\cdot f_{n+1}}{(f_n)^2}=1 \qquad &\iff \log_2\left(\frac{f_{n+2}\cdot f_{n+1}}{(f_n)^2}\right)=\log_2(1)\\ &\iff \log_2(f_{n+2}\cdot f_{n+1})-\log_2((f_n)^2)=0\\ &\iff \log_2(f_{n+2})+\log_2(f_{n+1})-2\log_2(f_n)=0\end{aligned}$$

Daraus folgt die Rekursionsgleichung

$$h_{n+2}+h_{n+1}-2h_n=0 \qquad (\forall n\geq 0)$$

mit Anfangsbedingungen $h_0=\log_2(8)=3$ und $h_1=\log_2(1)=0$.
Für h_n gilt:

$$\begin{aligned}&q^R(z)=z^2+z-2=(z-1)(z+2)\\ \rightsquigarrow\ &h_n=c_0\cdot 1^n+c_1\cdot(-2)^n=2\cdot 1^n+1\cdot(-2)^n=2+(-2)^n\end{aligned}$$

Daraus folgt $f_n=2^{h_n}=2^{2+(-2)^n}$.

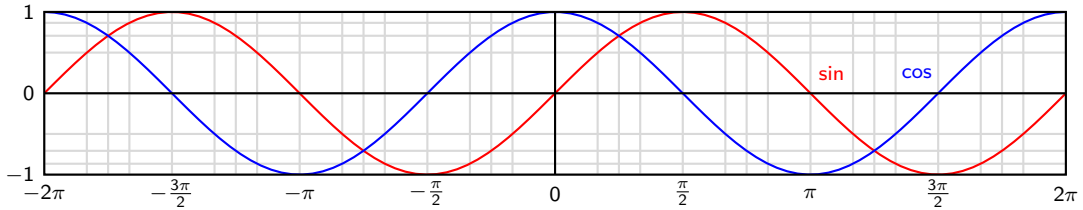
Themenübersicht

Sinus und Kosinus

Wertetabelle:

Winkel	$0°$	$30°$	$45°$	$60°$	$90°$	$120°$	$135°$	$150°$	$180°$	$210°$	$225°$	$240°$	$270°$	$300°$	$315°$	$330°$	$360°$
φ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	$\frac{2\pi}{3}$	$\frac{3\pi}{4}$	$\frac{5\pi}{6}$	π	$\frac{7\pi}{6}$	$\frac{5\pi}{4}$	$\frac{4\pi}{3}$	$\frac{3\pi}{2}$	$\frac{5\pi}{3}$	$\frac{7\pi}{4}$	$\frac{11\pi}{6}$	2π
$\sin(\varphi)$	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	1	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{1}{\sqrt{2}}$	$-\frac{\sqrt{3}}{2}$	-1	$-\frac{\sqrt{3}}{2}$	$-\frac{1}{\sqrt{2}}$	$-\frac{1}{2}$	0
$\cos(\varphi)$	1	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	0	$-\frac{1}{2}$	$-\frac{1}{\sqrt{2}}$	$-\frac{\sqrt{3}}{2}$	-1	$-\frac{\sqrt{3}}{2}$	$-\frac{1}{\sqrt{2}}$	$-\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	1

Graphen:

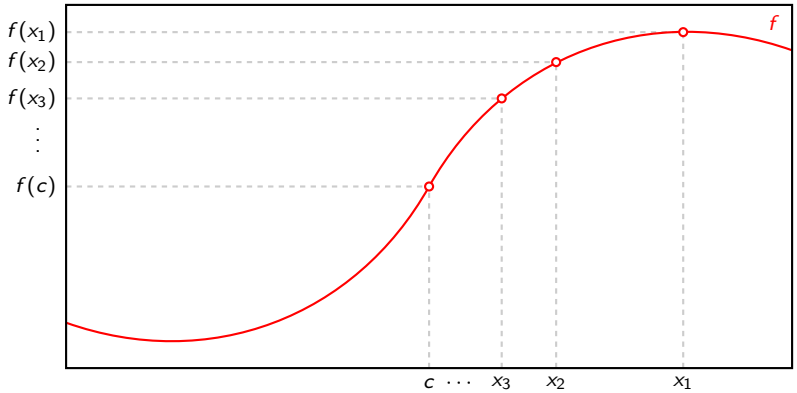


Themenübersicht

Definition: Folgencharakterisierung von Stetigkeit

Sei $D \subseteq \mathbb{R}$. Eine Funktion $f : D \to \mathbb{R}$ heißt stetig in $c \in D$, falls gilt:

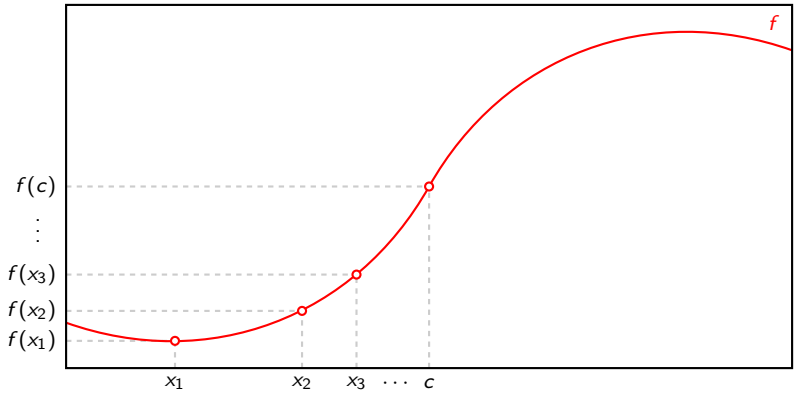
$$\forall (x_n)_{n\in\mathbb{N}} \text{ in } D\colon \lim_{n\to\infty} x_n = c \implies \lim_{n\to\infty} f(x_n) = f(c).$$



Definition: Folgencharakterisierung von Stetigkeit

Sei $D \subseteq \mathbb{R}$. Eine Funktion $f : D \to \mathbb{R}$ heißt stetig in $c \in D$, falls gilt:

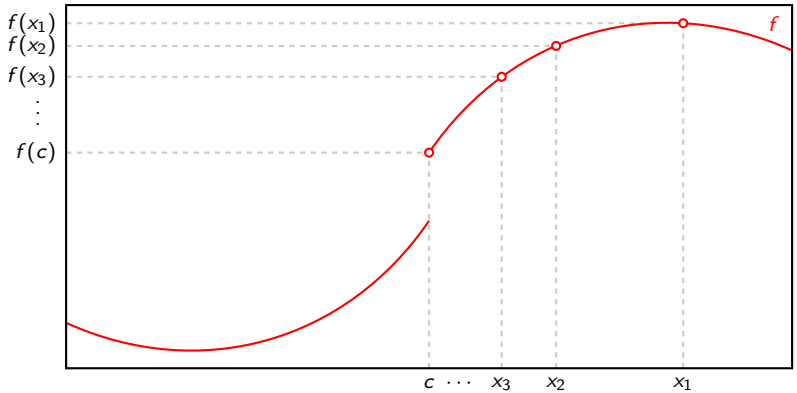
$$\forall (x_n)_{n\in\mathbb{N}} \text{ in } D\colon \lim_{n\to\infty} x_n = c \implies \lim_{n\to\infty} f(x_n) = f(c).$$



Definition: Folgencharakterisierung von Unstetigkeit

Sei $D \subseteq \mathbb{R}$. Eine Funktion $f : D \to \mathbb{R}$ heißt unstetig in $c \in D$, falls gilt:

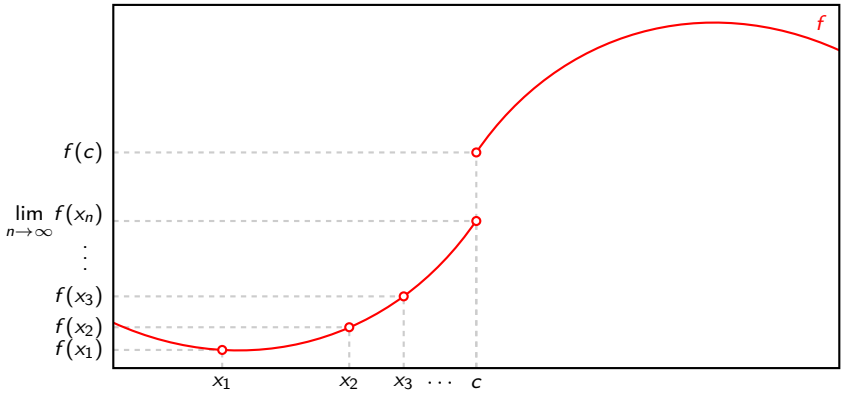
$$\exists (x_n)_{n\in\mathbb{N}} \text{ in } D\colon \lim_{n\to\infty} x_n = c \wedge \lim_{n\to\infty} f(x_n) \neq f(c).$$



Definition: Folgencharakterisierung von Unstetigkeit

Sei $D \subseteq \mathbb{R}$. Eine Funktion $f : D \to \mathbb{R}$ heißt unstetig in $c \in D$, falls gilt:

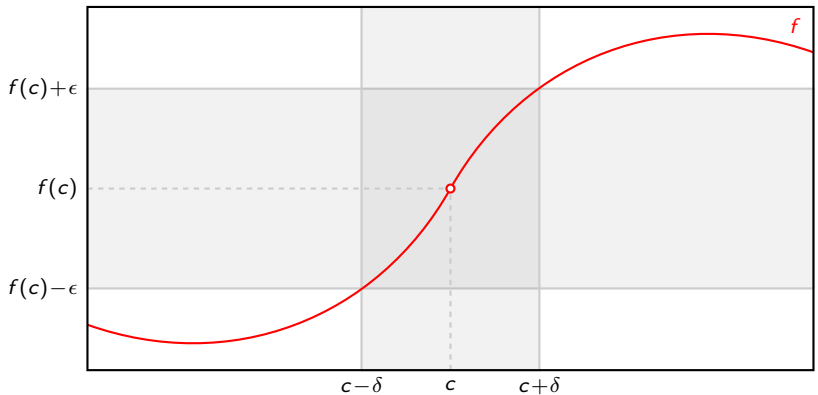
$$\exists (x_n)_{n\in\mathbb{N}} \text{ in } D\colon \lim_{n\to\infty} x_n = c \wedge \lim_{n\to\infty} f(x_n) \neq f(c).$$



Satz: ϵ-δ-Charakterisierung von Stetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann stetig in $c \in D$, wenn gilt:

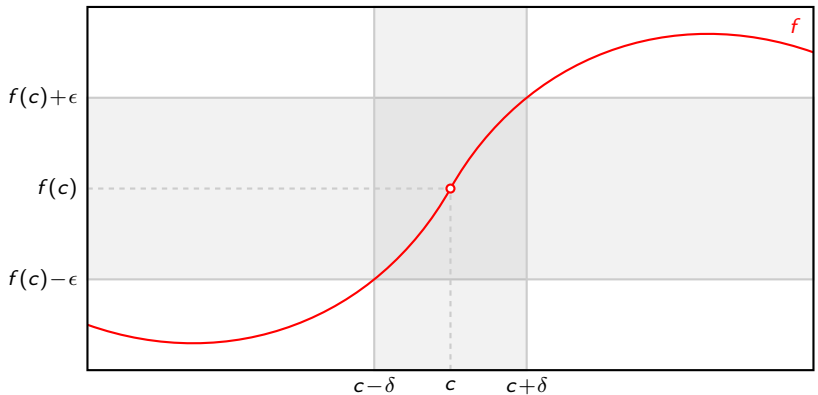
$$\forall \epsilon > 0 \colon \exists \delta > 0 \colon \forall x \in D \colon |x - c| < \delta \implies |f(x) - f(c)| < \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Stetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann stetig in $c \in D$, wenn gilt:

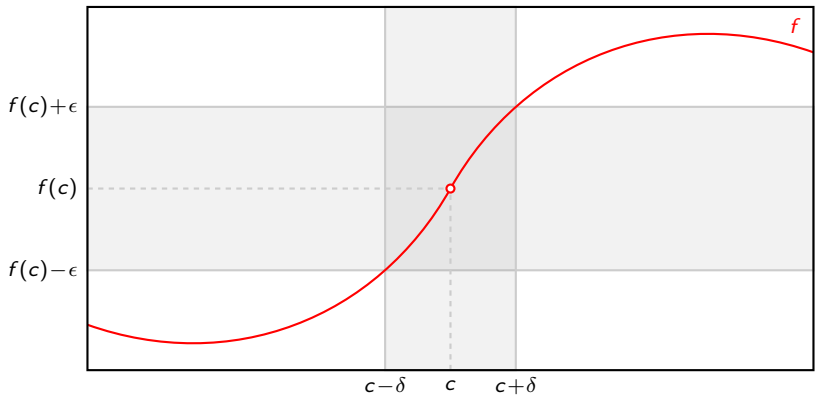
$$\forall \epsilon > 0 \colon \exists \delta > 0 \colon \forall x \in D \colon |x - c| < \delta \implies |f(x) - f(c)| < \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Stetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann stetig in $c \in D$, wenn gilt:

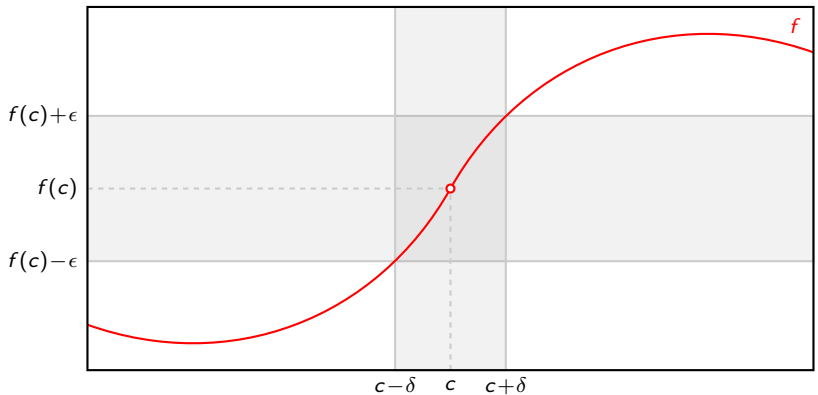
$$\forall \epsilon > 0 \colon \exists \delta > 0 \colon \forall x \in D \colon |x - c| < \delta \implies |f(x) - f(c)| < \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Stetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann stetig in $c \in D$, wenn gilt:

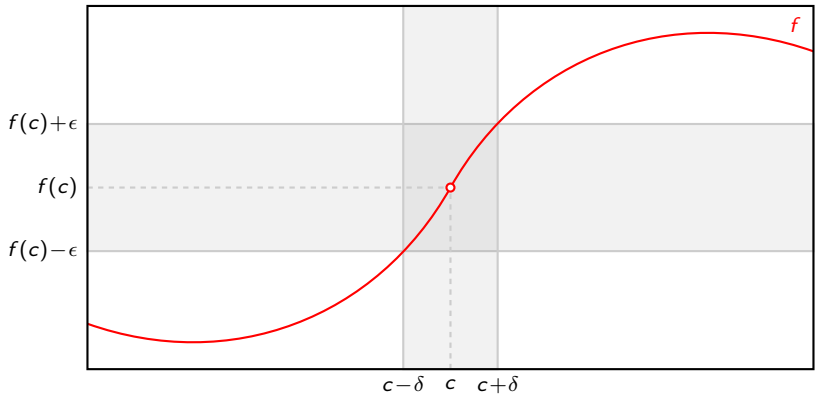
$$\forall \epsilon > 0 \colon \exists \delta > 0 \colon \forall x \in D \colon |x - c| < \delta \implies |f(x) - f(c)| < \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Stetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann stetig in $c \in D$, wenn gilt:

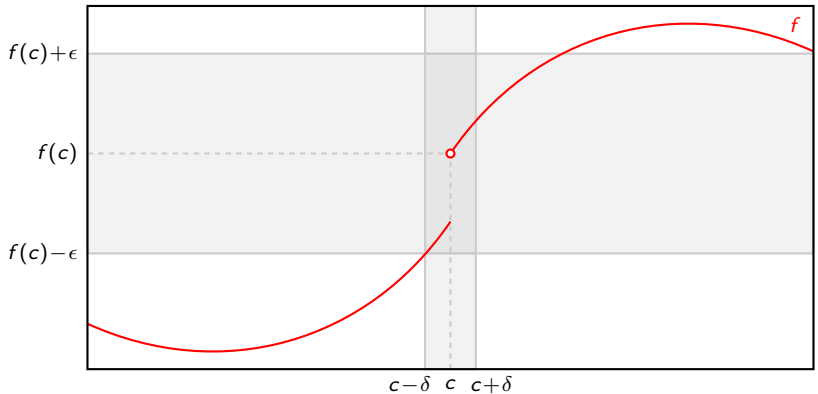
$$\forall \epsilon > 0 \colon \exists \delta > 0 \colon \forall x \in D \colon |x - c| < \delta \implies |f(x) - f(c)| < \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Unstetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann unstetig in $c \in D$, wenn gilt:

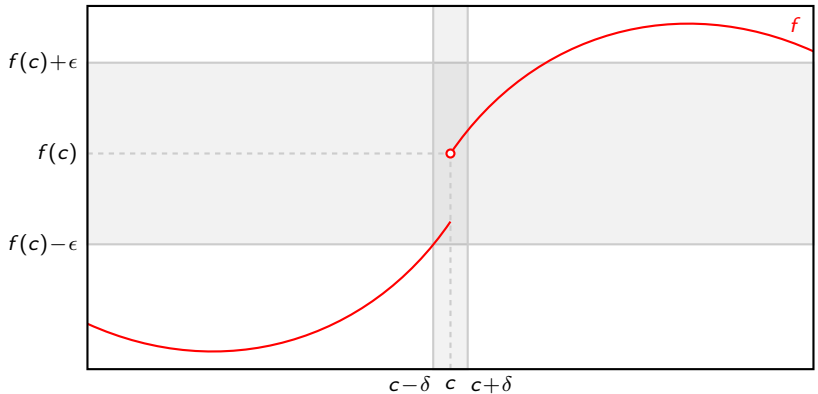
$$\exists \epsilon > 0 \colon \forall \delta > 0 \colon \exists x \in D \colon |x - c| < \delta \wedge |f(x) - f(c)| \geq \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Unstetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann unstetig in $c \in D$, wenn gilt:

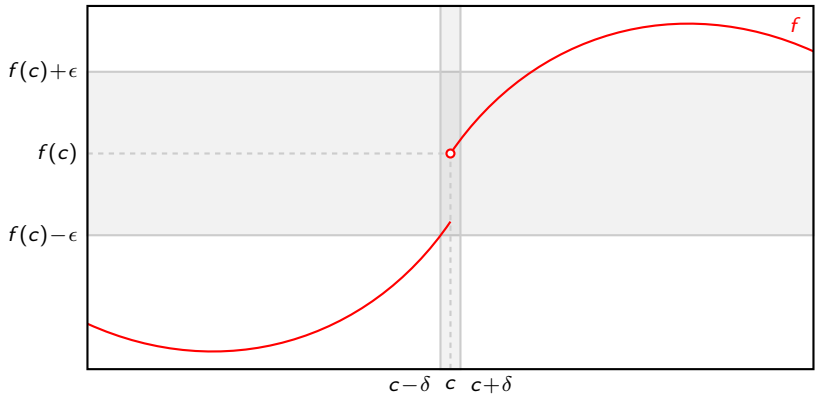
$$\exists \epsilon > 0 \colon \forall \delta > 0 \colon \exists x \in D \colon |x - c| < \delta \wedge |f(x) - f(c)| \geq \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Unstetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann unstetig in $c \in D$, wenn gilt:

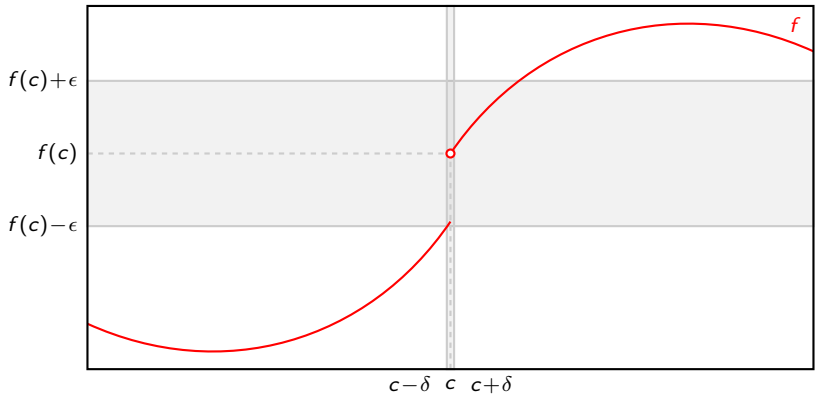
$$\exists \epsilon > 0 \colon \forall \delta > 0 \colon \exists x \in D \colon |x - c| < \delta \wedge |f(x) - f(c)| \geq \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Unstetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann unstetig in $c \in D$, wenn gilt:

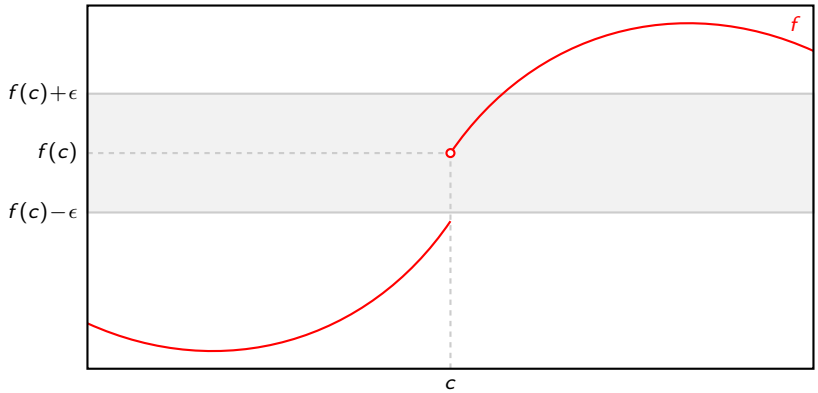
$$\exists \epsilon > 0 \colon \forall \delta > 0 \colon \exists x \in D \colon |x - c| < \delta \wedge |f(x) - f(c)| \geq \epsilon.$$



Satz: ϵ-δ-Charakterisierung von Unstetigkeit

Sei $D \subseteq \mathbb{R}$. $f : D \to \mathbb{R}$ ist genau dann unstetig in $c \in D$, wenn gilt:

$$\exists \epsilon > 0 \colon \forall \delta > 0 \colon \exists x \in D \colon |x - c| < \delta \wedge |f(x) - f(c)| \geq \epsilon.$$



Funktionsgrenzwerte

Für $D \subseteq \mathbb{R}$, $f : D \to \mathbb{R}$ und $b, c \in \mathbb{R} \cup \{-\infty, \infty\}$ gilt $\lim_{x \to c} f(x) = b$ genau dann, wenn gilt:

$$\forall (x_n)_{n \in \mathbb{N}} \text{ in } D\colon \lim_{n \to \infty} x_n = c \implies \lim_{n \to \infty} f(x_n) = b.$$

Um zu zeigen, dass $\lim_{x \to c} f(x)$ nicht existiert, reicht es zwei Folgen $(x_n)_{n \in \mathbb{N}}$ und $(y_n)_{n \in \mathbb{N}}$ zu finden mit $\lim_{n \to \infty} x_n = \lim_{n \to \infty} y_n$ und $\lim_{n \to \infty} f(x_n) \neq \lim_{n \to \infty} f(y_n)$.

„$-\infty = -\infty$“ und „$\infty = \infty$“ sind auch ok!

Zwischenwertsatz

Seien $a, b \in \mathbb{R}$ reelle Zahlen mit $a \leq b$ und $f\colon [a,b] \to \mathbb{R}$ eine stetige Funktion. Dann gilt:

$$\forall y \in [\min\{f(a), f(b)\}, \max\{f(a), f(b)\}]\colon \exists x \in [a,b]\colon f(x) = y.$$

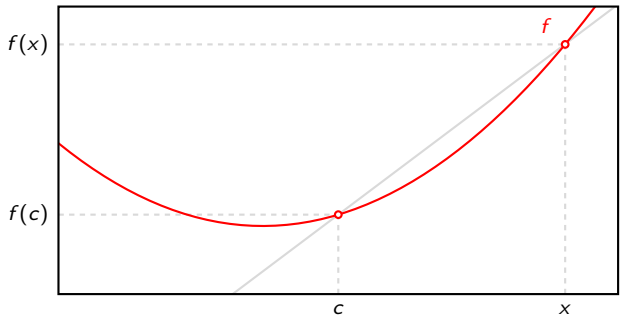
Themenübersicht

Ableitung

Sei $I \subseteq \mathbb{R}$ ein Intervall. Die Funktion $f : I \to \mathbb{R}$ heißt differenzierbar im Punkt $c \in I$, falls

$$f'(c) = \lim_{x \to c} \frac{f(x) - f(c)}{x - c}$$

existiert. Graphisch:

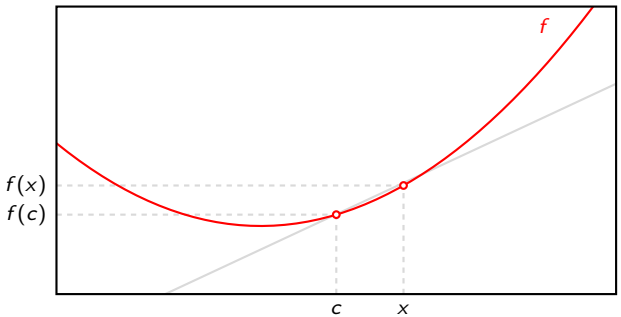


Ableitung

Sei $I \subseteq \mathbb{R}$ ein Intervall. Die Funktion $f : I \to \mathbb{R}$ heißt differenzierbar im Punkt $c \in I$, falls

$$f'(c) = \lim_{x \to c} \frac{f(x) - f(c)}{x - c}$$

existiert. Graphisch:

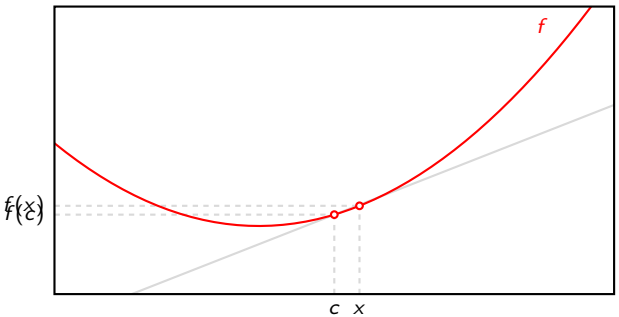


Ableitung

Sei $I \subseteq \mathbb{R}$ ein Intervall. Die Funktion $f : I \to \mathbb{R}$ heißt differenzierbar im Punkt $c \in I$, falls

$$f'(c) = \lim_{x \to c} \frac{f(x) - f(c)}{x - c}$$

existiert. Graphisch:

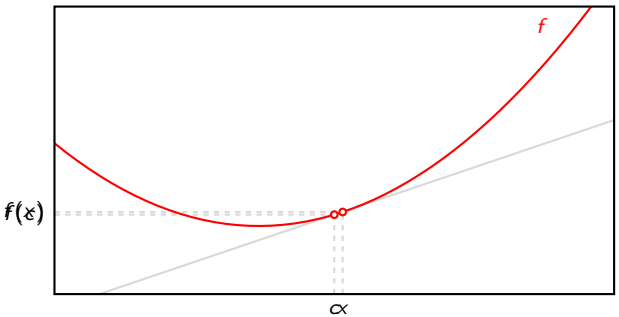


Ableitung

Sei $I \subseteq \mathbb{R}$ ein Intervall. Die Funktion $f : I \to \mathbb{R}$ heißt differenzierbar im Punkt $c \in I$, falls

$$f'(c) = \lim_{x \to c} \frac{f(x) - f(c)}{x - c}$$

existiert. Graphisch:

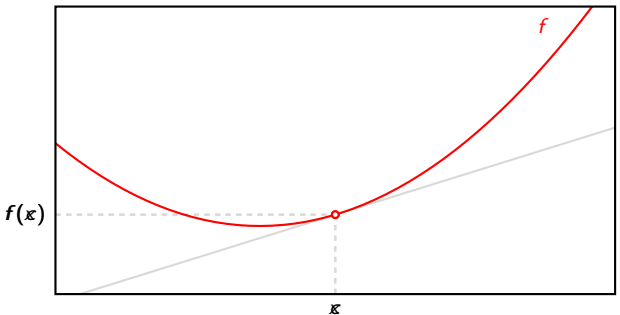


Ableitung

Sei $I \subseteq \mathbb{R}$ ein Intervall. Die Funktion $f : I \to \mathbb{R}$ heißt differenzierbar im Punkt $c \in I$, falls

$$f'(c) = \lim_{x \to c} \frac{f(x) - f(c)}{x - c}$$

existiert. Graphisch:



Ableitungsregeln

Für auf ein Intervall $I \subseteq \mathbb{R}$ differenzierbare Funktionen $f, g\colon I \to \mathbb{R}$ und $c \in \mathbb{R}$ gelten folgende Ableitungsregeln.

$f(x)$	c	x^c	$\frac{1}{x}$	e^x	$\sin(x)$	$\cos(x)$	$\ln(x)$
$f'(x)$	0	cx^{c-1}	$-\frac{1}{x^2}$	e^x	$\cos(x)$	$-\sin(x)$	$\frac{1}{x}$

- Summenregel:

$$(f(x) + g(x))' = f'(x) + g'(x).$$

  Beispiel: $(x^3 + x)' = 3x^2 + 1$.

- Faktorregel:

$$(c \cdot f(x))' = c \cdot f'(x).$$

  Beispiel: $(5x^2)' = 5 \cdot (x^2)' = 5 \cdot 2x = 10x$.

Ableitungsregeln

- Produktregel:
$$(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x).$$
Beispiel: $(\sin(x)\cos(x))' = \sin'(x)\cos(x) + \sin(x)\cos'(x) = (\cos(x))^2 - (\sin(x))^2$.

- Quotientenregel:
$$\left(\frac{f(x)}{g(x)}\right)' = \frac{f'(x) \cdot g(x) - f(x) \cdot g'(x)}{g(x)^2}.$$
Beispiel: $\left(\frac{\ln(x)}{x^2}\right)' = \frac{\ln'(x)x^2 - \ln(x)(x^2)'}{(x^2)^2} = \frac{x - \ln(x)2x}{x^4} = \frac{1-2\ln(x)}{x^3}$.

- Kettenregel:
$$(f(g(x)))' = f'(g(x)) \cdot g'(x).$$
Beispiel: $\left(\sin\left(x^2\right)\right)' = \sin'\left(x^2\right) \cdot \left(x^2\right)' = \cos\left(x^2\right) \cdot 2x$.

Infos

- Wir benutzen die übliche Notation f' für die Ableitung $\frac{\mathrm{d}f}{\mathrm{d}x}$ und $f(x)$ für eine Funktion f.
- Die Definition von Potenzen ($a^b = e^{b\ln(a)}$) hilft sehr bei Funktionen der Form $f(x) = g(x)^{h(x)}$. Zum Beispiel:

$$\begin{aligned}(x^x)' &= \left(e^{x\ln x}\right)' \\ &= e^{x\ln x}(x\ln x)' \\ &= e^{x\ln x}(x'\ln x + x(\ln x)') \\ &= e^{x\ln x}(\ln x + 1) \\ &= x^x(\ln x + 1).\end{aligned}$$

Wer das Ableiten in der Schule nicht richtig gelernt bzw. wieder vergessen hat, kann das mit den Aufgaben 1-7 in

`www.poenitz-[]net.de/Mathematik/5.Analysis/5.4.A.Ableitungsregeln.pdf`

nachholen. Sie sind vom Schwierigkeitsgrad her perfekt für Einsteiger!

Zusatzaufgaben für Übermotivierte

1. Sei $f(x) = e^{2x+1}$. Zeige für alle $n \in \mathbb{N}_0$: $f^{(n)}(x) = 2^n e^{2x+1}$.
2. Sei $f(x) = (e^x - 1)^2 - 1$. Zeige für alle $n \in \mathbb{N}_0$: $f^{(n)}(x) = 2^n e^{2x} - 2e^x$.
3. Sei $f(x) = \frac{1}{x+1}$. Zeige für alle $n \in \mathbb{N}_0$: $f^{(n)}(x) = (-1)^n \cdot \frac{n!}{(x+1)^{n+1}}$.

Infos:

- Benutze vollständige Induktion.
- Für die n-te Ableitung $f^{(n)}$ einer Funktion f gilt: $f^{(0)} = f$ und $f^{(n+1)} = \left(f^{(n)}\right)'$.

1. Sei $f(x) = e^{2x+1}$. Zeige für alle $n \in \mathbb{N}_0$: $f^{(n)}(x) = 2^n e^{2x+1}$.

   IA: $f^{(0)}(x) = 2^0 e^{2x+1} = e^{2x+1} = f(x)$.

   IS: Sei $n \in \mathbb{N}_0$ beliebig mit $f^{(n)}(x) = 2^n e^{2x+1}$. Dann folgt:

$$f^{(n+1)}(x) = \left(f^{(n)}(x)\right)' \overset{\text{IV}}{=} \left(2^n e^{2x+1}\right)' = 2^n (2x+1)' e^{2x+1} = 2^{n+1} e^{2x+1}.$$

2. Sei $f(x) = (e^x - 1)^2 - 1$. Zeige für alle $n \in \mathbb{N}_0$: $f^{(n)}(x) = 2^n e^{2x} - 2e^x$.

   IA: $f^{(0)}(x) = 2^0 e^{2x} - 2e^x = e^{2x} - 2e^x = (e^x - 1)^2 - 1 = f(x)$.

   IS: Sei $n \in \mathbb{N}_0$ beliebig mit $f^{(n)}(x) = 2^n e^{2x} - 2e^x$. Dann folgt:

$$f^{(n+1)}(x) = \left(f^{(n)}(x)\right)' \overset{\text{IV}}{=} \left(2^n e^{2x} - 2e^x\right)' = 2^n e^{2x}(2x)' - 2e^x = 2^{n+1} e^{2x} - 2e^x.$$

3. Sei $f(x) = \frac{1}{x+1}$. Zeige für alle $n \in \mathbb{N}_0$: $f^{(n)}(x) = (-1)^n \cdot \frac{n!}{(x+1)^{n+1}}$.

   IA: $f^{(0)}(x) = (-1)^0 \cdot \frac{0!}{(x+1)^{0+1}} = \frac{1}{x+1} = f(x)$.

   IS: Sei $n \in \mathbb{N}_0$ beliebig mit $f^{(n)}(x) = (-1)^n \cdot \frac{n!}{(x+1)^{n+1}}$. Dann folgt:

$$\begin{aligned} f^{(n+1)}(x) &= \left(f^{(n)}(x)\right)' \overset{\text{IV}}{=} \left((-1)^n \cdot \frac{n!}{(x+1)^{n+1}}\right)' \\ &= \left((-1)^n \cdot n! \cdot (x+1)^{-(n+1)}\right)' \\ &= (-1)^n \cdot n! \cdot (-(n+1)) \cdot (x+1)^{-(n+2)} \cdot (x+1)' \\ &= (-1)^n \cdot n! \cdot (-1) \cdot (n+1) \cdot (x+1)^{-(n+2)} \\ &= (-1)^{n+1} \cdot \frac{(n+1)!}{(x+1)^{n+2}}. \end{aligned}$$

Injektivität, Surjektivität und Bijektivität

Für eine beliebige Funktion $f\colon A \to B$ gilt:

$$
\begin{array}{lll}
f \text{ injektiv} & \iff & \text{Für jedes } y \in B \text{ gibt es höchstens ein } x \in A \text{ mit } f(x) = y. \\
f \text{ surjektiv} & \iff & \text{Für jedes } y \in B \text{ gibt es mindestens ein } x \in A \text{ mit } f(x) = y. \\
f \text{ bijektiv} & \iff & \text{Für jedes } y \in B \text{ gibt es genau ein } x \in A \text{ mit } f(x) = y. \\
& \iff & f \text{ injektiv und surjektiv.}
\end{array}
$$

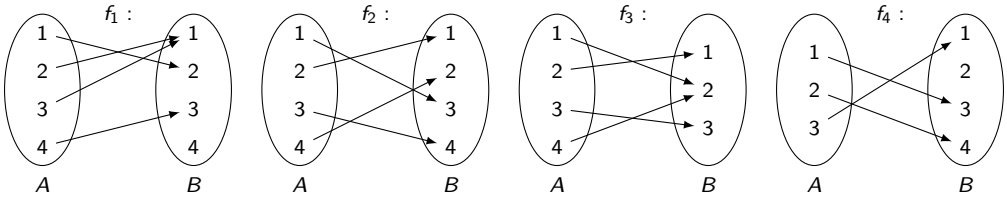
Falls f differenzierbar ist, dann gilt:

$$
\begin{array}{lll}
f'(x) > 0 \text{ für alle inneren Punkte } x \in A & \implies & f \text{ injektiv} \\
f'(x) < 0 \text{ für alle inneren Punkte } x \in A & \implies & f \text{ injektiv}
\end{array}
$$

falls f stetig ist, dann kann man oft die Surjektivität mit dem Zwischenwertsatz beweisen.

Einfache Beispiele

Seien $f_1, f_2, f_3, f_4 \colon A \to B$ folgende Funktionen.



- f_1 ist weder injektiv noch surjektiv.
- f_2 ist injektiv und surjektiv, also bijektiv.
- f_3 ist surjektiv, aber nicht injektiv.
- f_4 ist injektiv, aber nicht surjektiv.

Mehr Beispiele

.

- Die Funktion $f\colon \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$ ist nicht injetiv, weil es zwei $x \in \mathbb{R}$ gibt mit $f(x) = 1$, nämlich $x = -1$ und $x = 1$. Sie ist auch nicht surjektiv, weil es kein $x \in \mathbb{R}$ gibt mit $f(x) = -1$.
- Die Funktion $f\colon \mathbb{R} \to \mathbb{R}$ mit $f(x) = 2x + 5$ ist bijektiv, weil es für jedes $y \in \mathbb{R}$ genau ein $x \in \mathbb{R}$ mit $f(x) = y$ gibt, nämlich $x = \frac{y-5}{2}$. Dies folgt aus der Äquivalenz

$$2x + 5 = y \quad \iff \quad x = \frac{y-5}{2}.$$

Welche Eigenschaften besitzen folgende Funktionen $f_1, f_2, f_3, f_4 \colon \mathbb{R} \to \mathbb{R}$?

- $f_1(x) = |x|$.
- $f_2(x) = \sin x$.
- $f_3(x) = e^x$.
- $f_4(x) = x^3$.

Begründe deine Antworten ganz kurz!

- f_1 ist nicht injektiv, da $|-1| = 1 = |1|$. Wegen $|x| \geq 0$ ist f_1 auch nicht surjektiv, da es kein $x \in \mathbb{R}$ gibt mit $|x| = -1$.
- f_2 ist nicht injektiv, da $\sin(0) = 0 = \sin(2\pi)$. Wegen $-1 \leq \sin x \leq 1$ ist f_2 auch nicht surjektiv, da es kein $x \in \mathbb{R}$ gibt mit $\sin x = 2$.
- f_3 ist injektiv, denn für alle $x \in \mathbb{R}$ gilt: $(e^x)' = e^x > 0$. f_3 ist nicht surjektiv, da es kein $x \in \mathbb{R}$ gibt mit $e^x = 0$.
- f_4 ist bijektiv, weil es für jedes $y \in \mathbb{R}$ genau ein $x \in \mathbb{R}$ mit $x^3 = y$ gibt, nämlich

$$x = \begin{cases} \sqrt[3]{y} & \text{falls } y \geq 0 \\ -\sqrt[3]{-y} & \text{falls } y < 0. \end{cases}$$

Umkehrfunktionen

Ist $f\colon A \to B$ bijektiv, dann besitzt sie eine eindeutige Umkehrfunktion $f^{-1}\colon B \to A$ mit

$$f(a) = b \quad \Longleftrightarrow \quad f^{-1}(b) = a$$

für alle $a \in A$ und alle $b \in B$. Daraus folgt:

$$f^{-1}(f(a)) = a \quad (\forall a \in A) \qquad \text{und} \qquad f(f^{-1}(b)) = b \quad (\forall b \in B).$$

Merkt euch bitte diese 3 Eigenschaften oder schreibt sie euch auf!

Infos

Es gilt $(f^{-1})^{-1} = f$, d.h. wenn f^{-1} die Umkehrfunktion von f ist, dann ist f automatisch die Umkehrfunktion von f^{-1}. Man sagt auch, dass f und f^{-1} invers zueinander sind.

Beispiel

Die Umkehrfunktion von $f\colon \mathbb{R} \to \mathbb{R}^+$ mit $f(x) = e^x$ ist $f^{-1}\colon \mathbb{R}^+ \to \mathbb{R}$ mit $f^{-1}(x) = \ln x$.

Es gilt

$$e^a = b \quad \Longleftrightarrow \quad \ln b = a,$$

$\ln(e^a) = a$ und $e^{\ln b} = b$ für alle $a \in \mathbb{R}$ und alle $b \in \mathbb{R}^+$.

Themenübersicht

Satz von l'Hospital

Seien $c \in \mathbb{R} \cup \{-\infty, \infty\}$ und $f, g\colon (a, b) \to \mathbb{R}$ stetig differenzierbar mit $g'(x) \neq 0$ $(\forall x \in (a, b))$ und entweder

$$\lim_{x \to c} f(x) = \lim_{x \to c} g(x) = 0 \qquad \text{oder} \qquad \lim_{x \to c} f(x) = \lim_{x \to c} g(x) = \infty.$$

Falls $\lim_{x \to c} \frac{f'(x)}{g'(x)}$ existiert gilt, dann gilt:

$$\lim_{x \to c} \frac{f(x)}{g(x)} = \lim_{x \to c} \frac{f'(x)}{g'(x)}.$$

Themenübersicht

Taylor-Polynome und -Reihen

Sei $I \subseteq \mathbb{R}$ ein Intervall, $f : I \to \mathbb{R}$ eine Funktion und $c \in I$.

1. Sei $n \in \mathbb{N}$ und f n-mal stetig differenzierbar. Dann ist

$$T_n f(x; c) := \sum_{k=0}^{n} \frac{f^{(k)}(c)}{k!}(x - c)^k$$

   das n-te Taylor-Polynom von f in c.

2. Sei f unendlich oft stetig differenzierbar. Dann ist

$$T_\infty f(x; c) := \sum_{k=0}^{\infty} \frac{f^{(k)}(c)}{k!}(x - c)^k$$

   die Taylor-Reihe von f.

Themenübersicht

Themenübersicht

Stammfunktion

Seien $a, b, c \in \mathbb{R}$ mit $a < b$. Eine differenzierbare Funktion $F\colon [a, b] \to \mathbb{R}$ heißt Stammfunktion von $f\colon [a, b] \to \mathbb{R}$, falls $F' = f$ gilt.

Seien $a, c \in \mathbb{R}$ mit $a \neq -1$. Einige spezielle Stammfunktionen sind folgende.

$f(x)$	c	x^a	$\frac{1}{x}$	e^x	$\sin(x)$	$\cos(x)$	$\ln x$
$F(x)$	cx	$\frac{x^{a+1}}{a+1}$	$\ln \lvert x \rvert$	e^x	$-\cos(x)$	$\sin(x)$	$x \ln x - x$

Eigenschaften integrierbarer Funktionen

Seien $f, g\colon [a,b] \to \mathbb{R}$ integrierbar und $c \in \mathbb{R}$ beliebig. Dann gelten folgende Regeln.

1. Linearität:
$$\int_a^b c \cdot f(x)\,\mathrm{d}x = c \cdot \int_a^b f(x)\,\mathrm{d}x.$$
2. Additivität:
$$\int_a^b f(x) + g(x)\,\mathrm{d}x = \int_a^b f(x)\,\mathrm{d}x + \int_a^b g(x)\,\mathrm{d}x.$$
3. Monotonie:
$$\text{Wenn } f(x) \leq g(x) \text{ für alle } x \in [a,b], \text{ dann } \int_a^b f(x)\,\mathrm{d}x \leq \int_a^b g(x)\,\mathrm{d}x.$$
4. Zerlegbarkeit:
$$\text{Wenn } c \in (a,b), \text{ dann } \int_a^b f(x)\,\mathrm{d}x = \int_a^c f(x)\,\mathrm{d}x + \int_c^b f(x)\,\mathrm{d}x.$$

Hauptsatz der Differential- und Integralrechnung

Seien $a, b \in \mathbb{R}$ mit $a < b$ und $f\colon [a,b] \to \mathbb{R}$ stetig. Dann gilt:

1. Die Funktion $F\colon [a,b] \to \mathbb{R}$ mit

$$F(x) = \int_a^x f(t)\,\mathrm{d}t$$

   ist immer eine Stammfunktion von f.

2. Für jede Stammfunktion F von f gilt:

$$\int_a^b f(x)\,\mathrm{d}x = [F(x)]_{x=a}^b.$$

Info:

Wir werden immer wieder die Notationen $[F(x)]_{x=a}^b = F(b) - F(a)$ und $[F(x)]_{x=a} = F(a)$ benutzen.

Partielle Integration

Seien $f, g\colon [a,b] \to \mathbb{R}$ stetig differenzierbar. Dann gilt:

$$\int_a^b f(x) \cdot g'(x)\,\mathrm{d}x = [f(x) \cdot g(x)]_{x=a}^b - \int_a^b f'(x) \cdot g(x)\,\mathrm{d}x.$$

Beispiel:

$$\int_1^2 \ln x \cdot x\,\mathrm{d}x = \underset{\substack{\uparrow \\ f(x)=\ln x,\ g(x)=\frac{1}{2}x^2}}{\left[\ln x \cdot \frac{1}{2}x^2\right]_{x=1}^2} - \int_1^2 \frac{1}{2}x\,\mathrm{d}x = \left[\ln x \cdot \frac{1}{2}x^2\right]_{x=1}^2 - \left[\frac{1}{4}x^2\right]_{x=1}^2 = 2\ln 2 - \frac{3}{4}.$$

Partielle Integration für Stammfunktionen

Seien $f, g\colon [a,b] \to \mathbb{R}$ stetig differenzierbar und $\int f'(x) \cdot g(x)\,\mathrm{d}x$ eine beliebige Stammfunktion von $f'(x) \cdot g(x)$. Dann ist

$$\int f(x) \cdot g'(x)\,\mathrm{d}x = f(x) \cdot g(x) - \int f'(x) \cdot g(x)\,\mathrm{d}x$$

eine Stammfunktion von $f(x) \cdot g'(x)$.

Beispiel: Eine Stammfunktion von $\ln x \cdot x$ ist:

$$\int \ln x \cdot x\,\mathrm{d}x \underset{\substack{\uparrow \\ f(x)=\ln x,\ g(x)=\frac{1}{2}x^2}}{=} \ln x \cdot \frac{1}{2}x^2 - \int \frac{1}{2}x\,\mathrm{d}x = \ln x \cdot \frac{1}{2}x^2 - \frac{1}{4}x^2 = \frac{1}{2}x^2\left(\ln x - \frac{1}{2}\right).$$

Substitutionssregel

Seien $f, g\colon [a,b] \to \mathbb{R}$ stetig differenzierbar. Dann gilt:

$$\int_a^b f(g(x)) \cdot g'(x)\,\mathrm{d}x = \int_{g(a)}^{g(b)} f(y)\,\mathrm{d}y.$$

Wie kommt man intuitiv auf $\int_{g(a)}^{g(b)} f(y)\,\mathrm{d}y$?

1. Ersetze überall $g(x)$ durch y.
2. Schreibe $\int_a^b \ldots\,\mathrm{d}x$ in $\int_a^b \frac{\ldots}{y'}\,\mathrm{d}y$ um und kürze alle übrigen x weg.
3. Wende g auf beide Grenzen a und b an.

Beispiel:

$$\int_0^1 x^2 e^{x^3+1}\,\mathrm{d}x = \underset{\substack{\uparrow \\ y = x^3+1,\ y' = 3x^2}}{} \int_0^1 x^2 e^y \frac{1}{3x^2}\,\mathrm{d}y = \int_1^2 \frac{1}{3} e^y\,\mathrm{d}y = \left[\frac{1}{3}e^y\right]_{y=1}^2 = \frac{1}{3}(e^2 - e).$$

Substitutionssregel für Stammfunktionen

Seien $f, g\colon [a,b] \to \mathbb{R}$ stetig differenzierbar und $\int f(y)\,\mathrm{d}y$ eine beliebige Stammfunktion von $f(y)$. Dann ist

$$\int f(g(x)) \cdot g'(x)\,\mathrm{d}x = \left[\int f(y)\,\mathrm{d}y\right]_{y=g(x)}$$

eine Stammfunktion von $f(g(x)) \cdot g'(x)$.

Wie kommt man intuitiv auf $\int f(y)\,\mathrm{d}y$?

1. Ersetze überall $g(x)$ durch y.
2. Schreibe $\int \ldots\,\mathrm{d}x$ in $\int \frac{\ldots}{y'}\,\mathrm{d}y$ um und kürze alle übrigen x weg.

Beispiel: Eine Stammfunktion für $x^2 e^{x^3+1}$ ist:

$$\int x^2 e^{x^3+1}\,\mathrm{d}x = \int x^2 e^{y} \frac{1}{3x^2}\,\mathrm{d}y = \int \frac{1}{3} e^{y}\,\mathrm{d}y = \left[\frac{1}{3} e^{y}\right]_{y=x^3+1} = \frac{1}{3} e^{x^3+1}.$$

$y = x^3 + 1,\ y' = 3x^2$

Typische Stammfunktionen

Hier sind nochmal einige Herleitungen von typischen Stammfunktionen.

- Stammfunktionen der Form $\int f(x) \cdot f'(x)\ \mathrm{d}x$ oder $\int \frac{f'(x)}{f(x)}\ \mathrm{d}x$ lassen sich mithilfe der Substitutionsregel mit $y = f(x)$ berechnen. Man erhält:

$$\int f(x) \cdot f'(x)\ \mathrm{d}x = \left[\int y\ \mathrm{d}y\right]_{y=f(x)} = \left[\frac{1}{2}y^2\right]_{y=f(x)} = \frac{1}{2}f(x)^2,$$

$$\int \frac{f'(x)}{f(x)}\ \mathrm{d}x = \left[\int \frac{1}{y}\ \mathrm{d}y\right]_{y=f(x)} = \left[\ln|y|\right]_{y=f(x)} = \ln|f(x)|.$$

  Ich vermute, dass ihr diese zwei Formeln direkt anwenden dürft, aber ich kann es leider nicht garantieren. Die erste Formel haben wir für $f(x) = \sin(x)$ in der Übung hergeleitet und die zweite steht im Skript. Sicherheitshalber würde ich sie jedesmal neu herleiten. Gehen ja beide ganz schnell und man muss sich nur „Substitutionsregel mit $y = f(x)$“ merken :-)

Typische Stammfunktionen

- Für Polynome gilt:

$$\int a_n x^n + \ldots + a_1 x + a_0 \, \mathrm{d}x = \frac{a_n}{n+1} x^{n+1} + \ldots + \frac{a_1}{2} x^2 + a_0 x.$$

- Für Stammfunktionen der Form $\int \frac{c}{(x-b)^a} \, \mathrm{d}x$ gilt:

$$\int \frac{c}{(x-b)^a} \, \mathrm{d}x = \begin{cases} c \ln|x-b| & \text{falls } a = 1 \\ \frac{c(x-b)^{1-a}}{1-a} & \text{falls } a \neq 1. \end{cases}$$

- Für Stammfunktionen der Form $\int \frac{p(x)}{q(x)} \, \mathrm{d}x$ mit Polynomen p und q mit $\deg(p) < \deg(q)$ liefert die Partialbruchzerlegung (siehe ab Folie 1625) eine Darstellung der Form

$$\int \frac{p(x)}{q(x)} \, \mathrm{d}x = \int \frac{c_1}{(x-b_1)^{a_1}} \, \mathrm{d}x + \ldots + \int \frac{c_n}{(x-b_n)^{a_n}} \, \mathrm{d}x.$$

Typische Stammfunktionen

- Für Stammfunktionen der Form $\int \frac{p(x)}{q(x)}\,\mathrm{d}x$ mit Polynomen p und q mit $\deg(p) \geq \deg(q)$ liefert die Polynomdivision (siehe ab Folie 1322) eine Darstellung der Form

$$\int \frac{p(x)}{q(x)}\,\mathrm{d}x = \int s(x)\,\mathrm{d}x + \int \frac{r(x)}{q(x)}\,\mathrm{d}x$$

  für zwei Polynome r und s mit $\deg(r) < \deg(q)$, so dass man mit Partialbruchzerlegung den Ausdruck $\int \frac{r(x)}{q(x)}\,\mathrm{d}x$ vereinfachen kann.

- Bei Stammfunktionen der Form $\int \sqrt{x^2 + a}\,\mathrm{d}x$, $\int \sqrt{x^2 - a}\,\mathrm{d}x$ oder $\int \sqrt{a - x^2}\,\mathrm{d}x$ für ein $a > 0$ könnt ihr eine trigonometrische Substitution durchführen. YouTube und Google erklären euch gerne wie das geht.

Wer das Integrieren in der Schule nicht richtig gelernt bzw. wieder vergessen hat, kann das mit den Aufgaben 1-10 in

`www.poenitz-[]net.de/Mathematik/5.Analysis/5.5.A.Integralrechnung.pdf`

nachholen. Sie sind vom Schwierigkeitsgrad her perfekt für Einsteiger!

Themenübersicht

Partialbruchzerlegung

Seien p und q zwei Polynome mit $\deg(p) < \deg(q)$. Das Ziel der Partialbruchzerlegung ist es, die gebrochen rationale Funktion $\frac{p(x)}{q(x)}$ als Summe von Brüchen der Form

$$\frac{c_i}{(x - b_i)^{a_i}}$$

mit Konstanten a_i, b_i und c_i darzustellen.

Beispiel

Es gilt:

$$\frac{5x^2+3x+1}{x^3-3x-2} = \frac{3}{x-2} + \frac{2}{x+1} + \frac{-1}{(x+1)^2}.$$

Satz über die Existenz von Partialbruchzerlegungen

Seien $n \in \mathbb{N}$ eine natürliche Zahl, $p, q \in \mathbb{C}[x]$ Polynome mit $0 \leq \deg(p) < \deg(q) = n$. Dann existieren Konstanten $a_1, \ldots, a_n \in \mathbb{N}$ und $b_1, \ldots, b_n \in q^{-1}(0)$ und $c_1, \ldots, c_n \in \mathbb{C}$ mit

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{n} \frac{c_i}{(x - b_i)^{a_i}} \qquad (\forall x \in \mathbb{C} \setminus q^{-1}(0)).$$

Erinnerung: $q^{-1}(0)$ ist die Menge aller Nullstellen von q.

Beweis (für Interessierte)

Wir beweisen die Aussage durch vollständige Induktion nach n.

Induktionsanfang.

Für $n = 1$ existieren $p_0, q_0, q_1 \in \mathbb{C}$ mit $q_1 \neq 0$, $p(x) = p_0$ und $q(x) = q_1 x + q_0$. Dann ist $q^{-1}(0) = \left\{ -\frac{q_0}{q_1} \right\}$ und für $a_1 = 1$, $b_1 = -\frac{q_0}{q_1}$ und $c_1 = \frac{p_0}{q_1}$ gilt:

$$\frac{p(x)}{q(x)} = \frac{p_0}{q_1 x + q_0} = \frac{\frac{p_0}{q_1}}{x + \frac{q_0}{q_1}} = \frac{c_1}{(x - b_1)^{a_1}} = \sum_{i=1}^{1} \frac{c_i}{(x - b_i)^{a_i}} \qquad (\forall x \in \mathbb{C} \setminus q^{-1}(0)).$$

Beweis (für Interessierte)

Induktionsschritt.

Sei $n \in \mathbb{N}$ beliebig.

Angenommen für beliebige Polynome $p', q' \in \mathbb{C}[x]$ mit $0 \leq \deg(p) < \deg(q) = n$ existieren Konstanten $a_1, \ldots, a_n \in \mathbb{N}$ und $b_1, \ldots, b_n \in q^{-1}(0)$ und $c_1, \ldots, c_n \in \mathbb{C}$ mit

$$\frac{p'(x)}{q'(x)} = \sum_{i=1}^{n} \frac{c_i}{(x - b_i)^{a_i}} \qquad (\forall x \in \mathbb{C} \setminus q^{-1}(0)).$$

Seien nun $p, q \in \mathbb{C}[x]$ zwei Polynome mit $0 \leq \deg(p) < \deg(q) = n + 1$, $x_i \in \mathbb{C}$ eine beliebige Nullstelle von q und $m_i \in \mathbb{N}$ ihre Vielfachheit.

Beweis (für Interessierte)

$\Longrightarrow$ Es gibt ein Polynom r mit $r(x_i) \neq 0$ und $q(x) = (x - x_i)^{m_i} r(x)$, d.h.:

$$\frac{p(x)}{q(x)} = \frac{p(x) - \frac{p(x_i)}{r(x_i)} r(x)}{(x - x_i)^{m_i} r(x)} + \frac{\frac{p(x_i)}{r(x_i)}}{(x - x_i)^{m_i}} \qquad (\forall x \in \mathbb{C} \setminus q^{-1}(0)).$$

Für den Grad von r gilt:

$$\deg(r) = \deg(q) - m_i \leq n.$$

$\Longrightarrow$ $s(x) = p(x) - \frac{p(x_i)}{r(x_i)} r(x)$ ist ein Polynom mit $s(x_i) = 0$, d.h. es gibt ein Polynom $p' \neq 0$ mit

$$\frac{p(x)}{q(x)} = \frac{(x - x_i) p'(x)}{(x - x_i)^{m_i} r(x)} + \frac{\frac{p(x_i)}{r(x_i)}}{(x - x_i)^{m_i}} \qquad (\forall x \in \mathbb{C} \setminus q^{-1}(0)).$$

Für den Grad von p' gilt:

$$0 \leq \deg(p') = \deg(s) - 1 \leq \max\{\deg(p), \deg(r)\} - 1 \leq n - 1$$

Beweis (für Interessierte)

$\Longrightarrow$ Setzt man $q'(x) = (x - x_i)^{m_i - 1} r(x)$, so erhält man

$$\frac{p(x)}{q(x)} = \frac{p'(x)}{q'(x)} + \frac{\frac{p(x_i)}{r(x_i)}}{(x - x_i)^{m_i}} \qquad (\forall x \in \mathbb{C} \setminus q^{-1}(0)).$$

Für den Grad von q' gilt:

$$\deg(q') = \deg(q) - 1 = n.$$

$\Longrightarrow$ Wegen $0 \leq \deg(p') < \deg(q') = n$ existieren nach Annahme Konstanten $a_1, \ldots, a_n \in \mathbb{N}$ und $b_1, \ldots, b_n \in q^{-1}(0)$ und $c_1, \ldots, c_n \in \mathbb{C}$ mit

$$\frac{p'(x)}{q'(x)} = \sum_{i=1}^{n} \frac{c_i}{(x - b_i)^{a_i}} \qquad (\forall x \in \mathbb{C} \setminus q^{-1}(0)).$$

Beweis (für Interessierte)

Wähle $c_{n+1} = m_i$, $b_{n+1} = x_i$ und $c_{n+1} = \frac{p(x_i)}{r(x_i)}$. Dann gilt:

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{n} \frac{c_i}{(x - b_i)^{a_i}} + \frac{c_{n+1}}{(x - b_{n+1})^{c_{n+1}}} = \sum_{i=1}^{n+1} \frac{c_i}{(x - b_i)^{a_i}} \qquad (\forall x \in \mathbb{C} \setminus q^{-1}(0)).$$

□

Rezept: Partialbruchzerlegung

Gegeben: Zwei Polynome $p, q \in \mathbb{C}[x]$ mit $\deg(p) < \deg(q)$ und q normiert.
Gesucht: Die Partialbruchzerlegung von $\frac{p(x)}{q(x)}$.
Algorithmus:

1. **Faktorisiere den Nenner.** D.h. bringe $q(x)$ in die Form

$$q(x) = (x - x_1)^{m_1} \cdot \ldots \cdot (x - x_k)^{m_k}$$

   über, wobei $x_1, \ldots, x_k$ die Nullstellen (engl. *roots*) von q und $m_1, \ldots, m_k$ ihre Vielfachheiten (engl. *multiplicities*) sind.

2. **Stelle die allgemeine Partialbruchzerlegung auf.** Diese lautet:

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{k} \sum_{j=1}^{m_i} \frac{c_{i,j}}{(x - x_i)^j}.$$

   wobei die $c_{i,j}$ noch unbekannte Konstanten sind.

Rezept: Partialbruchzerlegung

3. **Ermittle die Konstanten.** Finde konkrete Werte für die Konstanten $c_{i,j}$, so dass gilt:

$$p(x) = q(x) \cdot \sum_{i=1}^{n} \sum_{j=1}^{m_i} \frac{c_{i,j}}{(x - x_i)^j}.$$

4. **Stelle die spezielle Partialbruchzerlegung auf.** Setze die Werte der $c_{i,j}$ in die allgemeine Partialbruchzerlegung ein.

Infos

- Ein Polynom $a_n x^n + \ldots + a_1 x + a_0$ heißt normiert, falls der Leitkoeffizient 1 ist, d.h. $a_n = 1$.
- Falls q nicht normiert ist, dann kann man den Bruch $\frac{p(x)}{q(x)}$ mit dem Kehrwert des Leitkoeffizients von q erweitern, z.B.:

$$\frac{x^3 + 2x^2 - 4x + 1}{2x^2 - x + 3} = \frac{\frac{1}{2}x^3 + x^2 - 2x + \frac{1}{2}}{x^2 - \frac{1}{2}x + \frac{3}{2}}.$$

- Beachte, dass die Faktorisierung bei Schritt 1 über $\mathbb{C}$ ist, d.h. einige Nullstellen x_i dürfen auch einen Imaginärteil $\mathrm{Im}(x_i) \neq 0$ haben.
- Die Konstanten $c_{i,j}$ kann man bei Schritt 2. auch umbenennen, z.B. auf $A, B, C, \ldots$.

Beispiel

Seien $p(x) = 2x^2 + 2x + 3$ und $q(x) = x^3 + 2x^2 - x - 2$.

1. Faktorisierung von q:
$$q(x) = (x+1)(x+2)(x-1).$$
2. Allgemeine Partialbruchzerlegung:
$$\frac{2x^2 + 2x + 3}{x^3 + 2x^2 - x - 2} = \frac{A}{x+1} + \frac{B}{x+2} + \frac{C}{x-1}.$$
3. Konstanten:
$$A = -\frac{3}{2}, B = \frac{7}{3}, C = \frac{7}{6}.$$
4. Spezielle Partialbruchzerlegung:
$$\frac{2x^2 + 2x + 3}{x^3 + 2x^2 - x - 2} = \frac{-\frac{3}{2}}{x+1} + \frac{\frac{7}{3}}{x+2} + \frac{\frac{7}{6}}{x-1}.$$

(Schön. Und wie kommt man auf die Konstanten?)

Beispiel

Durch Koeffizientenvergleich:

$$\frac{2x^2+2x+3}{x^3+2x^2-x-2} = \frac{A(x+2)(x-1) + B(x+1)(x-1) + C(x+1)(x+2)}{(x+1)(x+2)(x-1)}$$

$$\Leftrightarrow\ 2x^2+2x+3 = A(x^2+x-2) + B(x^2-1) + C(x^2+3x+2)$$

$$\Leftrightarrow\ 2x^2+2x+3 = (A+B+C)x^2 + (A+3C)x + (-2A-B+2C)$$

$$\rightsquigarrow \quad \left.\begin{array}{rrrl} A & +B & +C & = 2 \\ A & & +3C & = 2 \\ -2A & -B & +2C & = 3 \end{array}\right\}$$

Gauß-Elimination liefert:

$$A = -\frac{3}{2},\ B = \frac{7}{3},\ C = \frac{7}{6}$$

Beispiel

Trick: Nullstellen einsetzen

$$\frac{2x^2+2x+3}{x^3+2x^2-x-2} = \frac{A(x+2)(x-1) + B(x+1)(x-1) + C(x+1)(x+2)}{(x+1)(x+2)(x-1)}$$

$x = -1$

$$2(-1)^2+2(-1)+3 = A(-1+2)(-1-1) + \underbrace{B(-1+1)(-1-1)}_{=0} + \underbrace{C(-1+1)(-1+2)}_{=0}$$

$$\Leftrightarrow 3 = A(-2)$$

$$\Leftrightarrow A = -\frac{3}{2}$$

Beispiel

$x = -2$

$$2(-2)^2 + 2(-2) + 3 = \underbrace{A(-2+2)(-2-1)}_{=0} + B(-2+1)(-2-1) + \underbrace{C(-2+1)(-2+2)}_{=0}$$

$$\Leftrightarrow \quad 7 = B \cdot 3$$

$$\Leftrightarrow \quad B = \frac{7}{3}$$

$x = 1$

$$2 \cdot 1^2 + 2 \cdot 1 + 3 = \underbrace{A(1+2)(1-1)}_{=0} + \underbrace{B(1+1)(1-1)}_{=0} + C(1+1)(1+2)$$

$$\Leftrightarrow \quad 7 = C \cdot 6$$

$$\Leftrightarrow \quad C = \frac{7}{6}$$

Info

Der Trick mit dem Einsetzen der Nullstellen liefert nur so viele Konstanten, wie es verschiedene Nullstellen gibt. Hat q beispielsweise nur einfache Nullstellen, dann kann man sie alle mit diesem Trick bestimmen. Ansonsten kann man damit nur einige Konstanten bestimmen und muss danach Koeffizientenvergleich für die restlichen anwenden.

Beispiel

Gegeben seien die Polynome $p(x) = 3x^2 - 9x + 7$ und $q(x) = (x-1)^2(x-2)$. Die allgemeine Partialbruchzerlegung lautet:

$$\frac{3x^2 - 9x + 7}{x^3 - 4x^2 + 5x - 2} = \frac{A}{x-1} + \frac{B}{(x-1)^2} + \frac{C}{x-2}$$

Man könnte mit Koeffizientenvergleich ein lineares Gleichungssystem mit 3 Gleichungen und 3 Variablen lösen oder zuerst B und C durch Einsetzen der Nullstellen $x_1 = 1$ und $x_2 = 2$ in

$$3x^2 - 9x + 7 = (x-1)(x-2)A + (x-2)B + (x-1)^2C$$

berechnen und dann A durch Koeffizientenvergleich bestimmen.

Die Qual der Wahl gebührt euch ;-)

Welche Werte haben die Konstanten in folgenden Partialbruchzerlegungen?

1. $\frac{x+5}{x^2-1} = \frac{A}{x-1} + \frac{B}{x+1}$
2. $\frac{x+5}{x^2+x-2} = \frac{A}{x-1} + \frac{B}{x+2}$
3. $\frac{7x+11}{x^2+x-6} = \frac{A}{x-2} + \frac{B}{x+3}$
4. $\frac{3x-5}{x^2-3x+2} = \frac{A}{x-1} + \frac{B}{x-2}$
5. $\frac{8x+12}{x^2+3x+2} = \frac{A}{x+1} + \frac{B}{x+2}$
6. $\frac{x+11}{x^3+4x^2+x-6} = \frac{A}{x-1} + \frac{B}{x+2} + \frac{C}{x+3}$

Lösungen

1. $A = 3$ und $B = -2$.
2. $A = 2$ und $B = -1$.
3. $A = 5$ und $B = 2$.
4. $A = 2$ und $B = 1$.
5. $A = 4$ und $B = 4$.
6. $A = 1$, $B = -3$ und $C = 2$.

Themenübersicht

Kurve

Sein $I \subseteq \mathbb{R}$ ein Intervall. Eine n-dimensionale parametrisierte Kurve γ ist eine Funktion $\gamma\colon I \to \mathbb{R}^n$ mit

$$\gamma(t) = \begin{pmatrix} \gamma_1(t) \\ \vdots \\ \gamma_n(t) \end{pmatrix}.$$

γ_i nennt man die i-te Komponentenfunktion von γ.

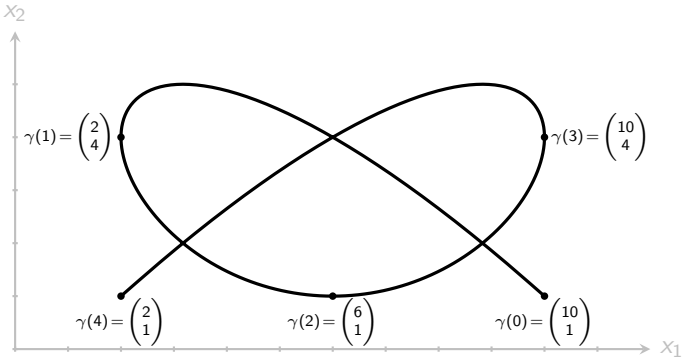
Für $n = 2$ ist γ eine ebene Kurve, für $n = 3$ eine Raumkurve und für $n = 1$ eine langweilige Kurve.

Beispiel 1: eine Breze

Beispiel einer ebenen Kurve ist $\gamma\colon [0,4] \to \mathbb{R}^2$ mit:

$$\gamma(t) = \begin{pmatrix} 2(t-1)^2(4-t)+2 \\ t(t-2)^2(4-t)+1 \end{pmatrix}.$$

Spur:

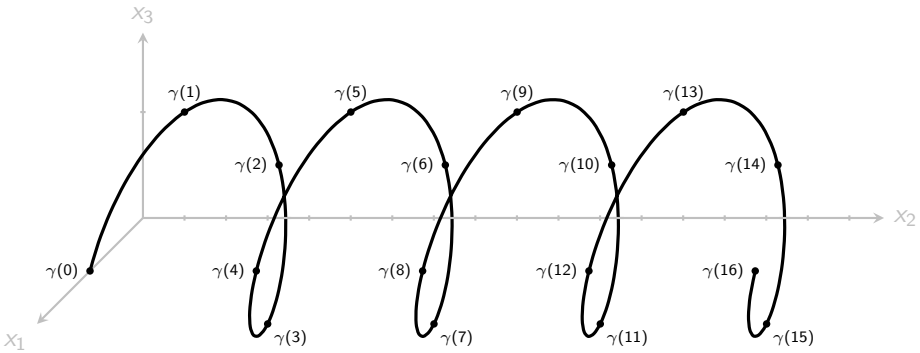


Beispiel 2: eine Helix

Beispiel einer Raumkurve ist $\gamma\colon [0,16] \to \mathbb{R}^3$ mit:

$$\gamma(t) = \begin{pmatrix} \cos(\pi t) \\ t \\ \sin(\pi t) \end{pmatrix}.$$

Spur:

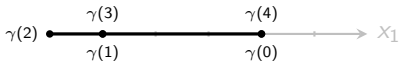


Beispiel 3: ein Witz

Beispiel einer langweiligen Kurve ist $\gamma\colon [0,4] \to \mathbb{R}^1$ mit:

$$\gamma(t) = \left((t-2)^2\right).$$

Spur:



Deswegen sind eindimensionale Kurven langweilig.

Infos zur Euklidischen Norm

- Für die Euklidische Norm $\|x\|_2$ eines Vektors $x \in \mathbb{R}^n$ gilt:

$$\|(x_1, \ldots, x_n)\|_2 = \sqrt{x_1^2 + \ldots + x_n^2}.$$

- Die Zahl 2 kommt daher, dass die Euklidische Norm ein Spezialfall der sogenannten p-Norm (für $p = 2$) ist.
- Weil die Euklidische Norm die natürlichste aller p-Normen ist, schreibt man auch oft nur $\|x\|$ statt $\|x\|_2$.

Für Interessierte: Wozu überhaupt andere p-Normen?

Für $x = (x_1, \ldots, x_n)$ und ein beliebiges $p \geq 1$ ist die p-Norm definiert als

$$\|x\|_p = \sqrt[p]{\sum_{i=1}^{n} |x_i|^p} \qquad \text{bzw.} \qquad \|x\|_\infty = \lim_{p \to \infty} \sqrt[p]{\sum_{i=1}^{n} |x_i|^p} = \max\{|x_i| \mid i \in [n]\}.$$

Die Euklidische Norm stellt den „direkten“ Abstand vom Punkt $(x_1, \ldots, x_n)$ zum Ursprung $(0, \ldots, 0)$ dar. Manchmal existiert allerdings der direkte Weg nicht oder es ist nicht relevant, ob der betrachtete Weg der direkte ist.

Ein Beispiel bei dem die 2-Norm nicht anwendbar ist, weil keine direkten Wege existieren, sind n-dimensionale Gittergraphen. Dort haben zwei Knoten $a = (a_1, \ldots, a_n)$ und $b = (b_1, \ldots, b_n)$ die Distanz

$$d(a, b) = \|a - b\|_1 = \sum_{i=1}^{n} |a_i - b_i|.$$

Siehe auch: Manhattan-Metrik.

Für Interessierte: Wozu überhaupt andere p-Normen?

Ein Beispiel, bei dem die 2-Norm zwar anwendbar, aber nicht erforderlich ist, sind sogenannte Splines (zu Deutsch: *Polynomzüge*). Splines sind parametrisierte Kurven, deren Form von Kontrollpunkten $P_1, \ldots, P_n \in \mathbb{R}^d$ bestimmt wird. Bei Zeichenprogrammen, die die gezeichneten Striche als Splines darstellen, wählt man beispielsweise $d = 2$ und definiert $P_i = (x_i, y_i)$ als denjenigen Punkt auf der Zeichenebene, auf dem sich der Stift nach i Zeiteinheiten befindet.

Für zwei gegebene Splines mit Kontrollpunkten $P = (P_1, \ldots, P_n)$ und $Q = (Q_1, \ldots, Q_n)$ kann man mit

$$d(P, Q) = \sqrt[p_2]{\sum_{i=1}^{n} \|P_i - Q_i\|_{p_1}^{p_2}}$$

ein Maß für den Unterschied zwischen ihnen definieren. D.h. man benutzt eine p_1-Norm, um den Unterschied zwischen zwei Punkten darzustellen und eine p_2-Norm für den Unterschied beider Kurven.

Für Interessierte: Wozu überhaupt andere p-Normen?

Mit $d(P, Q)$ kann man erkennen, ob die zwei Kurven ähnlich (d.h. $d(P, Q)$ klein) oder sehr unterschiedlich (d.h. $d(P, Q)$ groß) sind. Damit lassen sich unter Anderem Methoden implementieren, die die Anzahl an Kontrollpunkten reduzieren, d.h. Kontrollpunkte so löschen, dass die Form der Kurve minimal verändert wird.

Für $p_1 = 2$ und $p_2 = \infty$ erhält man beispielsweise

$$d(P, Q) = \max \{ \|P_i - Q_i\|_2 \mid i \in [n] \} .$$

Diese Wahl ist zwar unintuitiv, aber sie liefert gute Ergebnisse und kann sehr effizient implementiert werden.

Ansonsten habe ich zu Kurven nicht viel mehr zu sagen als das was im Skript steht. :-)

Themenübersicht

Definition

Gegeben seien $\vec{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{C}^n$ mit Länge n und eine n-te primitive Einheitswurzel $\omega \in \mathbb{C}$. Die Fouriertransformation $\mathcal{F}_{n,\omega}(\vec{a})$ von $\vec{a}$ ist ebenfalls ein Vektor aus $\mathbb{C}^n$ und ist definiert als:

$$\mathcal{F}_{n,\omega}(\vec{a}) := \left(P_{\vec{a}}(1), P_{\vec{a}}(\omega), P_{\vec{a}}(\omega^2), \ldots, P_{\vec{a}}(\omega^{n-1})\right).$$

Dabei ist $P_{\vec{a}}(x) := a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$ das durch den Vektor $\vec{a}$ kodierte Polynom.

Infos

- Für jedes $n \in \mathbb{N}$ ist $e^{\frac{2\pi}{n} i}$ eine primitive n-te Einheitswurzel.
- Die Fouriertransformation ist nichts anderes als eine bijektive Funktion $\mathcal{F}_{n,\omega} : \mathbb{C}^n \to \mathbb{C}^n$ zwischen der Menge aller komplexen n-Tupel und sich selbst.
- Die Umkehrfunktion $\mathcal{F}_{n,\omega}^{-1}$ von $\mathcal{F}_{n,\omega}$ ist

$$\mathcal{F}_{n,\omega}^{-1}(\vec{a}) = \frac{1}{n} \cdot \mathcal{F}_{n,\frac{1}{\omega}}(\vec{a}).$$

  Hierbei hat $\frac{1}{\omega}$ dieselbe Polarform wie ω, aber mit negativem Winkel. Der Faktor $\frac{1}{n}$ wird auf jede Komponente des Tupels $\mathcal{F}_{n,\frac{1}{\omega}}(\vec{a})$ dazumultipliziert.

Beispiele

Weil $e^{\frac{2\pi}{n}i}$ für jedes $n \in \mathbb{N}$ eine primitive n-te Einheitswurzel ist, werden wir für die Berechnung von $\mathcal{F}_{n,\omega}(\vec{a})$ meistens $\omega = e^{\frac{2\pi}{n}i}$ wählen.

- Für $n = 1$, $\omega = e^{2\pi i} = 1$ und $\vec{a} = (1)$ gilt

$$P_{\vec{a}}(x) = 1$$

und

$$\mathcal{F}_{1,1}((1)) = (P_{\vec{a}}(1)) = (1).$$

- Für $n = 2$, $\omega = e^{\pi i} = -1$ und $\vec{a} = (1, 2)$ gilt

$$P_{\vec{a}}(x) = 1 + 2x$$

und

$$\mathcal{F}_{2,-1}((1,2)) = (P_{\vec{a}}(1), P_{\vec{a}}(-1)) = (3, -1).$$

Beispiele

- Für $n = 3$, $\omega = e^{\frac{2\pi}{3}i} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ und $\vec{a} = (1, 2, 3)$ gilt

$$P_{\vec{a}}(x) = 1 + 2x + 3x^2$$

und

$$\begin{aligned}\mathcal{F}_{3,-\frac{1}{2}+\frac{\sqrt{3}}{2}i}((1,2,3)) &= \left(P_{\vec{a}}(1), P_{\vec{a}}\left(-\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i\right), P_{\vec{a}}\left(-\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i\right)\right) \\ &= \left(6, -\tfrac{3}{2} - \tfrac{\sqrt{3}}{2}i, -\tfrac{3}{2} + \tfrac{\sqrt{3}}{2}i\right).\end{aligned}$$

- Für $n = 4$, $\omega = e^{\frac{2\pi}{4}i} = i$ und $\vec{a} = (1, 2, 3, 4)$ gilt

$$P_{\vec{a}}(x) = 1 + 2x + 3x^2 + 4x^3$$

und

$$\mathcal{F}_{4,i}((1,2,3,4)) = (P_{\vec{a}}(1), P_{\vec{a}}(i), P_{\vec{a}}(-1), P_{\vec{a}}(-i)) = (10, -2 - 2i, -2, -2 + 2i).$$

Was sind die Ergebnisse folgender Fouriertransformationen?

1. $\mathcal{F}_{4,i}((3,2,0,2))$,
2. $\mathcal{F}_{4,i}((2i,3,-i,2))$,
3. $\mathcal{F}_{4,i}((4,1,-2,2))$,
4. $\mathcal{F}_{4,i}((2,1,2,1))$.

Benutze die Definition aus Folie 1655.

Antworten (ohne Rechnungen)

1. $\mathcal{F}_{4,i}((3,2,0,2)) = (7,3,-1,3)$,
2. $\mathcal{F}_{4,i}((2i,3,-i,2)) = (5+i,4i,-5+i,2i)$,
3. $\mathcal{F}_{4,i}((4,1,-2,2)) = (5,6-i,-1,6+i)$,
4. $\mathcal{F}_{4,i}((2,1,2,1)) = (6,0,2,0)$.

Schnelle Fouriertransformation

Seien $n \in \mathbb{N}$ gerade und ω eine primitive n-te Einheitswurzel. Sind

$$\mathcal{F}_{\frac{n}{2},\omega^2}\big((a_0, a_1, \ldots, a_{\frac{n}{2}-1})\big) = (c_0, c_1, \ldots, c_{\frac{n}{2}-1}) \text{ und}$$
$$\mathcal{F}_{\frac{n}{2},\omega^2}\big((b_0, b_1, \ldots, b_{\frac{n}{2}-1})\big) = (d_0, d_1, \ldots, d_{\frac{n}{2}-1}),$$

dann gilt:

$$\mathcal{F}_{n,\omega}\big((a_0, b_0, a_1, b_1, \ldots, a_{\frac{n}{2}-1}, b_{\frac{n}{2}-1})\big) =$$
$$(c_0 + d_0, c_1 + \omega d_1, \ldots, c_{\frac{n}{2}-1} + \omega^{\frac{n}{2}-1} d_{\frac{n}{2}-1}, c_0 - d_0, c_1 - \omega d_1, \ldots, c_{\frac{n}{2}-1} - \omega^{\frac{n}{2}-1} d_{\frac{n}{2}-1}).$$

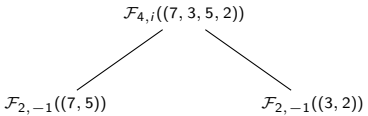
Beispiel

Seien $\vec{a} = (7, 3, 5, 2)$ und $\omega = i$.

$$\mathcal{F}_{4,i}((7, 3, 5, 2))$$

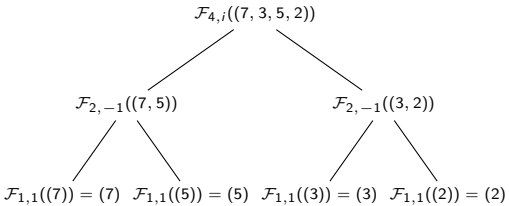
Beispiel

Seien $\vec{a} = (7, 3, 5, 2)$ und $\omega = i$.



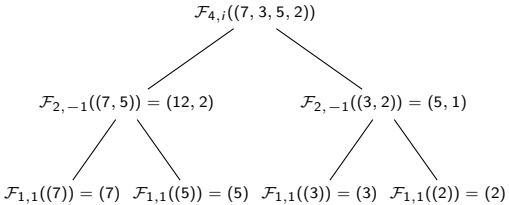
Beispiel

Seien $\vec{a} = (7, 3, 5, 2)$ und $\omega = i$.



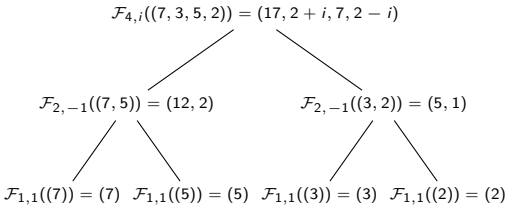
Beispiel

Seien $\vec{a} = (7, 3, 5, 2)$ und $\omega = i$.



Beispiel

Seien $\vec{a} = (7, 3, 5, 2)$ und $\omega = i$.

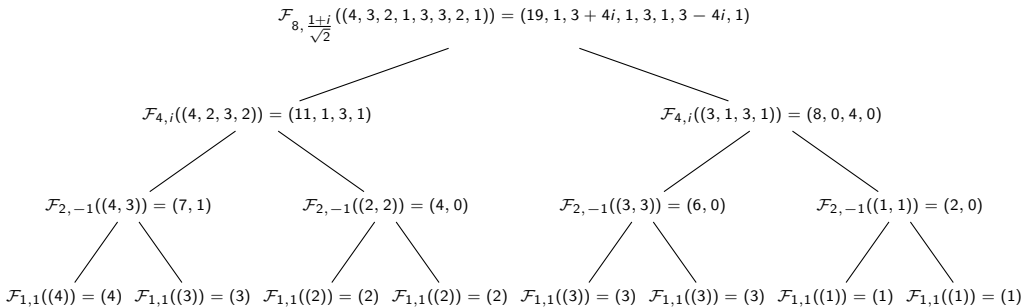


Daraus folgt:

$$\mathcal{F}_{4,i}((7,3,5,2)) = (17, 2+i, 7, 2-i).$$

Noch ein Beispiel

Seien $\vec{a} = (4, 3, 2, 1, 3, 3, 2, 1)$ und $\omega = \frac{1+i}{\sqrt{2}}$.



Daraus folgt:

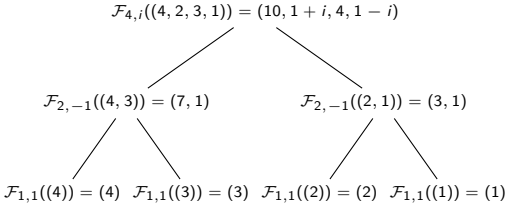
$$\mathcal{F}_{8,\frac{1+i}{\sqrt{2}}}((4,3,2,1,3,3,2,1)) = (19, 1, 3+4i, 1, 3, 1, 3-4i, 1).$$

Quizfrage

Was ist $\mathcal{F}_{4,i}((4,2,3,1))$?

Benutze die rekursive Berechnung aus Folie 1661.

Antwort


$\mathcal{F}_{4,i}((4,2,3,1)) = (10, 1+i, 4, 1-i)$
$\mathcal{F}_{2,-1}((4,3)) = (7,1)$
$\mathcal{F}_{2,-1}((2,1)) = (3,1)$
$\mathcal{F}_{1,1}((4)) = (4)$
$\mathcal{F}_{1,1}((3)) = (3)$
$\mathcal{F}_{1,1}((2)) = (2)$
$\mathcal{F}_{1,1}((1)) = (1)$

Noch eine Quizfrage

Sei $\omega = \frac{1+i}{\sqrt{2}}$. Was ist $\mathcal{F}_{8,\omega}((2i, 2, 3, 1, -i, 2, 2, 1))$?

Benutze die rekursive Berechnung aus Folie 1661. Du darfst auch die Ergebnisse aus der Quizfrage auf Folie 1659 benutzen, um Zeit zu sparen.

Antwort

$$\mathcal{F}_{8,\frac{1+i}{\sqrt{2}}}((2i,2,3,1,-i,2,2,1)) = (11+i, 4i, -5+3i, 2i, -1+i, 4i, -5-i, 2i)$$

$$\mathcal{F}_{4,i}((2i,3,-i,2)) = (5+i, 4i, -5+i, 2i)$$

$$\mathcal{F}_{4,i}((2,1,2,1)) = (6,0,2,0)$$

Mehr Quizfragen

Sei $\omega = \frac{1+i}{\sqrt{2}}$. Was sind die Ergebnisse folgender Fouriertransformationen?

1. $\mathcal{F}_{8,\omega}((2,2,2,2,2,2,2,2))$,
2. $\mathcal{F}_{8,\omega}((16,0,0,0,0,0,0,0))$,
3. $\mathcal{F}_{8,\omega}((8,0,0,0,-16,0,0,0))$.

Benutze die rekursive Berechnung aus Folie 1661.

Antworten (ohne Rechnungen)

1. $\mathcal{F}_{8,\omega}((2,2,2,2,2,2,2,2)) = (16,0,0,0,0,0,0,0)$,
2. $\mathcal{F}_{8,\omega}((16,0,0,0,0,0,0,0)) = (8,0,0,0,-16,0,0,0)$,
3. $\mathcal{F}_{8,\omega}((8,0,0,0,-16,0,0,0)) = (8,2+2i,0,2-2i,0,2+2i,0,2-2i)$.

Primitive Einheitswurzeln

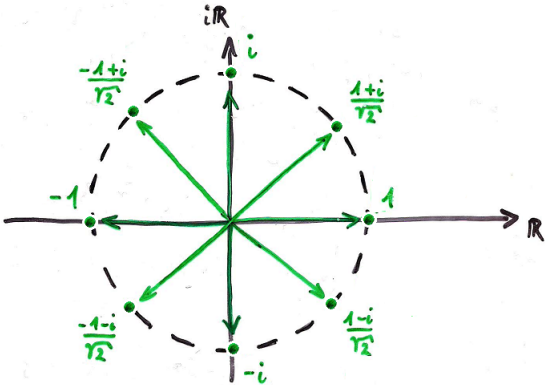
Wir haben für die Fouriertransformation bisher nur mit $n = 1$, $n = 2$, $n = 4$ und $n = 8$ gearbeitet. Mögliche primitive n-te Einheitswurzeln für diese Werte sind:

n	primitive n-te Einheitswurzeln	$e^{\frac{2\pi}{n}i}$
1	1	1
2	-1	-1
4	i, $-i$	i
8	$\frac{1+i}{\sqrt{2}}$, $\frac{-1+i}{\sqrt{2}}$, $\frac{-1-i}{\sqrt{2}}$, $\frac{1-i}{\sqrt{2}}$	$\frac{1+i}{\sqrt{2}}$

Wir haben in DS nur $\omega = e^{\frac{2\pi}{n}i}$ als primitive n-te Einheitswurzel benutzt und wahrscheinlich bleibt es auch so!

Tipp

Man kann mit Hilfe des komplexen Einheitskreises diese Werte leicht potenzieren. Nimmt man ω als Startpunkt und läuft n Schritte auf dem Einheitskreis gegen den Uhrzeiger (jeder Schritt ist so groß wie der Schritt von 1 zu ω), so landet man auf ω^n:



Tipp

Für $\omega = \frac{1+i}{\sqrt{2}}$ gilt beispielsweise:

$$\begin{array}{llll} \omega^0 = 1, & \omega^1 = \frac{1+i}{\sqrt{2}}, & \omega^2 = i, & \omega^3 = \frac{-1+i}{\sqrt{2}}, \\ \omega^4 = -1, & \omega^5 = \frac{-1-i}{\sqrt{2}}, & \omega^6 = -i, & \omega^7 = \frac{1-i}{\sqrt{2}}. \end{array}$$

Entsprechend gilt für $\omega = i$:

$$\omega^0 = 1, \quad \omega^1 = i, \quad \omega^2 = -1, \quad \omega^3 = -i.$$

Themenübersicht

Gradient und Hesse-Matrix

Seien $n \in \mathbb{N}$ und $M \subseteq \mathbb{R}^n$ offen. Für jede stetig differenzierbare Funktion $f\colon M \to \mathbb{R}$ heißt

$$\nabla f(x) = \begin{pmatrix} \partial_1 f(x) \\ \vdots \\ \partial_n f(x) \end{pmatrix}$$

der Gradient von f in $x \in M$. Ist f zweimal stetig, so heißt

$$\nabla^2 f(x) = \begin{pmatrix} \partial_{11} f(x) & \cdots & \partial_{1n} f(x) \\ \vdots & & \vdots \\ \partial_{n1} f(x) & \cdots & \partial_{nn} f(x) \end{pmatrix}$$

mit $\partial_{ij} f(x) = \partial_i \partial_j f(x) = \partial_j \partial_i f(x)$ die Hesse-Matrix von f in $x \in M$.

Mehrdimensionale Extrempunkte

Seien $n \in \mathbb{N}$ und $M \subseteq \mathbb{R}^n$ offen, $f : M \to \mathbb{R}$ zweimal stetig differenzierbar und $c \in M$. Dann gilt:

$$
\begin{array}{lcl}
f \text{ hat ein lokales Minimum in } c & \Longrightarrow & \nabla^2 f(c) \text{ positiv semidefinit}, \\
f \text{ hat ein lokales Maximum in } c & \Longrightarrow & \nabla^2 f(c) \text{ negativ semidefinit}, \\
\nabla f(c) = 0 \text{ und } \nabla^2 f(c) \text{ positiv definit} & \Longrightarrow & f \text{ hat ein isoliertes lokales Minimum in } c, \\
\nabla f(c) = 0 \text{ und } \nabla^2 f(c) \text{ negativ definit} & \Longrightarrow & f \text{ hat ein isoliertes lokales Maximum in } c, \\
\nabla f(c) = 0 \text{ und } \nabla^2 f(c) \text{ indefinit} & \Longrightarrow & f \text{ hat ein Sattelpunkt in } c.
\end{array}
$$

Info: Falls $\nabla f(c) = 0$, dann nennt man c einen kritischen Punkt.

Achtung!

Achtet bitte auf die Richtung der Pfeile! Beispielsweise muss f nicht notwendigerweise ein lokales Minimum in c haben, falls $\nabla^2 f(c)$ positiv semidefinit ist.

Wenn aber $\nabla^2 f(c)$ nicht positiv semidefinit ist, dann hat f garantiert kein lokales Minimum in c.

Erinnerung aus DS: $A \to B \equiv \neg B \to \neg A$.

Erinnerungen

- Für eine $(n \times n)$-Matrix A heißt

$$\chi_A(\lambda) = \det(A - \lambda I_n)$$

das charakteristische Polynom von A, wobei I_n die $(n \times n)$-Einheitsmatrix ist. Die Nullstellen von χ_A nennt man Eigenwerte von A.

- Die Matrix $A - \lambda I_n$ ist nichts anderes als A mit „$-\lambda$“ bei jedem Element der Hauptdiagonale.

- Für $n = 2$ und $n = 3$ gilt:

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21},$$

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

Erinnerungen

- Für ein allgemeines $n \in \mathbb{N}$ liefert der Laplacesche Entwicklungssatz eine Berechnungsmethode für de Determinante einer quadratischen Matrix. Prof. Google und Dr. YouTube helfen euch dabei, das sehr schnell wieder auffrischen!
- Für eine quadratische symmetriscshe Matrix $A \in \mathbb{R}^{n \times n}$ gilt:

$$
\begin{array}{lcl}
A \text{ positiv semidefinit} & \Longleftrightarrow & \text{Für alle Eigenwerte } \lambda \text{ von } A \text{ gilt } \lambda \geq 0, \\
A \text{ negativ semidefinit} & \Longleftrightarrow & \text{Für alle Eigenwerte } \lambda \text{ von } A \text{ gilt } \lambda \leq 0, \\
A \text{ positiv definit} & \Longleftrightarrow & \text{Für alle Eigenwerte } \lambda \text{ von } A \text{ gilt } \lambda > 0, \\
A \text{ negativ definit} & \Longleftrightarrow & \text{Für alle Eigenwerte } \lambda \text{ von } A \text{ gilt } \lambda < 0, \\
A \text{ indefinit} & \Longleftrightarrow & A \text{ hat sowohl positive als auch negative Eigenwerte.}
\end{array}
$$

Beispiel

Für die Matrix

$$A = \begin{pmatrix} 9 & 6 \\ 6 & -7 \end{pmatrix}$$

gilt:

$$\chi_A(\lambda) = \det \begin{pmatrix} 9-\lambda & 6 \\ 6 & -7-\lambda \end{pmatrix} = (9-\lambda)(-7-\lambda) - 6^2 = \lambda^2 - 2\lambda + 99.$$

χ_A hat die Nullstellen -9 und 11, d.h. A ist indefinit.

Übunsaufgabe

Sei $f\colon \mathbb{R}^+ \times \mathbb{R} \to \mathbb{R}$ mit $f(x, y) = x^y$.

1. Bestimme alle kritischen Punkte von f.
2. Untersuche, ob die kritischen Punkte von f lokale Maxima, lokale Minima oder Sattelpunkte sind.

Hinweise:

- $f\colon \mathbb{R}^+ \times \mathbb{R} \to \mathbb{R}$ besagt, dass $f(x, y)$ für alle $x, y \in \mathbb{R}$ mit $x > 0$ definiert ist.
- Eine Potenz a^b mit $a > 0$ ist definiert als $a^b = e^{b \ln(a)}$.

Sei $f\colon \mathbb{R}^+ \times \mathbb{R} \to \mathbb{R}$ mit $f(x,y) = x^y$.

1. Für den Gradienten von f gilt:

$$\nabla f(x,y) = \begin{pmatrix} \partial_1 x^y \\ \partial_2 x^y \end{pmatrix} = \begin{pmatrix} y x^{y-1} \\ \ln(x) e^{y \ln(x)} \end{pmatrix} = \begin{pmatrix} y x^{y-1} \\ \ln(x) x^y \end{pmatrix}.$$

Daraus folt:

$$\begin{aligned} (x,y) \text{ kritisch} &\iff y x^{y-1} = 0 \wedge \ln(x) x^y = 0 \\ &\iff (y = 0 \vee x^{y-1} = 0) \wedge (\ln(x) = 0 \vee x^y = 0) \\ &\iff (y = 0 \vee x = 0) \wedge (x = 1 \vee x = 0). \end{aligned}$$

Wegen $x > 0$ ist $(1,0)$ der einzige kritische Punkt von f.

2. Für die Hesse-Matrix von f gilt:

$$\nabla^2 f(x,y) = \begin{pmatrix} \partial_{11} x^y & \partial_{12} x^y \\ \partial_{21} x^y & \partial_{22} x^y \end{pmatrix} = \begin{pmatrix} y(y-1)x^{y-2} & (y\ln(x)+1)x^{y-1} \\ (y\ln(x)+1)x^{y-1} & \ln(x)^2 x^y \end{pmatrix}$$

und somit

$$\nabla^2 f(1,0) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Wegen

$$\det \begin{pmatrix} -\lambda & 1 \\ 1 & -\lambda \end{pmatrix} = (-\lambda)^2 - 1 = \lambda^2 - 1 = (\lambda+1)(\lambda-1)$$

besitzt $\nabla^2 f(1,0)$ die Eigenwerte -1 und 1 und ist nach den Erinnerungen ab Folie 1681 indefinit. Somit hat f nach Folie 1679 einen Sattelpunkt an der Stelle $(1,0)$.

Themenübersicht

Zweidimensionale Integrale

Eine Menge der Form

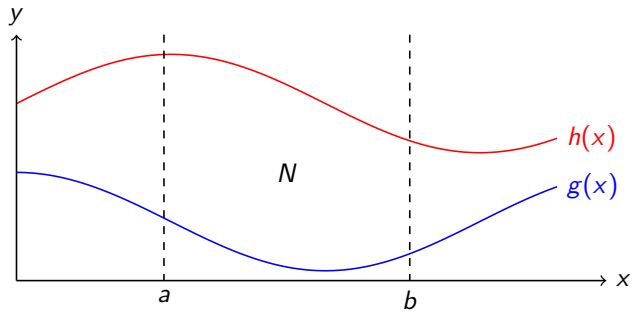
$$N = \left\{(x, y) \in \mathbb{R}^2 \,\middle|\, a \leq x \leq b, g(x) \leq y \leq h(x)\right\}$$

heißt Normalbereich. Für N gilt:

$$\iint\limits_N f(x, y) d(x, y) := \int_a^b \left(\int_{g(x)}^{h(x)} f(x, y) \, \mathrm{d}y \right) \mathrm{d}x.$$

Zweidimensionale Integrale

Graphisch:



Das Ergebnis des Integrals ist das Volumen eines Körpers mit Grundfläche N und Höhe $f(x, y)$.

Übrigens: Man kann x und y vertauschen, d.h. die Skizze an der Hauptdiagonale spiegeln.

Themenübersicht

Ziel

Sei $I \subseteq \mathbb{R}$ ein Intervall und $y\colon I \to \mathbb{R}$ eine Funktion.

Für eine gegebene Gleichung, in der t, $y(t)$ und Ableitungen von $y(t)$ vorkommen, suchen wir entweder eine oder alle möglichen Funktionen $y(t)$, die diese Gleichung erfüllen.

Auf den nächsten Folien werden Methoden für bestimmte Klassen von Differentialgleichungen vorgestellt.

Wegweiser

Für uns sind folgende 6 Methoden wichtig.

Differentialgleichung	Parameter	Folie
$y'(t) = f(t) \cdot g(y(t))$	$f, g \colon \mathbb{R} \to \mathbb{R}$	1693
$y'(t) + a(t) \cdot y(t) = 0$	$a \colon \mathbb{R} \to \mathbb{R}$	1698
$y'(t) + a(t) \cdot y(t) = f(t)$	$a, f \colon \mathbb{R} \to \mathbb{R}$	1701
$y''(t) + ay'(t) + by(t) = 0$	$a, b \in \mathbb{R}$	1705
$y''(t) + ay'(t) + by(t) = a_n t^n + \ldots + a_1 t + a_0$	$a, b, a_0, \ldots, a_n \in \mathbb{R},\ b, a_n \neq 0$	1709
$y''(t) + ay'(t) + by(t) = e^{\alpha t}(a_1 \cos(\beta t) + a_2 \sin(\beta t))$	$a, b, \alpha, \beta, a_1, a_2 \in \mathbb{R},\ b \neq 0$	1713

Methode 1 („Trennung der Variablen“)

Gegeben: Differentialgleichung 1. Ordnung

$$y'(t) = f(t) \cdot g(y(t))$$

für $t_0, y_0 \in \mathbb{R}$ und Funktionen $g\colon \mathbb{R} \to \mathbb{R}$ und $f\colon I \to \mathbb{R}$.

Lösungsmethode: Jede allgemeine Lösung erfüllt die Gleichung

$$G(y(t)) = F(t) + c \qquad \text{für} \qquad c \in \mathbb{R},$$

wobei $F(t) = \int f(t)\,\mathrm{d}t$ und $G(t) = \int \frac{1}{g(t)}\,\mathrm{d}t$ beliebige Stammfunktionen von $f(t)$ und $\frac{1}{g(t)}$ sind.

Die spezielle Lösung für $y(t_0) = y_0$ erfüllt die Gleichung

$$\int_{y_0}^{y(t)} \frac{1}{g(u)}\,\mathrm{d}u = \int_{t_0}^{t} f(s)\,\mathrm{d}s.$$

In beiden Fällen hofft man, dass die entstehende Gleichung nach $y(t)$ gelöst werden kann.

Beispiel

Aufgabe: Finde alle Lösungen zu

$$y'(t) = \frac{t+3}{y(t)}.$$

Lösung: Es gilt $y'(t) = (t+3) \cdot \frac{1}{y(t)}$, d.h. $f(t) = t+3$ und $g(y(t)) = \frac{1}{y(t)}$.

Eine Stammfunktion von $f(t)$ ist

$$F(t) = \int f(t)\,\mathrm{d}t = \int t+3\,\mathrm{d}t = \frac{1}{2}t^2 + 3t.$$

Eine Stammfunktion von $\frac{1}{g(t)}$ ist

$$G(t) = \int \frac{1}{g(t)}\,\mathrm{d}t = \int t\,\mathrm{d}t = \frac{1}{2}t^2.$$

Beispiel

Wegen

$$\begin{aligned} G(y(t)) = F(t) + c \quad &\Longleftrightarrow \quad \frac{1}{2}(y(t))^2 = \frac{1}{2}t^2 + 3t + c \\ &\Longleftrightarrow \quad (y(t))^2 = t^2 + 6t + 2c \\ &\Longleftrightarrow \quad |y(t)| = \sqrt{t^2 + 6t + 2c} \\ &\Longleftrightarrow \quad y(t) = \pm\sqrt{t^2 + 6t + 2c} \end{aligned}$$

hat jede allgemeine Lösung eine der Formen

$$y(t) = \sqrt{t^2 + 6t + 2c} \qquad \text{oder} \qquad y(t) = -\sqrt{t^2 + 6t + 2c} \qquad \text{für} \qquad c \in \mathbb{R}.$$

Noch ein Beispiel

Aufgabe: Finde die spezielle Lösung zu

$$y'(t) = \frac{t+3}{y(t)} \qquad \text{mit} \qquad y(0) = 3.$$

Lösung: Es gilt $t_0 = 0$, $y_0 = 3$ und $y'(t) = (t+3) \cdot \frac{1}{y(t)}$, d.h. $f(t) = t+3$ und $g(y(t)) = \frac{1}{y(t)}$.

Aus dem Beispiel davor haben wir noch die Stammfunktionen

$$F(t) = \int f(t)\,\mathrm{d}t = \frac{1}{2}t^2 + 3t \qquad \text{und} \qquad G(t) = \int t\,\mathrm{d}t = \frac{1}{2}t^2.$$

Noch ein Beispiel

Wegen

$$\begin{aligned}
\int_3^{y(t)} \frac{1}{g(u)}\,\mathrm{d}u = \int_0^t f(s)\,\mathrm{d}s \quad &\iff \quad G(y(t)) - G(3) = F(t) - F(0) \\
&\iff \quad \frac{1}{2}y(t)^2 - \frac{9}{2} = \frac{1}{2}t^2 + 3t - 0 \\
&\iff \quad y(t)^2 = t^2 + 6t + 9 \\
&\iff \quad |y(t)| = \sqrt{t^2 + 6t + 9} \\
&\iff \quad y(t) = \pm\sqrt{t^2 + 6t + 9} = \pm(t+3)
\end{aligned}$$

kann $y(t)$ sowohl $t+3$ als auch $-t-3$ sein. Wegen $y(0) = 3$ scheidet $-t-3$ aus und wir erhalten

$$y(t) = t + 3$$

als einzige spezielle Lösung.

Methode 2

Gegeben: Homogene lineare Differentialgleichung 1. Ordnung

$$y'(t) + a(t) \cdot y(t) = 0$$

mit einer Funktion $a\colon I \to \mathbb{R}$.

Lösungsmethode:

1. Bestimme eine beliebige Stammfunktion $A(t) = \int a(t)\,\mathrm{d}t$ von $a(t)$.
2. Allgemeine Lösung:
$$y(t) = ce^{-A(t)} \qquad \text{für} \qquad c \in \mathbb{R}.$$
Spezielle Lösung für $y(t_0) = y_0$:
$$y(t) = y_0 e^{A(t_0) - A(t)}.$$

Beispiel

Aufgabe: Finde alle Lösungen zu

$$y'(t) - \frac{y(t)}{t+1} = 0.$$

Lösung: Es gilt $y'(t) - \frac{1}{t+1} \cdot y(t) = 0$, d.h. $a(t) = -\frac{1}{t+1}$.

1. Eine Stammfunktion von $a(t)$ ist

$$A(t) = \int a(t)\,\mathrm{d}t = \int -\frac{1}{t+1}\,\mathrm{d}t = -\ln|t+1|.$$

2. Die allgemeine Lösung lautet also:

$$y(t) = ce^{-A(t)} = ce^{\ln|t+1|} = c|t+1| \qquad \text{für} \qquad c \in \mathbb{R}.$$

Noch ein Beispiel

Aufgabe: Finde die spezielle Lösung zu

$$y'(t) - \frac{y(t)}{t+1} = 0 \qquad \text{mit} \qquad y(0) = 2.$$

Lösung: Es gilt $t_0 = 0$, $y_0 = 2$ und $y'(t) - \frac{1}{t+1} \cdot y(t) = 0$, d.h. $a(t) = -\frac{1}{t+1}$.

1. Aus dem Beispiel davor haben wir

$$A(t) = -\ln|t+1|.$$

2. Die spezielle Lösung lautet dann:

$$y(t) = y_0 e^{A(t_0)-A(t)} = 2e^{\ln|0+1|-(-\ln|t+1|)} = 2e^{\ln|t+1|} = 2|t+1|.$$

Methode 3

Gegeben: Inhomogene lineare Differentialgleichung 1. Ordnung

$$y'(t) + a(t) \cdot y(t) = f(t)$$

mit Funktionen $a, f : I \to \mathbb{R}$.

Lösungsmethode:

1. Bestimme eine beliebige Stammfunktion $A(t) = \int a(t)\ \mathrm{d}t$ von $a(t)$.
2. Allgemeine Lösung:

   $$y(t) = e^{-A(t)} \cdot (c + B(t)) \qquad \text{für} \qquad c \in \mathbb{R},$$

   wobei $B(t) = \int e^{A(t)} \cdot f(t)\ \mathrm{d}t$ eine beliebige Stammfunktion von $e^{A(t)} \cdot f(t)$ ist.
   Spezielle Lösung für $y(t_0) = y_0$:

   $$y(t) = e^{A(t_0) - A(t)} \cdot \left(y_0 + \int_{t_0}^{t} e^{A(s) - A(t_0)} \cdot f(s)\ \mathrm{d}s \right).$$

Beispiel

Aufgabe: Finde alle Lösungen zu

$$y'(t) - \cos(t) \cdot y(t) = \cos(t).$$

Lösung: Es gilt $a(t) = -\cos(t)$ und $f(t) = \cos(t)$.

1. Eine Stammfunktion von $a(t)$ ist

$$A(t) = \int a(t)\,\mathrm{d}t = \int -\cos(t)\,\mathrm{d}t = -\sin(t).$$

2. Eine Stammfunktion von $e^{A(t)} \cdot f(t)$ ist

$$B(t) = \int e^{A(t)} \cdot f(t)\,\mathrm{d}t = \int e^{-\sin(t)} \cdot \cos(t)\,\mathrm{d}t = -e^{-\sin(t)}.$$

Dann lautet die allgemeine Lösung:

$$y(t) = e^{-A(t)} \cdot (c + B(t)) \quad = e^{\sin(t)} \cdot \left(c - e^{-\sin(t)}\right) = ce^{\sin(t)} - 1 \qquad \text{für} \qquad c \in \mathbb{R}.$$

Noch ein Beispiel

Aufgabe: Finde die spezielle Lösung zu

$$y'(t) - \cos(t) \cdot y(t) = \cos(t) \qquad \text{mit} \qquad y(0) = 2.$$

Lösung: Es gilt $t_0 = 0$, $y_0 = 2$ und $a(t) = -\cos(t)$ und $f(t) = \cos(t)$.

1. Aus dem Beispiel davor haben wir

$$A(t) = -\sin(t).$$

Noch ein Beispiel

2. Die spezielle Lösung lautet dann:

$$
\begin{aligned}
y(t) &= e^{A(0)-A(t)} \cdot \left(2 + \int_0^t e^{A(s)-A(0)} \cdot f(s)\ \mathrm{d}s\right) \\
&= e^{-\sin(0)-(-\sin(t))} \cdot \left(2 + \int_0^t e^{-\sin(s)-(-\sin(0))} \cdot \cos(s)\ \mathrm{d}s\right) \\
&= e^{\sin(t)} \cdot \left(2 + \int_0^t e^{-\sin(s)} \cdot \cos(s)\ \mathrm{d}s\right) \\
&= e^{\sin(t)} \cdot \left(2 + \left[-e^{-\sin(s)}\right]_{s=0}^{t}\right) \\
&= e^{\sin(t)} \cdot \left(3 - e^{-\sin(t)}\right) \\
&= 3e^{\sin(t)} - 1.
\end{aligned}
$$

Methode 4

Gegeben: Homogene lineare Differentialgleichung 2. Ordnung

$$y''(t) + ay'(t) + by(t) = 0.$$

mit konstanten Koeffizienten $a, b \in \mathbb{R}$.

Lösungsmethode falls $a^2 > 4b$:

1. Bestimme beide Lösungen λ_1, λ_2 der charakteristischen Gleichung $\lambda^2 + a\lambda + b = 0$, d.h.

$$\lambda_1 = -\frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 - b} \qquad \text{und} \qquad \lambda_2 = -\frac{a}{2} - \sqrt{\left(\frac{a}{2}\right)^2 - b}.$$

2. Die allgemeine Lösung für $y(t)$ lautet dann:

$$y(t) = c_1 e^{\lambda_1 t} + c_2 e^{\lambda_2 t} \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Methode 4

Lösungsmethode falls $a^2 = 4b$:

1. Bestimme die eindeutige Lösung λ der charakteristischen Gleichung $\lambda^2 + a\lambda + b = 0$, d.h.

$$\lambda_0 = -\frac{a}{2}.$$

2. Die allgemeine Lösung für $y(t)$ lautet dann:

$$y(t) = (c_1 + c_2 t)e^{\lambda_0 t} \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Methode 4

Lösungsmethode falls $a^2 < 4b$:

1. Bestimme α und β, so dass beide Lösungen λ_1, λ_2 der charakteristischen Gleichung $\lambda^2 + a\lambda + b = 0$ von den Formen $\lambda_1 = \alpha + \beta i$ und $\lambda_2 = \alpha - \beta i$ sind, d.h.

$$\alpha = -\frac{a}{2} \qquad \text{und} \qquad \beta = \sqrt{b - \left(\frac{a}{2}\right)^2}.$$

2. Die allgemeine Lösung für $y(t)$ lautet dann:

$$y(t) = (c_1 \cos(\beta t) + c_2 \sin(\beta t))e^{\alpha t} \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Sucht man die spezielle Lösung für Anfangsbedingungen $y(t_0) = y_0$ und $y'(t_1) = y_1$, dann setzt man $t = t_0$ und $t = t_1$ in die allgemeine Lösung ein und bestimmt c_1 und c_2.

Beispiel

Aufgabe: Finde alle Lösungen zu

$$y''(t) - y(t) = 0.$$

Lösung: Es gilt $a = 0$ und $b = -1$, d.h. $a^2 > 4b$.

1. Die Lösungen der charakteristischen Gleichung sind $\lambda_1 = -1$ und $\lambda_2 = 1$.
2. Die allgemeine Lösung lautet:

$$y(t) = c_1 e^{\lambda_1 t} + c_2 e^{\lambda_2 t} = c_1 e^{-t} + c_2 e^{t} \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Methode 5

Gegeben: Inhomogene lineare Differentialgleichung 2. Ordnung

$$y''(t) + ay'(t) + by(t) = a_n t^n + \ldots + a_1 t + a_0.$$

mit konstanten Koeffizienten $a, b, a_1, \ldots, a_n \in \mathbb{R}$ $(b, a_n \neq 0)$.

Lösungsmethode:

1. Bestimme die allgemeine Lösung $y_h(t)$ von

$$y_h''(t) + ay_h'(t) + by_h(t) = 0.$$

2. Stelle ein Polynom

$$y_p(t) = b_n t^n + \ldots + b_1 t + b_0$$

mit Parametern $b_0, b_1, \ldots, b_n$ auf.

Methode 5

3. Setze $y_p(t)$, $y_p'(t)$ und $y_p''(t)$ in

$$y_p''(t) + ay_p'(t) + by_p(t) = p(t)$$

ein und ermittle die Werte von $b_0, b_1, \ldots, b_n$ durch Koeffizientenvergleich.

4. Die allgemeine Lösung für $y(t)$ lautet dann:

$$y(t) = y_h(t) + y_p(t) \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Sucht man die spezielle Lösung für Anfangsbedingungen $y(t_0) = y_0$ und $y'(t_1) = y_1$, dann setzt man $t = t_0$ und $t = t_1$ in die allgemeine Lösung ein und bestimmt c_1 und c_2.

Beispiel

Aufgabe: Finde alle Lösungen zu

$$y''(t) - y(t) = t - 2.$$

Lösung: Es sind $a = 0$, $b = -1$ und $p(t) = t - 2$ Polynom mit Grad 1.

1. Die allgemeine Lösung von $y_h''(t) - y_h(t) = 0$ ist

   $$y_h(t) = c_1 e^{-t} + c_2 e^{t} \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

   (Siehe Folie 1708.)

2. Wegen $n = \deg(p) = 1$ gilt: $y_p(t) = a_1 t + a_0$.

Beispiel

3. Mit $y_p'(t) = a_1$ und $y_p''(t) = 0$ erhält man:

$$\begin{aligned} y''(t) - y(t) = t - 2 \quad &\iff \quad 0 - (a_1 t + a_0) = t - 2 \\ &\iff \quad -a_1 t - a_0 = t - 2 \\ &\iff \quad a_1 = -1, a_0 = 2. \end{aligned}$$

   D.h. $y_p(t) = -t + 2$.

4. Die allgemeine Lösung lautet:

$$y(t) = y_h(t) + y_p(t) = c_1 e^{-t} + c_2 e^{t} - t + 2 \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Methode 6

Gegeben: Inhomogene lineare Differentialgleichung 2. Ordnung

$$y''(t) + ay'(t) + by(t) = e^{\alpha t}(a_1 \cos(\beta t) + a_2 \sin(\beta t)).$$

mit konstanten Koeffizienten $a, b, \alpha, \beta, a_1, a_2 \in \mathbb{R}$ $(b \neq 0)$.

Lösungsmethode:

1. Bestimme die allgemeine Lösung $y_h(t)$ von

$$y_h''(t) + ay_h'(t) + by_h(t) = 0.$$

2. Stelle $y_p(t) = e^{\alpha t}(b_1 \cos(\beta t) + b_2 \sin(\beta t))$ in Abhängigkeit von Parametern b_1, b_2 auf.
3. Setze $y_p(t)$, $y_p'(t)$ und $y_p''(t)$ in

$$y_p''(t) + ay_p'(t) + by_p(t) = e^{\alpha t}(a_1 \cos(\beta t) + a_2 \sin(\beta t))$$

ein und ermittle die Werte von b_1 und b_2.

Methode 6

4. Die allgemeine Lösung für $y(t)$ lautet dann:

$$y(t) = y_h(t) + y_p(t) \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Sucht man die spezielle Lösung für Anfangsbedingungen $y(t_0) = y_0$ und $y'(t_1) = y_1$, dann setzt man $t = t_0$ und $t = t_1$ in die allgemeine Lösung ein und bestimmt c_1 und c_2.

Beispiel

Aufgabe: Finde alle Lösungen zu

$$y''(t) - y(t) = \sin(t).$$

Lösung: Es gilt $a = 0$, $b = -1$, $\alpha = 0$, $\beta = 1$, $a_1 = 0$ und $a_2 = 1$.

1. Die allgemeine Lösung von $y_h''(t) - y_h(t) = 0$ ist

   $$y_h(t) = c_1 e^{-t} + c_2 e^{t} \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

   (Siehe Folie 1708.)

2. Es gilt:

   $$y_p(t) = b_1 \cos(t) + b_2 \sin(t).$$

Beispiel

3. Mit $y_p'(t) = -b_1 \sin(t) + b_2 \cos(t)$ und $y_p''(t) = -b_1 \cos(t) - b_2 \sin(t)$ erhält man:

$$\begin{aligned} y''(t) - y(t) = \sin(t) \quad &\iff \quad -b_1 \cos(t) - b_2 \sin(t) - (b_1 \cos(t) + b_2 \sin(t)) = \sin(t) \\ &\iff \quad -2b_1 \cos(t) - 2b_2 \sin(t) = \sin(t) \\ &\iff \quad b_1 = 0, b_2 = -\frac{1}{2}. \end{aligned}$$

   D.h. $y_p(t) = -\frac{1}{2} \sin(t)$.

4. Die allgemeine Lösung lautet dann:

$$y(t) = y_h(t) + y_p(t) = c_1 e^{-t} + c_2 e^{t} - \frac{1}{2} \sin(t) \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Wie kann man eine inhomogene Differentialgleichung 2. Ordnung der Form

$$y''(t) + ay'(t) = f(t)$$

lösen?

Weil sie inhomogen ist und Ordnung 2 hat, kommen Methoden 1-4 nicht infrage. Weil Methoden 5 und 6 $b \neq 0$ fordern, kann man sie auch nicht benutzen.

Eine Möglichkeit ist $z(t) = y'(t)$ zu setzen, die Differentialgleichung

$$z'(t) + az(t) = f(t)$$

mit Methode 3 lösen und die Menge aller Stammfunktionen von $z(t)$ als allgemeine Lösung von $y(t)$ angeben.

Lineare Systeme von Differentialgleichungen

Gegeben: Eine Gleichung der Form

$$y'(t) = Ay(t)$$

für $A \in \mathbb{R}^{n \times n}$ und $y \colon \mathbb{R} \to \mathbb{R}^n$.

Lösungsmethode:

1. Berechne die Eigenwerte $\lambda_1, \ldots, \lambda_k$ von A, d.h. die Nullstellen von $\chi_A(\lambda) = \det(A - \lambda I_n)$. (Hier habe ich k statt n benutzt, weil es nicht immer genau n Eigenwerte sind.)
2. Berechne die zugehörigen Eigenvektoren $v_1, \ldots, v_k$. Für alle $i = 1, \ldots, k$ soll gelten:

$$(A - \lambda_i I_n) v_i = 0.$$

3. Die allgemeine Lösung für $y(t)$ lautet dann:

$$y(t) = c_1 e^{\lambda_1 t} v_1 + \ldots + c_k e^{\lambda_k t} v_k \qquad \text{für} \qquad c_1, \ldots, c_k \in \mathbb{R}.$$

Beispiel

Aufgabe: Finde alle Lösungen zu $y'(t) = Ay(t)$ für $y\colon \mathbb{R} \to \mathbb{R}^2$ und $A \in \mathbb{R}^{2\times 2}$ mit

$$A = \begin{pmatrix} 1 & 2 \\ -1 & 4 \end{pmatrix}, \qquad \text{d.h.} \qquad \begin{pmatrix} y_1'(t) \\ y_2'(t) \end{pmatrix} = \begin{pmatrix} y_1(t) + 2y_2(t) \\ -y_1(t) + 4y_2(t) \end{pmatrix}.$$

Lösung:

1. Nach Folie 1681 gilt:

$$\chi_A(\lambda) = \det \begin{pmatrix} 1-\lambda & 2 \\ -1 & 4-\lambda \end{pmatrix} = (1-\lambda)(4-\lambda) - 2 \cdot (-1) = \lambda^2 - 5\lambda + 6.$$

Somit sind $\lambda_1 = \frac{5}{2} + \sqrt{\left(\frac{5}{2}\right)^2 - 6} = 3$ und $\lambda_2 = \frac{5}{2} - \sqrt{\left(\frac{5}{2}\right)^2 - 6} = 2$ die Eigenwerte von A.

Beispiel

2. Für die zugehörigen Eigenvektoren $v_1 = \begin{pmatrix} v_{11} \\ v_{12} \end{pmatrix}$ und $v_2 = \begin{pmatrix} v_{21} \\ v_{22} \end{pmatrix}$ gilt:

$$\begin{pmatrix} -2 & 2 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} v_{11} \\ v_{12} \end{pmatrix} = 0 \qquad \text{und} \qquad \begin{pmatrix} -1 & 2 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} v_{11} \\ v_{12} \end{pmatrix} = 0,$$

d.h.:

$$\begin{array}{rcrcl} -2v_{11} & + & 2v_{12} & = & 0 \\ -v_{11} & + & v_{12} & = & 0 \end{array} \qquad \text{und} \qquad \begin{array}{rcrcl} -v_{11} & + & 2v_{12} & = & 0 \\ -v_{11} & + & 2v_{12} & = & 0 \end{array}.$$

Mögliche Lösungen für die zwei Gleichungssysteme sind $v_{11} = 1$, $v_{12} = 1$, $v_{21} = 2$ und $v_{22} = 1$, d.h.:

$$v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \text{und} \qquad v_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Beispiel

3. Die allgemeine Lösung für $y(t)$ lautet dann:

$$y(t) = c_1 e^{3t} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + c_2 e^{2t} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} c_1 e^{3t} + 2c_2 e^{2t} \\ c_1 e^{3t} + c_2 e^{2t} \end{pmatrix} \qquad \text{für} \qquad c_1, c_2 \in \mathbb{R}.$$

Themenübersicht

Themenübersicht

Diskrete Wahrscheinlichkeitsräume

Ein diskreter Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ besteht aus

- einer abzählbaren Ergebnismenge

$$\Omega = \{\omega_1, \omega_2, \omega_3, \ldots\}$$

- und einem Wahrscheinlichkeitsmaß

$$\Pr\colon \Omega \to [0, 1]$$

  wobei $\sum_{\omega \in \Omega} \Pr[\omega] = 1$ gelten muss.

Ω darf endlich oder abzählbar unendlich sein. Bei Laplaceschen Wahrscheinlichkeitsräumen ist Ω endlich und es gilt $\Pr[\omega] = \frac{1}{|\Omega|}$ für alle $\omega \in \Omega$.

Wichtig!

Jedes mal, wenn ein Wahrscheinlichkeitsraum definiert werden soll, sollte man:

1. Ω definieren (z.B. intensional oder extensional),
2. argumentieren, dass $\Pr[\omega] \geq 0$ für alle $\omega \in \Omega$ gilt und
3. $\sum_{\omega \in \Omega} \Pr[\omega] = 1$ zeigen.

Ein kleines Beispiel

Wir modellieren das Werfen eines fairen Würfels als Laplaceschen Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ mit $\Omega = [6]$ und $\Pr[k] = \frac{1}{6}$ für alle $k \in [6]$.

W ist gültig, da $\frac{1}{6} \geq 0$ und

$$\sum_{\omega \in \Omega} \Pr[\omega] = \sum_{k=1}^{6} \frac{1}{6} = 1. \qquad \checkmark$$

Ein beliebig großes Beispiel

Wir betrachten eine Urne mit Kugeln. Eine davon ist mit „1“ beschriftet, zwei mit „2“, drei mit „3“, usw. Insgesamt enthält die Urne also $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ Kugeln für ein $n \in \mathbb{N}$. Wir modellieren das Ziehen einer Kugel als nicht-Laplaceschen Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ mit $\Omega = [n]$ und

$$\Pr[k] = \frac{k}{n(n+1)/2} = \frac{2k}{n(n+1)}$$

für alle $k \in [n]$.

W ist gültig, da $\frac{2k}{n(n+1)} \geq 0$ und

$$\sum_{\omega \in \Omega} \Pr[\omega] = \sum_{k=1}^{n} \frac{2k}{n(n+1)} = \frac{2}{n(n+1)} \cdot \sum_{k=1}^{n} k = \frac{2}{n(n+1)} \cdot \frac{n(n+1)}{2} = 1. \qquad \checkmark$$

Ein unendlich großes Beispiel

Wir modellieren das Werfen einer fairen Münze bis das erste mal *Kopf* erscheint als unendlichen Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ mit $\Omega = \mathbb{N}$ und $\Pr[k] = \left(\frac{1}{2}\right)^k$ für alle $k \in \Omega$.

W ist gültig, da $\left(\frac{1}{2}\right)^k \geq 0$ für alle $k \in \Omega$ und

$$\sum_{\omega \in \Omega} \Pr[\omega] = \sum_{k=1}^{\infty} \left(\frac{1}{2}\right)^k = \sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^k - 1 \overset{(*)}{=} \frac{1}{1 - \frac{1}{2}} - 1 = 1. \qquad \checkmark$$

$(*)$ siehe nächste Folie.

Wichtig!

In der letzten Folie wurde an der Stelle $(*)$ die geometrische Reihe benutzt. Diese besagt, dass

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$$

für alle $x \in \mathbb{R}$ mit $|x| < 1$ gilt.

Diese Reihe ist mit Abstand die wichtigste in DWT. Schreibt sie euch unbedingt auf.

Info

Elementarereignisse müssen nicht immer Zahlen sein! Man kann den Ergebnisraum Ω beliebig definieren: als Zahlenmenge, als Tupelmenge, als Menge von Wörtern, als Menge von Mengen, etc.

Für das Beispiel auf Folie 1729 hätten wir beispielsweise auch

$$\Omega = \left\{ Z^k K \;\middle|\; k \in \mathbb{N}_0 \right\} = \{K, ZK, ZZK, ZZZK, ZZZZK, \ldots\}$$

mit $\Pr[\omega] = \left(\frac{1}{2}\right)^{|\omega|}$ für alle $\omega \in \Omega$ wählen können.

Ereignisse

Ein Ereignis $E \subseteq \Omega$ ist nichts anderes als eine Menge von Elementarereignissen. Man beschreibt sie auch öfter durch eine beliebige Eigenschaft in der Form

$$E : „\ldots“,$$

wobei immer $E = \{\omega \in \Omega \mid „\ldots“\}$ gemeint ist. Die Wahrscheinlichkeit eines Ereignisses ist definiert als:

$$\Pr[E] = \sum_{\omega \in E} \Pr[\omega].$$

In Laplaceschen Wahrscheinlichkeitsräumen gilt immer $\Pr[E] = \frac{|E|}{|\Omega|}$.

Das kleine Beispiel nochmal

Wir betrachten wieder die Modellierung aus Folie 1727 für das Werfen eines fairen Würfels mit $\Omega = [6]$ und $\Pr[k] = \frac{1}{6}$ für alle $k \in [6]$.

Mögliche Ereignisse wären:

1. E_1 : „Die Augenzahl ist prim“, d.h. $E_1 = \{2, 3, 5\}$.
2. E_2 : „Die Augenzahl ist nicht zwei“, d.h. $E_2 = [6] \setminus \{2\} = \{1, 3, 4, 5, 6\}$.
3. E_3 : „Die Augenzahl ist prim, aber keine zwei“, d.h. $E_3 = E_1 \cap E_2 = \{3, 5\}$.

Für diese Ereignisse gilt:

1. $\Pr[E_1] = \Pr[\{2, 3, 5\}] = \Pr[2] + \Pr[3] + \Pr[5] = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$,
2. $\Pr[E_2] = 1 - \Pr[2] = 1 - \frac{1}{6} = \frac{5}{6}$,
3. $\Pr[E_3] = \Pr[\{3, 5\}] = \Pr[3] + \Pr[5] = \frac{1}{6} + \frac{1}{6} = \frac{1}{3}$.

Info

Logische Verknüpfungen wie *und*, *oder*, *nicht*, *entweder oder* usw. bedeuten nichts anderes als Mengenoperationen wie

$$E_1 \cap E_2, \qquad E_1 \cup E_2, \qquad \overline{E_1}, \qquad E_1 \Delta E_2,$$

usw.

Das unendlich große Beispiel nochmal

Wir betrachten wieder die Modellierung aus Folie 1729 für das Werfen einer fairen Münze, bis zum ersten mal *Kopf* erscheint, mit $\Omega = \mathbb{N}$ und $\Pr[k] = \left(\frac{1}{2}\right)^k$ für alle $k \in \Omega$.

Ein mögliches Ereignis wäre:

$$E : \text{„Die Anzahl der Würfe ist ungerade“}$$

Formal:

$$E = \{k \in \Omega \mid k \text{ ist ungerade}\},$$

mit:

$$\begin{aligned}\Pr[E] &= \left(\frac{1}{2}\right)^1 + \left(\frac{1}{2}\right)^3 + \left(\frac{1}{2}\right)^5 + \left(\frac{1}{2}\right)^7 + \left(\frac{1}{2}\right)^9 + \left(\frac{1}{2}\right)^{11} + \left(\frac{1}{2}\right)^{13} + \dots \\ &= \sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^{2k+1} = \frac{1}{2} \cdot \sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^{2k} = \frac{1}{2} \cdot \sum_{k=0}^{\infty} \left(\frac{1}{4}\right)^k \overset{(*)}{=} \frac{1}{2} \cdot \frac{1}{1 - \frac{1}{4}} = \frac{2}{3}\end{aligned}$$

$(*)$ da ist sie wieder, die geometrische Reihe!

Einige Rechenregeln

$A_1, \ldots, A_n$ seien beliebige Ereignisse über ein beliebiges Ω.

- Falls $A_1, \ldots, A_n$ disjunkt sind, dann gilt:

$$\Pr\left[\bigcup_{k=1}^{n} A_k\right] = \sum_{k=1}^{n} \Pr[A_k] \qquad \text{(Additionssatz)}$$

- Es gilt immer:

$$\Pr\left[\bigcup_{k=1}^{n} A_k\right] \leq \sum_{k=1}^{n} \Pr[A_k] \qquad \text{(Bool'sche Ungleichung)}$$

Info

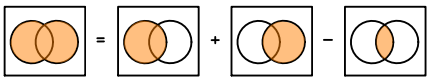
Diese Regeln gelten auch für $n \to \infty$.

Inklusion und Exklusion bzw. Siebformel (für $n = 2$)

Für beliebige Ereignisse A und B gilt:

$$\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B].$$

Graphisch:

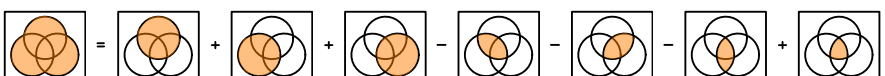


Inklusion und Exklusion bzw. Siebformel (für $n = 3$)

Für beliebige Ereignisse A, B und C gilt:

$$\Pr[A \cup B \cup C] = \Pr[A] + \Pr[B] + \Pr[C] - \Pr[A \cap B] - \Pr[A \cap C] - \Pr[B \cap C] + \Pr[A \cap B \cap C].$$

Graphisch:



Inklusion und Exklusion bzw. Siebformel (für ein allgemeines n)

Für beliebige Ereignisse $A_1, \ldots, A_n$ gilt:

$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{S \subseteq [n], S \neq \emptyset} (-1)^{|S|-1} \cdot \Pr\left[\bigcap_{i \in S} A_i\right].$$

- Das Summenzeichen $\sum_{S \subseteq [n], S \neq \emptyset}$ summiert über alle möglichen nichtleeren Teilmengen von $[n]$.
- Der Ausdruck $(-1)^{|S|-1}$ ist für den Vorzeichenwechsel zuständig. Ist $|S|$ gerade, so hat $\Pr\left[\bigcap_{i \in S} A_i\right]$ Minus als Vorzeichen. Ist $|S|$ ungerade, so hat $\Pr\left[\bigcap_{i \in S} A_i\right]$ Plus als Vorzeichen.

Beispiel ($n = 2$)

$$\begin{aligned}
\Pr[A_1 \cup A_2] &= \sum\nolimits_{S \subseteq [2], S \neq \emptyset} (-1)^{|S|-1} \cdot \Pr\left[\bigcap\nolimits_{i \in S} A_i\right] \\
&= \Pr\left[\bigcap\nolimits_{i \in \{1\}} A_i\right] + \Pr\left[\bigcap\nolimits_{i \in \{2\}} A_i\right] - \Pr\left[\bigcap\nolimits_{i \in \{1,2\}} A_i\right] \\
&= \Pr[A_1] + \Pr[A_2] - \Pr[A_1 \cap A_2].
\end{aligned}$$

Noch ein Beispiel ($n = 3$)

$$
\begin{aligned}
\Pr[A_1 \cup A_2 \cup A_3] &= \sum\nolimits_{S \subseteq [3], S \neq \emptyset} (-1)^{|S|-1} \cdot \Pr\left[\bigcap\nolimits_{i \in S} A_i\right] \\
&= \Pr\left[\bigcap\nolimits_{i \in \{1\}} A_i\right] + \Pr\left[\bigcap\nolimits_{i \in \{2\}} A_i\right] + \Pr\left[\bigcap\nolimits_{i \in \{3\}} A_i\right] - \Pr\left[\bigcap\nolimits_{i \in \{1,2\}} A_i\right] \\
&\quad - \Pr\left[\bigcap\nolimits_{i \in \{1,3\}} A_i\right] - \Pr\left[\bigcap\nolimits_{i \in \{2,3\}} A_i\right] + \Pr\left[\bigcap\nolimits_{i \in \{1,2,3\}} A_i\right] \\
&= \Pr[A_1] + \Pr[A_2] + \Pr[A_3] - \Pr[A_1 \cap A_2] \\
&\quad - \Pr[A_1 \cap A_3] - \Pr[A_2 \cap A_3] + \Pr[A_1 \cap A_2 \cap A_3].
\end{aligned}
$$

Beweis der Siebformel (für Interessierte)

Mit vollständiger Induktion nach der Anzahl n der vorhandenen Mengen.

- Induktionsanfang ($n = 2$):
  Da A_1 und $A_2 \setminus (A_1 \cap A_2)$ disjunkt sind, gilt:

$$\Pr[A_1 \cup (A_2 \setminus (A_1 \cap A_2))] = \Pr[A_1] + \Pr[A_2 \setminus (A_1 \cap A_2)].$$

  Da $A_1 \cap A_2$ und $A_2 \setminus (A_1 \cap A_2)$ ebenfalls disjunkt sind, gilt:

$$\Pr[A_2] = \Pr[(A_1 \cap A_2) \cup (A_2 \setminus (A_1 \cap A_2))] = \Pr[A_1 \cap A_2] + \Pr[A_2 \setminus (A_1 \cap A_2)],$$

  d.h.

$$\Pr[A_2 \setminus (A_1 \cap A_2)] = \Pr[A_2] - \Pr[A_1 \cap A_2].$$

  Aus $A_1 \cup A_2 = A_1 \cup (A_2 \setminus (A_1 \cap A_2))$ folgt:

$$\begin{aligned}\Pr[A_1 \cup A_2] &= \Pr[A_1 \cup (A_2 \setminus (A_1 \cap A_2))] \\ &= \Pr[A_1] + \Pr[A_2 \setminus (A_1 \cap A_2)] \\ &= \Pr[A_1] + \Pr[A_2] - \Pr[A_1 \cap A_2].\end{aligned}$$

Beweis der Siebformel (für Interessierte)

- Induktionsschritt: Sei $n \in \mathbb{N}$ beliebig mit

$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{S \subseteq [n], S \neq \emptyset} (-1)^{|S|-1} \cdot \Pr\left[\bigcap_{i \in S} A_i\right]$$

für beliebige endliche Mengen $A_1, \ldots, A_n$.

Seien nun $A_1, \ldots, A_{n+1}$ beliebige endliche Mengen. Dann gilt:

Beweis der Siebformel (für Interessierte)

$$\begin{aligned}
\Pr\left[\bigcup_{i=1}^{n+1} A_i\right] &= \Pr\left[\left(\bigcup_{i=1}^{n} A_i\right) \cup A_{n+1}\right] = \Pr\left[\bigcup_{i=1}^{n} A_i\right] + |A_{n+1}| - \Pr\left[\left(\bigcup_{i=1}^{n} A_i\right) \cap A_{n+1}\right] \\
&= \Pr\left[\bigcup_{i=1}^{n} A_i\right] + |A_{n+1}| - \Pr\left[\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\right] \\
&= \sum_{S\subseteq[n],S\neq\emptyset} (-1)^{|S|-1} \cdot \Pr\left[\bigcap_{i\in S} A_i\right] + |A_{n+1}| - \sum_{S\subseteq[n],S\neq\emptyset} (-1)^{|S|-1} \cdot \Pr\left[\bigcap_{i\in S} (A_i \cap A_{n+1})\right] \\
&= \sum_{\substack{S\subseteq[n+1],S\neq\emptyset \\ n+1\notin S}} (-1)^{|S|-1} \cdot \Pr\left[\bigcap_{i\in S} A_i\right] + \sum_{\substack{S\subseteq[n+1],S\neq\emptyset \\ n+1\in S}} (-1)^{|S|-1} \cdot \Pr\left[\bigcap_{i\in S} A_i\right] \\
&= \sum_{\substack{S\subseteq[n+1], \\ S\neq\emptyset}} (-1)^{|S|-1} \cdot \Pr\left[\bigcap_{i\in S} A_i\right].
\end{aligned}$$

□

Spezialfall

Falls die Wahrscheinlichkeit einer Schnittmenge von k Ereignissen nur von der Anzahl k an beteiligten Ereignissen und nicht von den Ereignissen selbst abhängig ist, dann gilt:

$$\Pr\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{S\subseteq[n],S\neq\emptyset} (-1)^{|S|-1} \cdot \Pr\left[\bigcap_{i\in S} A_i\right] = \sum_{k=1}^{n} (-1)^{k-1} \cdot \binom{n}{k} \cdot \Pr\left[\bigcap_{i=1}^{k} A_i\right]$$

Es gibt genau $\binom{n}{k}$ k-elementige Teilmengen von $[n]$. Sind alle Summanden $\Pr\left[\bigcap_{i\in S} A_i\right]$ für $|S| = k$ gleich, dann kann man $\binom{n}{k}$ mal einen beliebigen nehmen, z.B. $\Pr\left[\bigcap_{i=1}^{k} A_i\right]$.

Beispiel

4 verschiedene Gäste bestellen beim selben Kellner 4 verschiedene Gerichte. Dummerweise vergisst der Kellner sofort, wer was bestellt hat, und beschließt, die Verteilung der Gerichte dem Zufall zu überlassen. Mit welcher Wahrscheinlichkeit bekommt keiner der 4 Gäste seine Bestellung?

Wir definieren Ω als alle $4! = 24$ möglichen Verteilungen (Permutationen) und für $i = 1, 2, 3, 4$ definieren wir A_i als dasjenige Ereignis, bei dem Gast i sein bestelltes Essen bekommt. $A_1 \cup A_2 \cup A_3 \cup A_4$ ist somit das Ereignis, dass mindestens ein Gast sein bestelltes Essen bekommt.

Wir sind also an der Wahrscheinlichkeit

$$\Pr\left[\overline{A_1 \cup A_2 \cup A_3 \cup A_4}\right] = 1 - \Pr[A_1 \cup A_2 \cup A_3 \cup A_4]$$

interessiert.

Beispiel

Mit

$$\begin{aligned}
\Pr[A_1] &= \tfrac{3!}{4!} = \tfrac{1}{4},\\
\Pr[A_1 \cap A_2] &= \tfrac{2!}{4!} = \tfrac{1}{12},\\
\Pr[A_1 \cap A_2 \cap A_3] &= \tfrac{1!}{4!} = \tfrac{1}{24},\\
\Pr[A_1 \cap A_2 \cap A_3 \cap A_4] &= \tfrac{0!}{4!} = \tfrac{1}{24}
\end{aligned}$$

folgt:

$$\begin{aligned}
\Pr[A_1 \cup A_2 \cup A_3 \cup A_4] &= \binom{4}{1} \cdot \frac{1}{4} - \binom{4}{2} \cdot \frac{1}{12} + \binom{4}{3} \cdot \frac{1}{24} - \binom{4}{4} \cdot \frac{1}{24}\\
&= 1 - \frac{1}{2} + \frac{1}{6} - \frac{1}{24} = \frac{5}{8}.
\end{aligned}$$

D.h. mit Wahrscheinlichkeit $\frac{5}{8}$ bekommt mindestens ein Gast sein bestelltes Essen und mit Wahrscheinlichkeit $1 - \frac{5}{8} = \frac{3}{8} = 0.375$ keiner der 4.

Info:

Beispiel

Hier durfte man den Spezialfall der Siebformel verwenden, weil die Kardinalität jeder Schnittmenge nur von der Anzahl an beteiligten Ereignissen und nicht von den Mengen selbst anhängig ist, d.h.:

$$\Pr[A_1] = \Pr[A_2] = \Pr[A_3] = \Pr[A_4] = \frac{3!}{4!},$$

$$\Pr[A_1 \cap A_2] = \Pr[A_1 \cap A_3] = \Pr[A_1 \cap A_4] = \Pr[A_2 \cap A_3] = \Pr[A_2 \cap A_4] = \Pr[A_3 \cap A_4] = \frac{2!}{4!},$$

$$\Pr[A_1 \cap A_2 \cap A_3] = \Pr[A_1 \cap A_2 \cap A_4] = \Pr[A_1 \cap A_3 \cap A_4] = \Pr[A_2 \cap A_3 \cap A_4] = \frac{1!}{4!},$$

$$\Pr[A_1 \cap A_2 \cap A_3 \cap A_4] = \frac{0!}{4!}.$$

Übungsaufgabe

Gegeben seien ein Alphabet $\Sigma = \{a, b, c, d\}$, eine Ergebnismenge $\Omega = \{w \in \Sigma^* \mid |w| = 6\}$ mit $\Pr[\omega] = \frac{1}{|\Omega|}$ für alle $w \in \Omega$ und folgende Ereignisse $A, B, C, D \subseteq \Omega$:

$$A = \{w \in \Omega \mid \text{in } w \text{ kommt kein } a \text{ vor}\}, \qquad B = \{w \in \Omega \mid \text{in } w \text{ kommt kein } b \text{ vor}\},$$
$$C = \{w \in \Omega \mid \text{in } w \text{ kommt kein } c \text{ vor}\}, \qquad D = \{w \in \Omega \mid \text{in } w \text{ kommt kein } d \text{ vor}\}.$$

Bestimme die Wahrscheinlichkeit mit der ein Wort $w \in \Omega$ jedes der Zeichen aus Σ mindestens einmal enthält.

Hinweise:

- Betrachte das Ereignis $A \cup B \cup C \cup D$.
- Beachte, dass für $k = 1, 2, 3, 4$ die Wahrscheinlichkeit der Schnittmenge von k Ereignissen aus A, B, C, D nur von k und nicht von den Ereignissen selbst abhängig ist.

Es gibt n^k Wörter der Länge k über einem n-elementigen Alphabet, d.h. $|\Omega| = 4^6$. Für die Wahrscheinlichkeit von $A \cup B \cup C \cup D$ gilt nach dem Spezialfall der Siebformel für $n = 4$:

$$\begin{aligned}
\Pr[A \cup B \cup C \cup D] &= \binom{4}{1} \Pr[A] - \binom{4}{2} \Pr[A \cap B] + \binom{4}{3} \Pr[A \cap B \cap C] - \binom{4}{4} \Pr[A \cap B \cap C \cap D] \\
&= 4 \Pr[A] - 6 \Pr[A \cap B] + 4 \Pr[A \cap B \cap C] - \Pr[A \cap B \cap C \cap D] \\
&= 4 \cdot \frac{3^6}{4^6} - 6 \cdot \frac{2^6}{4^6} + 4 \cdot \frac{1^6}{4^6} - \frac{0^6}{4^6} \\
&= \frac{2536}{4^6} \\
&\approx 0.62.
\end{aligned}$$

Die gesuchte Wahrscheinlichkeit beträgt dann $1 - \frac{2536}{4^6} \approx 1 - 0.62 = 0.38$.

Übungsaufgabe

Mit einem fairen Würfel wird 5 mal hintereinander gewürfelt. Bestimme die Wahrscheinlichkeit mit der mindestens drei mal hintereinander eine 6 gewürfelt wurde.

Tipp: Benutze folgende Ereignisse A, B und C.

A : Bei den ersten drei Würfen kommt 6 raus.
B : Bei den mittleren drei Würfen kommt 6 raus.
C : Bei den letzten drei Würfen kommt 6 raus.

Von den insgesamt 6^6 Wurfkombinationen enthält A diejenigen der Form (⚅, ⚅, ⚅, ?, ?, ?). Das sind genau 6^3. Daher gilt beispielsweise

$$\Pr[A] = \frac{6^3}{6^6} = \frac{1}{6^3}.$$

Analog berechnet man:

Ereignis	Form	Anzahl	Wahrscheinlichkeit
A	(⚅, ⚅, ⚅, ?, ?, ?)	6^2	$1/6^3$
B	(?, ⚅, ⚅, ⚅, ?)	6^2	$1/6^3$
C	(?, ?, ⚅, ⚅, ⚅)	6^2	$1/6^3$
$A \cap B$	(⚅, ⚅, ⚅, ⚅, ?)	6	$1/6^4$
$A \cap C$	(⚅, ⚅, ⚅, ⚅, ⚅)	1	$1/6^5$
$B \cap C$	(?, ⚅, ⚅, ⚅, ⚅)	6	$1/6^4$
$A \cap B \cap C$	(⚅, ⚅, ⚅, ⚅, ⚅)	1	$1/6^5$

Für die gesuchte Wahrscheinlichkeit $\Pr[A \cup B \cup C]$ gilt dann:

$$\Pr[A \cup B \cup C] = \frac{1}{6^3} + \frac{1}{6^3} + \frac{1}{6^3} - \frac{1}{6^4} - \frac{1}{6^5} - \frac{1}{6^4} + \frac{1}{6^5} = \frac{1}{81}.$$

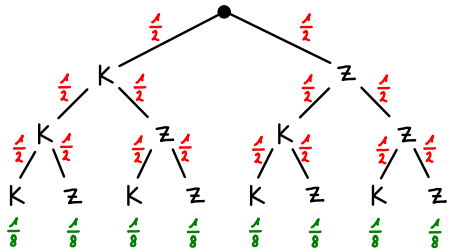
Mehrstufige Experimente

Experimente, die aus endlich vielen Schritten bestehen, lassen sich sehr schön mit Baumdiagrammen modellieren. Dabei gilt:

- Die Elementarereignisse sind die Pfade von der Wurzel zu den Blättern.
- Die Summe der Wahrscheinlichkeiten aller Kanten, die einen Knoten verlassen, ist 1.
- Die Wahrscheinlichkeit eines Pfades ist das Produkt der Kantengewichte.

Beispiel

Eine faire Münze wird drei mal geworfen. Bei jedem Wurf erhalten wir entweder *Kopf* („K“) oder *Zahl* („Z“), jeweils mit Wahrscheinlichkeit $\frac{1}{2}$.



Ein möglicher Wahrscheinlichkeitsraum ist $W = (\Omega, \Pr)$ mit

$$\Omega = \{K, Z\}^3 = \{KKK, KKZ, KZK, KZZ, ZKK, ZKZ, ZZK, ZZZ\}$$

und $\Pr[\omega] = \left(\frac{1}{2}\right)^3 = \frac{1}{8}$ für alle $\omega \in \Omega$.

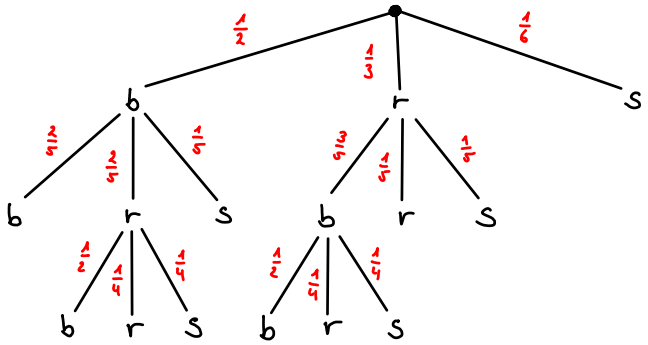
Noch ein Beispiel

Eine Schublade enthält 3 blaue und 2 rote Socken. Außerdem enthält sie eine fette, haarige Spinne. Es ist dunkel, so dass man den Inhalt der Schublade schlecht erkennt. Wir ziehen so lange (ohne Zurücklegen) Socken aus der Schublade bis wir entweder zwei gleichfarbige Socken zum Anziehen haben oder bis wir die Spinne anfassen und vor Schreck ohne Socken davonlaufen.

Wir nehmen an, dass bei jedem Schritt jedes der übriggebliebenen Objekte (Socke oder Spinne) mit derselben Wahrscheinlichkeit gewählt werden kann.

Noch ein Beispiel

Modellierung als Baumdiagramm:



Beispielsweise gilt: $\Pr[brb] = \frac{1}{2} \cdot \frac{2}{5} \cdot \frac{1}{2} = \frac{1}{10}$.

Noch ein Beispiel

Wir erhalten $W = (\Omega, \Pr)$ mit

$$\Omega = \{bb, brb, brr, brs, bs, rbb, rbr, rbs, rr, rs, s\}$$

und:

ω	bb	brb	brr	brs	bs	rbb	rbr	rbs	rr	rs	s
$\Pr[\omega]$	$1/5$	$1/10$	$1/20$	$1/20$	$1/10$	$1/10$	$1/20$	$1/20$	$1/15$	$1/15$	$1/6$

W ist gültig, da $\Pr[\omega] \geq 0$ für alle $\omega \in \Omega$ gilt und:

$$\sum_{\omega \in \Omega} \Pr[\omega] = \frac{1}{5} + \frac{1}{10} + \frac{1}{20} + \frac{1}{20} + \frac{1}{10} + \frac{1}{10} + \frac{1}{20} + \frac{1}{20} + \frac{1}{15} + \frac{1}{15} + \frac{1}{6} = 1. \qquad \checkmark$$

Noch ein Beispiel

Was ist nun die Wahrscheinlichkeit folgender Ereignisse?

B : „Wir ziehen blaue Socken an.“
R : „Wir ziehen rote Socken an.“
K : „Wir ziehen keine Socken an.“

Für B, R und K gilt:

$$\Pr[B] = \Pr[\{bb, brb, rbb\}] = \frac{1}{5} + \frac{1}{10} + \frac{1}{10} = \frac{2}{5} = 0.4,$$
$$\Pr[R] = \Pr[\{brr, rbr, rr\}] = \frac{1}{20} + \frac{1}{20} + \frac{1}{15} = \frac{1}{6} = 0.1\overline{6},$$
$$\Pr[K] = \Pr[\{brs, bs, rbs, rs, s\}] = \frac{1}{20} + \frac{1}{10} + \frac{1}{20} + \frac{1}{15} + \frac{1}{6} = \frac{13}{30} = 0.4\overline{3}.$$

Themenübersicht

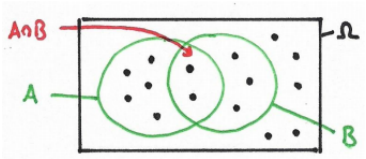
Definition bedingte Wahrscheinlichkeit

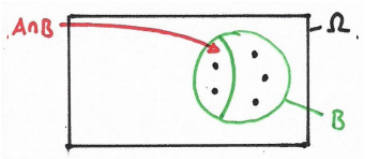
Seien $A, B \subseteq \Omega$ zwei Ereignisse mit $\Pr[B] \neq 0$, dann gilt:

$$\Pr[A|B] := \frac{\Pr[A \cap B]}{\Pr[B]}.$$

$\Pr[A|B]$ ist die Wahrscheinlichkeit von A bedingt B und stellt die Wahrscheinlichkeit für A dar, falls bekannt ist, dass B aufgetreten ist.

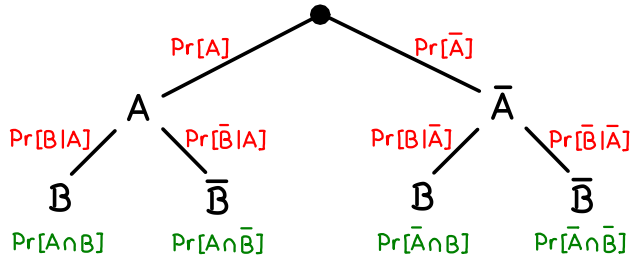
Graphisch:





Man skaliert die Wahrscheinlichkeiten aller Elementarereignissen mit dem Faktor $\frac{1}{\Pr[B]}$, damit $\Pr[B] = 1$ gilt (B ist ja aufgetreten!) und dann berechnet man die skalierte Wahrscheinlichkeit für alle Elementareignisse in A, die auch in B sind.

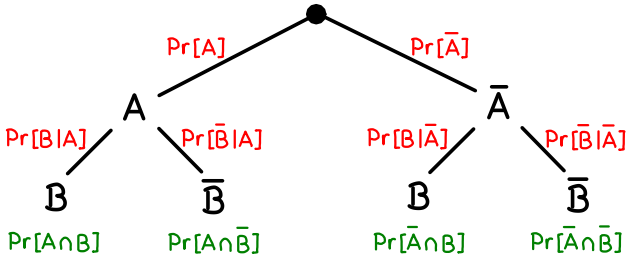
Bedingte Wahrscheinlichkeiten als Baumdiagramme



Rechenregeln für Komplementärereignisse:

$$\begin{aligned} \Pr\left[\overline{A}\right] &= 1 - \Pr[A], \\ \Pr\left[\overline{B}\middle|A\right] &= 1 - \Pr[B|A], \\ \Pr\left[\overline{B}\middle|\overline{A}\right] &= 1 - \Pr\left[B\middle|\overline{A}\right]. \end{aligned}$$

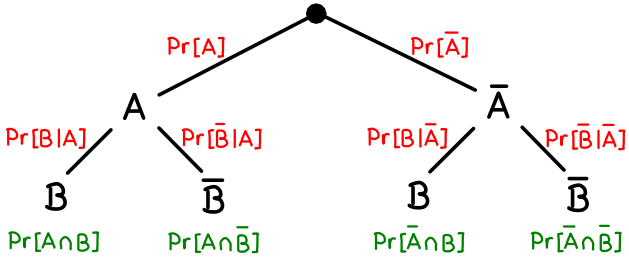
Bedingte Wahrscheinlichkeiten als Baumdiagramme



Rechenregeln für Schnittmengen:

$$
\begin{aligned}
\Pr[A \cap B] &= \Pr[A] \cdot \Pr[B|A], \\
\Pr[A \cap \overline{B}] &= \Pr[A] \cdot \Pr[\overline{B}|A], \\
\Pr[\overline{A} \cap B] &= \Pr[\overline{A}] \cdot \Pr[B|\overline{A}], \\
\Pr[\overline{A} \cap \overline{B}] &= \Pr[\overline{A}] \cdot \Pr[\overline{B}|\overline{A}].
\end{aligned}
$$

Bedingte Wahrscheinlichkeiten als Baumdiagramme

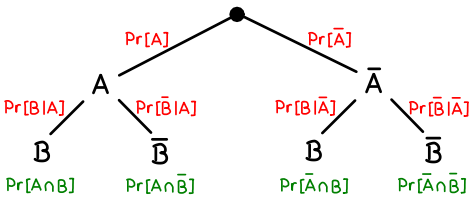


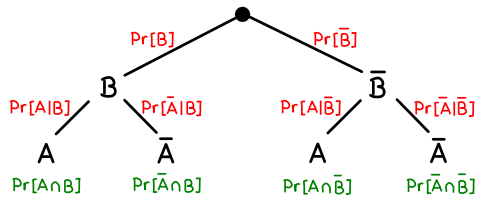
Rechenregeln für Vereinigungsmengen:

$$
\begin{array}{lcllcl}
\Pr[A \cup B] & = & \Pr[A \cap B] + \Pr[A \cap \overline{B}] + \Pr[\overline{A} \cap B] & = & 1 - \Pr[\overline{A} \cap \overline{B}], \\
\Pr[A \cup \overline{B}] & = & \Pr[A \cap B] + \Pr[A \cap \overline{B}] + \Pr[\overline{A} \cap \overline{B}] & = & 1 - \Pr[\overline{A} \cap B], \\
\Pr[\overline{A} \cup B] & = & \Pr[A \cap B] + \Pr[\overline{A} \cap B] + \Pr[\overline{A} \cap \overline{B}] & = & 1 - \Pr[A \cap \overline{B}], \\
\Pr[\overline{A} \cup \overline{B}] & = & \Pr[A \cap \overline{B}] + \Pr[\overline{A} \cap B] + \Pr[\overline{A} \cap \overline{B}] & = & 1 - \Pr[A \cap B].
\end{array}
$$

Achtung!

Im Gegensatz zu den normalen Baumdiagrammen, modellieren diese Bäume keine mehrstufigen Experimente in denen die kausale Reihenfolge der Ereignisse eine wichtige Rolle spielen. Die Reihenfolge der Ereignisse A und B ist also egal und die Modellierung ist nicht eindeutig.



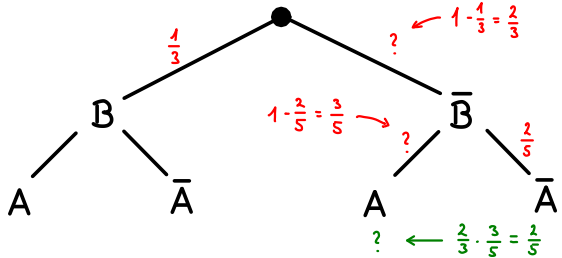


Die Wahrscheinlichkeiten $\Pr[A|B]$ und $\Pr[B|A]$ existieren beide immer, zumindest solange die jeweilige Bedingung positive Wahrscheinlichkeit hat, und beide Baumdiagramme sind zulässig. Die Kausalität der Ereignisse ist egal.

Quizfrage

Seien $A, B \subseteq \Omega$ zwei Ereignisse mit $\Pr[B] = \frac{1}{3}$ und $\Pr\left[\overline{A} \middle| \overline{B}\right] = \frac{2}{5}$. Was ist $\Pr\left[A \cap \overline{B}\right]$?

Als Baumdiagramm:



Es folgt: $\Pr\left[A \cap \overline{B}\right] = \frac{2}{3} \cdot \frac{3}{5} = \frac{2}{5}$.

Formal:

$$\Pr\left[A \cap \overline{B}\right] = \Pr\left[A \middle| \overline{B}\right] \cdot \Pr\left[\overline{B}\right] = \left(1 - \Pr\left[\overline{A} \middle| \overline{B}\right]\right) \cdot (1 - \Pr[B]) = \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{2}{5}\right) = \frac{2}{3} \cdot \frac{3}{5} = \frac{2}{5}$$

Seien A und B zwei Ereignisse mit $\Pr[A], \Pr[B] > 0$. Wann gilt $\Pr[A|B] = \Pr[B|A]$?

Gib eine möglichst einfache notwendige und hinreichende Bedingung an.

Erinnerung:

- F ist eine notwendige Bedingung für G, falls $F \impliedby G$.
- F ist eine hinreichende Bedingung für G, falls $F \implies G$.
- F ist eine notwendige und hinreichende Bedingung für G, falls $F \iff G$.

Es gilt:

$$\Pr[A|B] = \Pr[B|A] \iff \frac{\Pr[A \cap B]}{\Pr[B]} = \frac{\Pr[A \cap B]}{\Pr[A]} \iff \Pr[A \cap B] = 0 \vee \Pr[A] = \Pr[B].$$

Es muss also $\Pr[A \cap B] = 0$ oder $\Pr[A] = \Pr[B]$ (oder beides) erfüllt sein.

Multiplikationssatz

Seien $A_1, \ldots, A_n$ Ereignisse mit $\Pr[A_1 \cap \ldots \cap A_n] \neq 0$. Dann gilt

$$\Pr\left[\bigcap_{i=1}^{n} A_i\right] = \prod_{i=1}^{n} \Pr\left[A_i \middle| \bigcap_{j=1}^{i-1} A_j\right],$$

wobei $\Pr\left[A_1 \middle| \bigcap_{j=1}^{0} A_j\right] = \Pr[A_1|\Omega] = \Pr[A_1]$.

Beispiele:

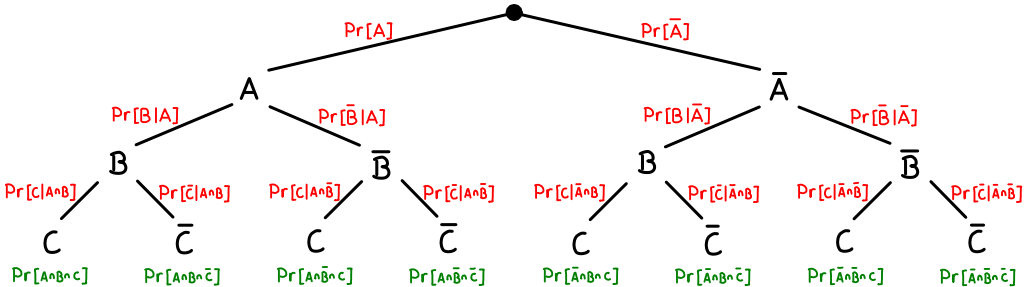
- Falls $n = 2$:
$$\Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2|A_1].$$
- Falls $n = 3$:
$$\Pr[A_1 \cap A_2 \cap A_3] = \Pr[A_1] \cdot \Pr[A_2|A_1] \cdot \Pr[A_3|A_1 \cap A_2].$$
- Falls $n = 4$:
$$\Pr[A_1 \cap A_2 \cap A_3 \cap A_4] = \Pr[A_1] \cdot \Pr[A_2|A_1] \cdot \Pr[A_3|A_1 \cap A_2] \cdot \Pr[A_4|A_1 \cap A_2 \cap A_3].$$

Der Multiplikationssatz als Baumdiagramm

Auch den Multiplikationssatz kann man sehr schön mit Baumdiagrammen graphisch darstellen. In diesem Fall darf der Baum beliebig hoch sein. Für die Reihenfolge der Ereignissen gibt es keine Einschränkung.

Beispiel

Seien $W = (\Omega, \Pr)$ ein Wahrscheinlichkeitsraum und $A, B, C \subseteq \Omega$ Ereignisse. Eine mögliche Modellierung als Baumdiagramm ist folgende:



Dann gilt beispielsweise:

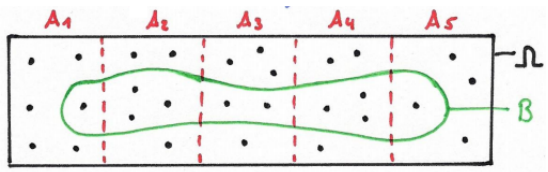
$$\Pr\left[\overline{A} \cap B \cap \overline{C}\right] = \Pr\left[\overline{A}\right] \cdot \Pr\left[B \middle| \overline{A}\right] \cdot \Pr\left[\overline{C} \middle| \overline{A} \cap B\right]$$

Satz der totalen Wahrscheinlichkeit

Seien B ein Ereignis und P eine Partition von Ω mit $\Pr[A] > 0$ für alle $A \in P$. Dann gilt:

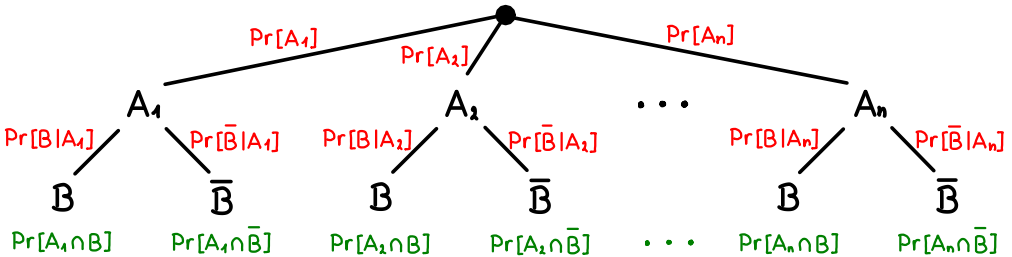
$$\Pr[B] = \sum_{A \in P} \Pr[B \cap A] = \sum_{A \in P} \Pr[A] \cdot \Pr[B|A].$$

Graphische Darstellung für eine 5-Partition $P = \{A_1, \ldots, A_5\}$ von Ω:



Satz der totalen Wahrscheinlichkeit

Als Baumdiagramm:



Um $\Pr[B]$ (bzw. $\Pr[\overline{B}]$) zu bestimmen, berechnet man die Wahrscheinlichkeiten aller Pfade die nach B (bzw. $\overline{B}$) führen und addiert sie zusammen:

$$\begin{aligned}\Pr[B] &= \Pr[A_1]\cdot\Pr[B|A_1] + \Pr[A_2]\cdot\Pr[B|A_2] + \ldots + \Pr[A_n]\cdot\Pr[B|A_n],\\ \Pr[\overline{B}] &= \Pr[A_1]\cdot\Pr[\overline{B}|A_1] + \Pr[A_2]\cdot\Pr[\overline{B}|A_2] + \ldots + \Pr[A_n]\cdot\Pr[\overline{B}|A_n].\end{aligned}$$

Infos

- Erinnerung: Eine Partition $P = \{A_1, \ldots, A_n\}$ von Ω ist eine Menge von paarweise disjunkten Ereignissen $A_1, \ldots, A_n \subseteq \Omega$ mit $\Omega = A_1 \cup \ldots \cup A_n$.
- Eine Partition kann auch unendlich groß sein.
- Der Satz der totalen Wahrscheinlichkeit verkörpert die Fallunterscheidung in der Wahrscheinlichkeitsrechnung.
- Die einfachste (und üblichste) Partition P von Ω ist $P = \left\{A, \overline{A}\right\}$ für ein beliebiges Ereignis A. Daraus folgt die wohl einfachste Version von diesem Satz:

$$\Pr[B] = \Pr[B|A] \cdot \Pr[A] + \Pr\left[B\middle|\overline{A}\right] \cdot \Pr\left[\overline{A}\right].$$

Beispiel

Eine Urne enthält 3 blaue, 2 rote und eine gelbe Kugel. Wir ziehen eine von den 6 Kugeln zufällig und legen 3 von derselben Farbe wieder zurück. Danach ziehen wir von den nun 8 Kugeln eine zweite.

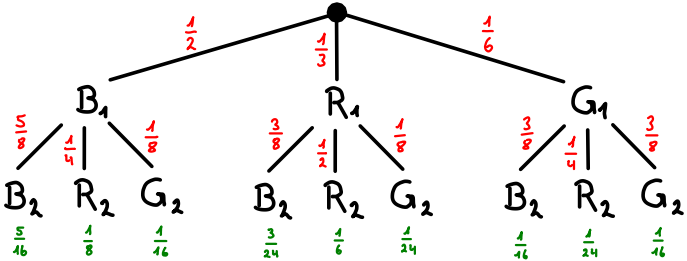
Wir definieren für $i \in \{1, 2\}$ folgende Ereignisse:

B_i : In der i-ten Ziehung wurde eine blaue Kugel gezogen,
R_i : In der i-ten Ziehung wurde eine rote Kugel gezogen,
G_i : In der i-ten Ziehung wurde eine gelbe Kugel gezogen.

Was ist die Wahrscheinlichkeit, dass wir in der zweiten Ziehung eine rote Kugel ziehen, also $\Pr[R_2]$?

Beispiel

Als Baumdiagramm:



$$\begin{aligned}\Pr[R_2] &= \Pr[B_1]\cdot\Pr[R_2|B_1] + \Pr[R_1]\cdot\Pr[R_2|R_1] + \Pr[G_1]\cdot\Pr[R_2|G_1] \\ &= \frac{1}{2}\cdot\frac{1}{4} + \frac{1}{3}\cdot\frac{1}{2} + \frac{1}{6}\cdot\frac{1}{4} \\ &= \frac{1}{3}\end{aligned}$$

Satz von Bayes

Seien A und B zwei Ereignisse mit $\Pr[A], \Pr[B] \neq 0$. Dann gilt:

$$\Pr[A|B] = \frac{\Pr[B|A] \cdot \Pr[A]}{\Pr[B]}.$$

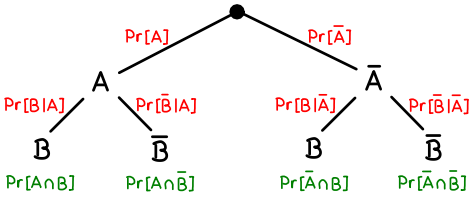
Der Satz von Bayes benutzt zweimal die Definition von bedingten Wahrscheinlichkeiten, um $\Pr[A|B]$ und $\Pr[B|A]$ in Beziehung zu setzen:

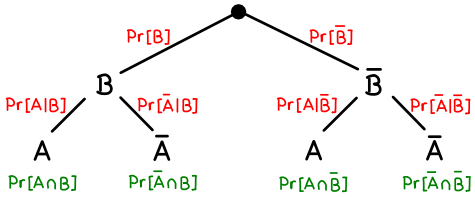
$$\Pr[B|A] \cdot \Pr[A] = \Pr[A \cap B] = \Pr[A|B] \cdot \Pr[B].$$

Oft wendet man den Satz der totalen Wahrscheinlichkeit auf $\Pr[B]$ an.

Satz von Bayes

Mit Baumdiagrammen:





Rechenregeln:

$$
\begin{aligned}
\Pr[A]\cdot\Pr[B|A] &= \Pr[A\cap B] &&= \Pr[B]\cdot\Pr[A|B],\\
\Pr[A]\cdot\Pr[\overline{B}|A] &= \Pr[A\cap \overline{B}] &&= \Pr[\overline{B}]\cdot\Pr[A|\overline{B}],\\
\Pr[\overline{A}]\cdot\Pr[B|\overline{A}] &= \Pr[\overline{A}\cap B] &&= \Pr[B]\cdot\Pr[\overline{A}|B],\\
\Pr[\overline{A}]\cdot\Pr[\overline{B}|\overline{A}] &= \Pr[\overline{A}\cap \overline{B}] &&= \Pr[\overline{B}]\cdot\Pr[\overline{A}|\overline{B}].
\end{aligned}
$$

Infos

- Man benutzt den Satz von Bayes immer wenn eine bedingte Wahrscheinlichkeit $\Pr[A|B]$ einfach zu bestimmen oder gegeben ist, aber nach der bedingten Wahrscheinlichkeit $\Pr[B|A]$ gefragt wird.
- Stellt man beide Baumdiagramme auf, so kann man die Wahrscheinlichkeit von jedem Pfad des einen Baumes mit der von genau einem Pfad des anderen Baumes gleichsetzen.

Beispiel (nochmal)

Nochmal das Beispiel aus Folie 1779:

Eine Urne enthält 3 blaue, 2 rote und eine gelbe Kugel. Wir ziehen eine von den 6 Kugeln zufällig und legen 3 von derselben Farbe wieder zurück. Danach ziehen wir von den nun 8 Kugeln eine zweite Kugel.

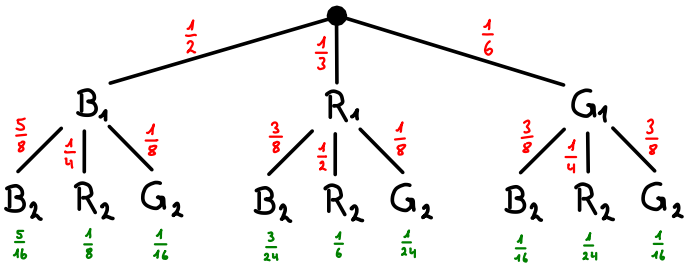
Wir definieren für $i \in \{1, 2\}$ folgende Ereignisse:

B_i : In der i-ten Ziehung wurde eine blaue Kugel gezogen,
R_i : In der i-ten Ziehung wurde eine rote Kugel gezogen,
G_i : In der i-ten Ziehung wurde eine gelbe Kugel gezogen.

Angenommen in der zweiten Ziehung wird eine rote Kugel gezogen. Was ist die Wahrscheinlichkeit dafür, dass in der ersten Ziehung eine gelbe Kugel gezogen wurde, also $\Pr[G_1|R_2]$?

Beispiel (nochmal)

Mit derselben Modellierung wie davor und dem Satz von Bayes erhalten wir:



Für $\Pr[G_1|R_2]$ gilt dann:

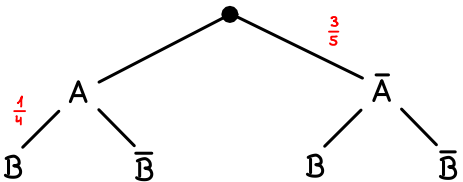
$$\Pr[G_1|R_2] = \frac{\Pr[R_2|G_1] \cdot \Pr[G_1]}{\Pr[R_2]} = \frac{\frac{1}{4} \cdot \frac{1}{6}}{\frac{1}{3}} = \frac{1}{8}.$$

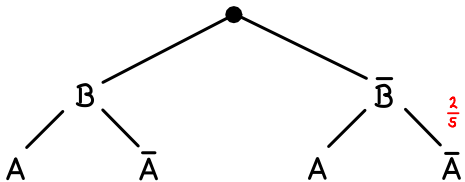
Erinnerung: Auf dem Beispiel aus Folie 1779 haben wir $\Pr[R_2] = \frac{1}{3}$ berechnet.

Ausführliches Beispiel

Gegeben sei ein Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ mit Ereignissen $A, B \subseteq \Omega$ und

$$\Pr[\overline{A}] = \frac{3}{5}, \qquad \Pr[B|A] = \frac{1}{4}, \qquad \Pr[\overline{A}|\overline{B}] = \frac{2}{5}.$$

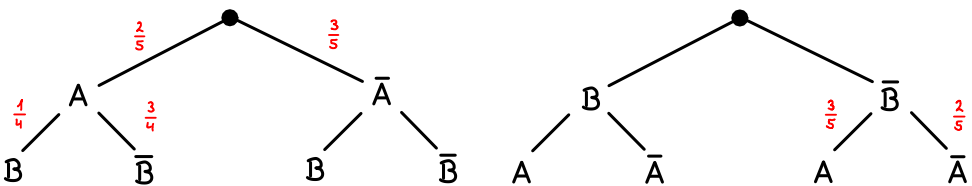




Ausführliches Beispiel

Für die Komplementärereignisse gilt:

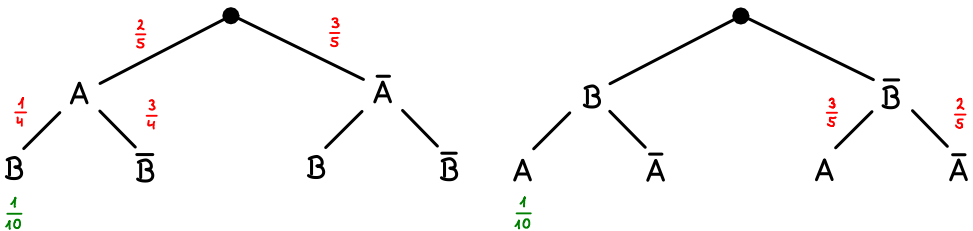
$$\Pr[A] = 1 - \frac{3}{5} = \frac{2}{5}, \qquad \Pr\left[\overline{B}\middle|A\right] = 1 - \frac{1}{4} = \frac{3}{4}, \qquad \Pr\left[A\middle|\overline{B}\right] = 1 - \frac{2}{5} = \frac{3}{5}.$$



Ausführliches Beispiel

Aus der Definition für bedingte Wahrscheinlichkeiten folgt:

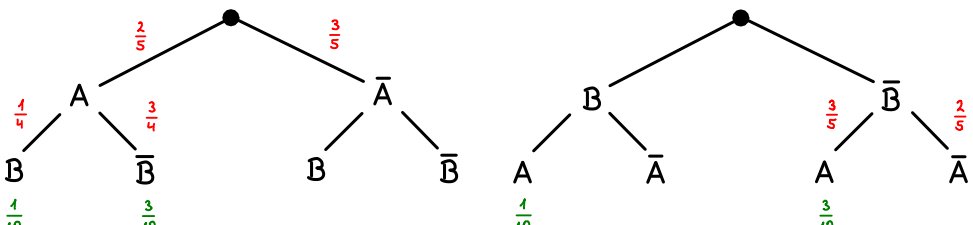
$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B|A] = \frac{2}{5} \cdot \frac{1}{4} = \frac{1}{10}.$$



Ausführliches Beispiel

Aus der Definition für bedingte Wahrscheinlichkeiten folgt:

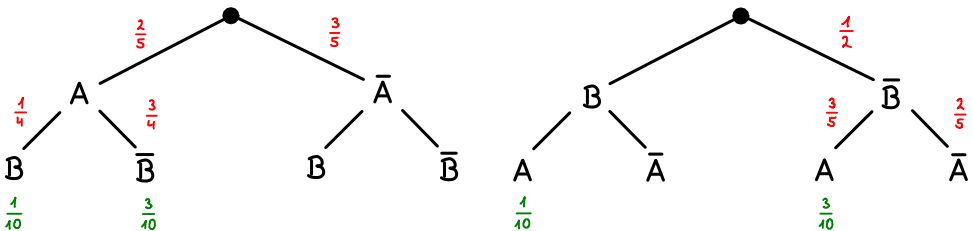
$$\Pr\left[A \cap \overline{B}\right] = \Pr[A] \cdot \Pr\left[\overline{B} \middle| A\right] = \frac{2}{5} \cdot \frac{3}{4} = \frac{3}{10}.$$



Ausführliches Beispiel

Aus der Definition für bedingte Wahrscheinlichkeiten folgt:

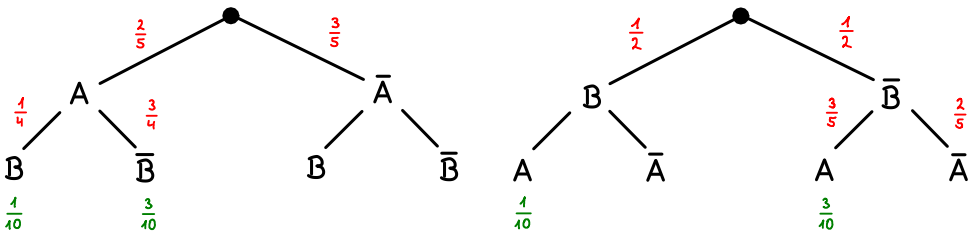
$$\Pr[A \cap \overline{B}] = \Pr[\overline{B}] \cdot \Pr[A|\overline{B}] \iff \frac{3}{10} = \Pr[\overline{B}] \cdot \frac{3}{5} \iff \Pr[\overline{B}] = \frac{1}{2}.$$



Ausführliches Beispiel

Für das Komplementärereignis folgt:

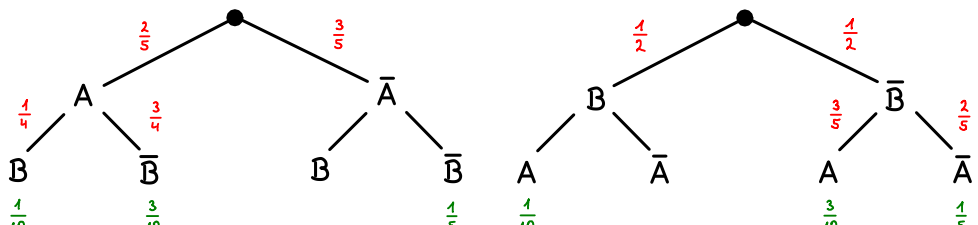
$$\Pr[B] = 1 - \Pr\left[\overline{B}\right] = 1 - \frac{1}{2} = \frac{1}{2}.$$



Ausführliches Beispiel

Aus der Definition für bedingte Wahrscheinlichkeiten folgt:

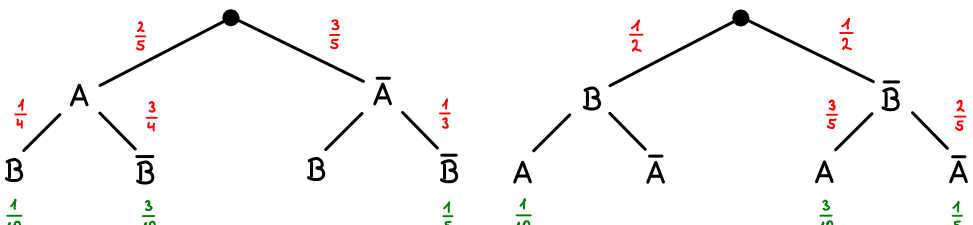
$$\Pr\left[\overline{A} \cap \overline{B}\right] = \Pr\left[\overline{B}\right] \cdot \Pr\left[\overline{A} \middle| \overline{B}\right] = \frac{1}{2} \cdot \frac{2}{5} = \frac{1}{5}.$$



Ausführliches Beispiel

Aus der Definition für bedingte Wahrscheinlichkeiten folgt:

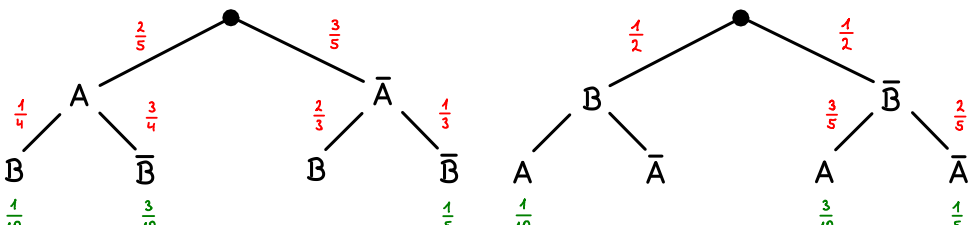
$$\Pr[\overline{A} \cap \overline{B}] = \Pr[\overline{A}] \cdot \Pr[\overline{B}|\overline{A}] \iff \frac{1}{5} = \frac{3}{5} \cdot \Pr[\overline{B}|\overline{A}] \iff \Pr[\overline{B}|\overline{A}] = \frac{1}{3}.$$



Ausführliches Beispiel

Für das Komplementärereignis folgt:

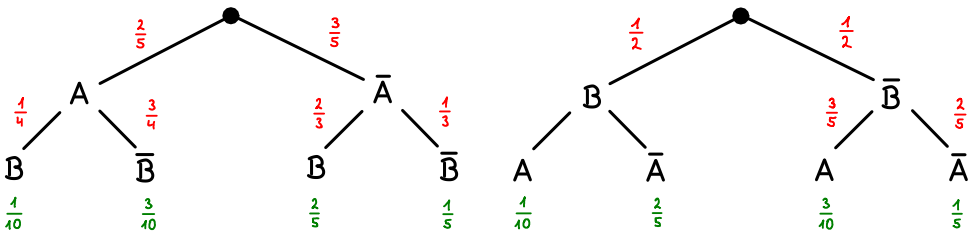
$$\Pr\left[B \middle| \overline{A}\right] = 1 - \Pr\left[\overline{B} \middle| \overline{A}\right] = 1 - \frac{1}{3} = \frac{2}{3}.$$



Ausführliches Beispiel

Aus der Definition für bedingte Wahrscheinlichkeiten folgt:

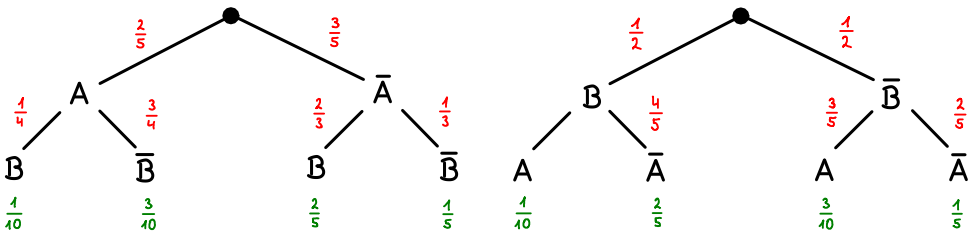
$$\Pr\left[\overline{A} \cap B\right] = \Pr\left[\overline{A}\right] \cdot \Pr\left[B \middle| \overline{A}\right] = \frac{3}{5} \cdot \frac{2}{3} = \frac{2}{5}.$$



Ausführliches Beispiel

Aus der Definition für bedingte Wahrscheinlichkeiten folgt:

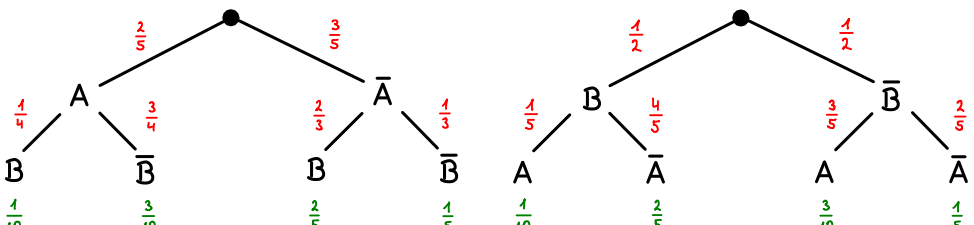
$$\Pr\left[\overline{A} \cap B\right] = \Pr[B] \cdot \Pr\left[\overline{A} \middle| B\right] \iff \frac{2}{5} = \frac{1}{2} \cdot \Pr\left[\overline{A} \middle| B\right] \iff \Pr\left[\overline{A} \middle| B\right] = \frac{4}{5}.$$



Ausführliches Beispiel

Für das Komplementärereignis folgt:

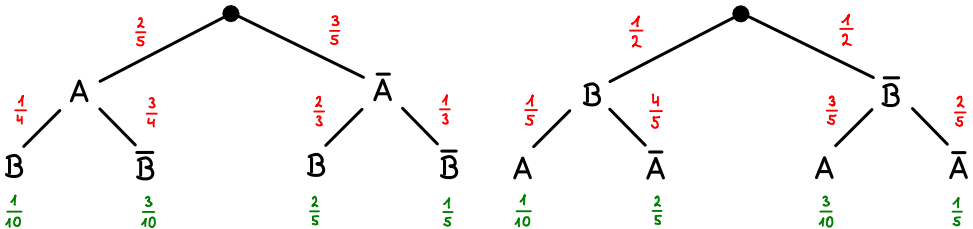
$$\Pr[A|B] = 1 - \Pr\left[\overline{A}\middle|B\right] = 1 - \frac{4}{5} = \frac{1}{5}.$$



Ausführliches Beispiel

Für beispielsweise $\Pr[A \cup B]$ addiert man alle Pfade die A oder B enthalten:

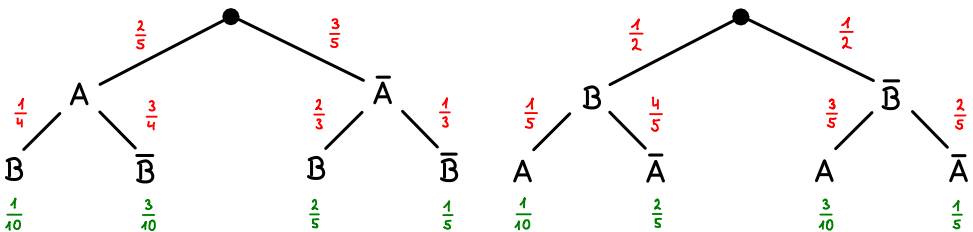
$$\Pr[A \cup B] = \frac{1}{10} + \frac{3}{10} + \frac{2}{5} = \frac{4}{5}.$$



Ausführliches Beispiel

Oder noch besser:

$$\Pr[A \cup B] = 1 - \Pr\left[\overline{A} \cap \overline{B}\right] = 1 - \frac{1}{5} = \frac{4}{5}.$$



Zusammenfassung: Rechenregeln für bedingte Wahrscheinlichkeiten

- **Bedingte Wahrscheinlichkeiten**
  Für Ereignisse A und B mit $\Pr[B] > 0$ gilt:

$$\Pr[A|B] := \frac{\Pr[A \cap B]}{\Pr[B]}.$$

- **Multiplikationssatz**
  Für Ereignisse $A_1, \ldots, A_n$ mit $\Pr[A_1 \cap \ldots \cap A_n] > 0$ gilt:

$$\Pr\left[\bigcap_{i=1}^{n} A_i\right] = \prod_{i=1}^{n} \Pr\left[A_i \middle| \bigcap_{j=1}^{i-1} A_j\right],$$

  wobei $\Pr\left[A_1 \middle| \bigcap_{j=1}^{0} A_j\right] = \Pr[A_1|\Omega] = \Pr[A_1]$.

Zusammenfassung: Rechenregeln für bedingte Wahrscheinlichkeiten

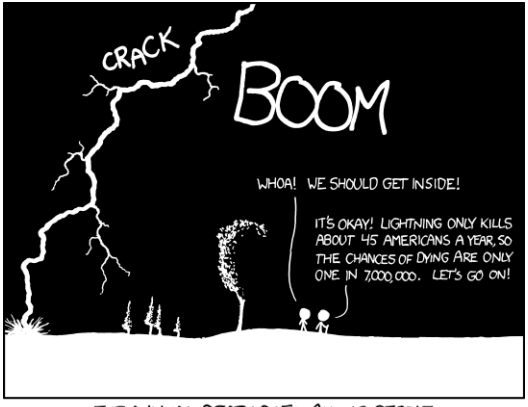
- **Satz der totalen Wahrscheinlichkeit**
  Für ein Ereignis B und eine Partition P von Ω mit $\Pr[A] > 0$ für alle $A \in P$. Dann gilt:

$$\Pr[B] = \sum_{A \in P} \Pr[A] \cdot \Pr[B|A].$$

- **Satz von Bayes**
  Für Ereignisse A und B mit $\Pr[A], \Pr[B] > 0$ gilt:

$$\Pr[A|B] = \frac{\Pr[B|A] \cdot \Pr[A]}{\Pr[B]}.$$

Conditional Risk



Quelle: `xkcd.com/795`.

Themenübersicht

Diskrete Zufallsvariablen

- Eine diskrete Zufallsvariable X ist eine Funktion

$$X : \Omega \to \mathbb{R},$$

  die jedem Elementarereignis $\omega \in \Omega$ eine reelle Zahl $X(\omega)$ zuordnet.

- Der Wertebereich W_X einer Zufallsvariable X ist

$$W_X = \{X(\omega) \,|\, \omega \in \Omega\}\,.$$

- Für jedes $k \in W_X$ bezeichnet „$X = k$“ das Ereignis

$$\{\omega \in \Omega \,|\, X(\omega) = k\}\,.$$

Beispiel

Wir betrachten wieder den Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ aus Folie 1756 mit

$$\Omega = \{KKK, KKZ, KZK, KZZ, ZKK, ZKZ, ZZK, ZZZ\}$$

und $\Pr\omega = \frac{1}{8}$ für alle $\omega \in \Omega$ und definieren folgende Zufallsvariable:

$$X: \quad \text{Anzahl der } \textit{Kopf}\text{-Würfe.}$$

Es gilt $W_X = \{0, 1, 2, 3\}$ und

$$\begin{array}{lcll} \Pr[X=0] & = & \Pr[\{ZZZ\}] & = & 1/8, \\ \Pr[X=1] & = & \Pr[\{KZZ, ZKZ, ZZK\}] & = & 3/8, \\ \Pr[X=2] & = & \Pr[\{KKZ, KZK, ZKK\}] & = & 3/8, \\ \Pr[X=3] & = & \Pr[\{KKK\}] & = & 1/8. \end{array}$$

Beispielsweise gilt für das Ereignis „X ist gerade“:

$$\Pr[X \text{ ist gerade}] = \Pr[X=0] + \Pr[X=2] = \frac{1}{8} + \frac{3}{8} = \frac{1}{2}.$$

Infos

- Mit Zufallsvariablen können wir irrelevante Informationen über $(\Omega, \Pr)$ ausblenden und mit Zahlen statt mit Tupeln, Wörtern o.ä. arbeiten.
- Wir schreiben einfach „X : Anzahl der *Kopf*-Würfe“ statt „$X : \Omega \to \mathbb{R},\ X(\omega) = |\omega|_K$“ und „$X$ gerade“ statt „$\{\omega \in \Omega \mid X(\omega) \text{ gerade}\}$“.
- Ereignisse der Form $X = k$ bilden eine Partition von Ω. Sie sind nämlich disjunkt und es gilt immer:

$$\Omega = \bigcup_{k \in W_X} (X = k).$$

Im letzten Beispiel entstand folgende Partition P von Ω:

$$P = \{\underbrace{\{ZZZ\}}_{X=0}, \underbrace{\{ZZK, ZKZ, KZZ\}}_{X=1}, \underbrace{\{ZKK, KZK, KKZ\}}_{X=2}, \underbrace{\{KKK\}}_{X=3}\}.$$

Diese Ereignisse lassen sich z.B. wunderbar mit dem Satz der totalen Wahrscheinlichkeit kombinieren:

$$\Pr[B] = \sum_{k \in W_X} \Pr[B|X = k] \cdot \Pr[X = k]$$

Dichte- und Verteilungsfunktion

Sei X eine diskrete Zufallsvariable.

- Die Dichtefunktion $f_X : \mathbb{R} \to [0, 1]$ von X ist für alle $x \in \mathbb{R}$ definiert als:

$$f_X(x) := \Pr[X = x].$$

- Die Verteilungsfunktion $F_X : \mathbb{R} \to [0, 1]$ von X ist für alle $x \in \mathbb{R}$ definiert als:

$$F_X(x) := \Pr[X \leq x].$$

- $f_{X|Y=y}(x) = xy$, $f_X(x|Y = y) = xy$

Beispiel

Wir modellieren das Würfeln mit einem weißen und einem schwarzen fairen Würfel als Laplaceschen Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ mit

$$\Omega = \{\boxdot, \boxdot, \boxdot, \boxdot, \boxdot, \boxdot\} \times \{\blacksquare, \blacksquare, \blacksquare, \blacksquare, \blacksquare, \blacksquare\}$$

und $\Pr[\omega] = \frac{1}{36}$ für alle $\omega \in \Omega$.

Mögliche Zufallsvariaben wären:

X : Minimum der Augenzahlen beider Würfel,
Y : Maximum der Augenzahlen beider Würfel,
Z : Summe der Augenzahlen beider Würfel.

Dann gilt beispielsweise: $X(\boxdot, \blacksquare) = 2$, $Y(\boxdot, \blacksquare) = 3$ und $Z(\boxdot, \blacksquare) = 10$.

Beispiel

Für X erhalten wir:

X	⚀	⚁	⚂	⚃	⚄	⚅
⚀	1	1	1	1	1	1
⚁	1	2	2	2	2	2
⚂	1	2	3	3	3	3
⚃	1	2	3	4	4	4
⚄	1	2	3	4	5	5
⚅	1	6	3	4	5	6

Daraus folgt $W_X = \{1, \ldots, 6\}$ und:

x	1	2	3	4	5	6
$f_X(x)$	11/36	1/4	7/36	5/36	1/12	1/36
$F_X(x)$	11/36	5/9	25/36	8/9	35/36	1

Beispiel

Für Y erhalten wir:

Y	⚀	⚁	⚂	⚃	⚄	⚅
⚀	1	2	3	4	5	6
⚁	2	2	3	4	5	6
⚂	3	3	3	4	5	6
⚃	4	4	4	4	5	6
⚄	5	5	5	5	5	6
⚅	6	6	6	6	6	6

Daraus folgt $W_Y = \{1, \ldots, 6\}$ und:

y	1	2	3	4	5	6
$f_Y(y)$	1/36	1/12	5/36	7/36	1/4	11/36
$F_Y(y)$	1/36	1/9	1/4	4/9	25/36	1

Beispiel

Für Z erhalten wir:

Z	⚀	⚁	⚂	⚃	⚄	⚅
⚀	2	3	4	5	6	7
⚁	3	4	5	6	7	8
⚂	4	5	6	7	8	9
⚃	5	6	7	8	9	10
⚄	6	7	8	9	10	11
⚅	7	8	9	10	11	12

Daraus folgt $W_Z = \{2, \ldots, 12\}$ und:

z	2	3	4	5	6	7	8	9	10	11	12
$f_Z(z)$	1/36	1/18	1/12	1/9	5/36	1/6	5/36	1/9	1/12	1/18	1/36
$F_Z(z)$	1/36	1/12	1/6	5/18	5/12	7/12	13/18	5/6	11/12	35/36	1

Infos

- Zufallsvariablen können auch aus anderen Zufallsvariablen zusammengesetzt sein. Für jede Funktion $f : \mathbb{R}^n \to \mathbb{R}$ und Zufallsvariablen $X_1, \ldots, X_n$ kann auch $f(X_1, \ldots, X_n)$ als eine Funktion von Ω nach $\mathbb{R}$, also auch als Zufallsvariable aufgefasst werden.
- Beispielsweise sind für Zufallsvariablen X, Y, Z auch

$$e^X, \sqrt{X^2 + Y^2}, \min\{X, Y\} \text{ und } \frac{X - Y}{Z}$$

  Zufallsvariablen.
- Im letzten Beispiel war Z eine aus X und Y zusammengesetzte Zufallsvariable. Es galt:

$$Z = X + Y.$$

Dichte und Verteilung bedingter Zufallsvariablen

Seien X eine diskrete Zufallsvariable und B ein Ereignis.

- Die bedingte Dichtefunktion $f_{X|B} : \mathbb{R} \to [0,1]$ von $X|B$ ist definiert als:

$$f_{X|B}(k) := \Pr[X = k|B] = \frac{\Pr[X = k \cap B]}{\Pr[B]}.$$

- Die bedingte Verteilungsfunktion $F_{X|B} : \mathbb{R} \to [0,1]$ von $X|B$ ist definiert als:

$$F_{X|B}(k) := \Pr[X \leq k|B] = \frac{\Pr[X \leq k \cap B]}{\Pr[B]}.$$

Man nennt $X|B$ eine bedingte Zufallsvariable.

Infos

- Die Wahrscheinlichkeitsverteilung von X wird eindeutig durch f_X oder durch F_X bestimmt. Es gilt nämlich:

$$F_X(k) = \sum_{i \leq k} f_X(i) \quad \text{und} \quad f_X(k) = F_X(k) - \sup\{F_X(i) \mid i < k\}$$

  D.h. man kann aus der einen Funktion die andere gewinnen.

- Am besten kann man sich das vorstellen, wenn $W_X \subseteq \mathbb{N}_0$ gilt. Dann erhält man:

$$F_X(k) = \sum_{i=0}^{k} f_X(i) \quad \text{und} \quad f_X(k) = F_X(k) - F_X(k-1)$$

- Wenn zwei Zufallsvariablen X und Y identisch verteilt sind, dann heißt das, dass sie genau dieselbe Dichte- bzw. Verteilungsfunktionen haben, also $f_X = f_Y$ und $F_X = F_Y$. Das heißt aber nicht, dass sie immer gleiche Werte liefern, also dass $X = Y$ gilt! Beispielsweise sind X und Y aus Folie 1809 unterschiedliche, jedoch identisch verteilte Zufallsvariablen.

Erwartungswert und Varianz

Sei X eine Zufallsvariable.

- Der Erwartungswert $\mathbb{E}[X]$ einer Zufallsvariable X ist der Wert den X im Mittel annimmt. Es gilt:
$$\mathbb{E}[X] := \sum_{k \in W_X} k \cdot f_X(k).$$
- Die Varianz $\mathrm{Var}[X]$ einer Zufallsvariable X ist ein Maß für die Abweichung von X von ihrem Erwartungswert. Es gilt:
$$\mathrm{Var}[X] := \mathbb{E}\big[(X - \mathbb{E}[X])^2\big] = \sum_{k \in W_X} (k - \mathbb{E}[X])^2 \cdot f_X(k).$$
Nimmt eine Zufallsvariable z.B. nur einen Wert mit Wahrscheinlichkeit 1 an, so ist ihre Varianz gleich Null.

Infos

- Identisch verteilte Zufallsvariablen X und Y haben auch dieselben Erwartungswerte und Varianzen, d.h.:

$$f_X(k) = f_Y(k), \quad F_X(k) = F_Y(k), \quad \mathbb{E}[X] = \mathbb{E}[Y], \quad \mathrm{Var}[X] = \mathrm{Var}[Y].$$

  Aber (nochmal): X, Y *identisch verteilt* heißt nicht $X = Y$!

- Für jede Funktion $g : \mathbb{R} \to \mathbb{R}$ gilt:

$$\mathbb{E}[g(X)] = \sum_{k \in W_X} g(k) \cdot f_X(k).$$

  Beispielsweise gilt: $\mathbb{E}\left[\sqrt{X}\right] = \sum_{k \in W_X} \sqrt{k} \cdot f_X(k)$ oder $\mathbb{E}\left[e^X\right] = \sum_{k \in W_X} e^k \cdot f_X(k)$.

- Verschiebungssatz: Für die Varianz $\mathrm{Var}[X]$ von X gilt:

$$\mathrm{Var}[X] = \mathbb{E}\left[X^2\right] - \mathbb{E}[X]^2.$$

  Hier bestimmt man $\mathbb{E}\left[X^2\right]$ mithilfe der obigen Formel: $\mathbb{E}\left[X^2\right] = \sum_{k \in W_X} k^2 \cdot f_X(k)$.

Beispiel

Wir betrachten die Zufallsvariable X aus Folie 1805 mit $W_X = \{0, 1, 2, 3\}$ und folgender Dichte:

k	0	1	2	3
$f_X(k)$	1/8	3/8	3/8	1/8

Aus den Definitionen für $\mathbb{E}[X]$ und $\mathrm{Var}[X]$ erhalten wir:

$$\mathbb{E}[X] = 0 \cdot \frac{1}{8} + 1 \cdot \frac{3}{8} + 2 \cdot \frac{3}{8} + 3 \cdot \frac{1}{8} = \frac{3}{2},$$

$$\mathrm{Var}[X] = \left(0 - \frac{3}{2}\right)^2 \cdot \frac{1}{8} + \left(1 - \frac{3}{2}\right)^2 \cdot \frac{3}{8} + \left(2 - \frac{3}{2}\right)^2 \cdot \frac{3}{8} + \left(3 - \frac{3}{2}\right)^2 \cdot \frac{1}{8} = \frac{3}{4}.$$

Die Berechnung der Varianz ist mit der Definition meistens sehr umständlich. Daher werden wir meistens den Verschiebungssatz verwenden.

Im vorherigen Beispiel erhalten wir mit dem Verschiebungssatz:

$$\mathrm{Var}[X] = \mathbb{E}\left[X^2\right] - \mathbb{E}[X]^2 = 0^2 \cdot \frac{1}{8} + 1^2 \cdot \frac{3}{8} + 2^2 \cdot \frac{3}{8} + 3^2 \cdot \frac{1}{8} - \left(\frac{3}{2}\right)^2 = \frac{3}{4}.$$

Gemeinsame Dichte

- Die gemeinsame Dichte zweier Zufallsvariablen X und Y ist definiert als:

$$f_{X,Y}(x,y) := \Pr[X = x, Y = y].$$

- f_X und f_Y kann man aus $f_{X,Y}(x,y)$ mit folgenden Formeln gewinnen:

$$f_X(x) = \sum_{y \in W_Y} f_{X,Y}(x,y), \qquad f_Y(y) = \sum_{x \in W_X} f_{X,Y}(x,y).$$

  Man nennt f_X und f_Y auch Randdichten.

- Folgende Schreibweisen sind äquivalent:

$$\Pr[X = x, Y = y], \qquad \Pr[X = x \cap Y = y], \qquad \Pr[X = x \wedge Y = y].$$

- Für n Zufallsvariablen $X_1, \ldots, X_n$ definiert man die gemeinsame Dichte $f_{X_1,\ldots,X_n}$ analog:

$$f_{X_1,\ldots,X_n}(x_1, \ldots, x_n) := \Pr[X_1 = x_1, \ldots, X_n = x_n].$$

Die Randdichten f_X und f_Y sind genau die einzelnen Dichten der Zufallsvariablen X und Y. Es gilt nämlich:

$$
\begin{aligned}
f_X(x) &= \sum_{y \in W_Y} f_{X,Y}(x,y) && \text{(Definition)} \\
&= \sum_{y \in W_Y} \Pr[X = x, Y = y] && \text{(Definition)} \\
&= \sum_{y \in W_Y} \Pr[X = x | Y = y] \cdot \Pr[Y = y] && \text{(bedingte Wahrscheinlichkeit)} \\
&= \Pr[X = x] && \text{(Satz der totalen Wahrscheinlichkeit)}
\end{aligned}
$$

Analog für f_Y.

Beispiel

Wir betrachten einen weißen und einen schwarzen Würfel. Der weiße Würfel hat eine ⚀-Seite, zwei ⚁-Seiten und drei ⚂-Seiten. Der schwarze Würfel hat eine ⚃-Seite, zwei ⚄-Seiten und drei ⚅-Seiten.

Wir modellieren das gleichzeitige Würfeln mit ihnen als Wahrscheinlichkeitsraum $(\Omega, \Pr)$ mit

$$\Omega = \{⚀, ⚁, ⚂\} \times \{⚃, ⚄, ⚅\}$$

und

ω	(⚀,⚃)	(⚀,⚄)	(⚀,⚅)	(⚁,⚃)	(⚁,⚄)	(⚁,⚅)	(⚂,⚃)	(⚂,⚄)	(⚂,⚅)
$\Pr\omega$	1/12	1/18	1/36	1/6	1/9	1/18	1/4	1/6	1/12

Dazu betrachten wir die Zufallsvariablen:

X : Augenzahl des weißen Würfels,
Y : Augenzahl des schwarzen Würfels.

Beispiel

Aus

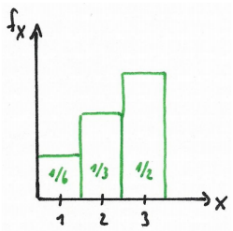
ω	(⚀,⚀)	(⚀,⚁)	(⚀,⚂)	(⚀,⚃)	(⚀,⚄)	(⚀,⚅)	(⚁,⚃)	(⚁,⚄)	(⚁,⚅)
$\Pr\omega$	1/12	1/18	1/36	1/6	1/9	1/18	1/4	1/6	1/12

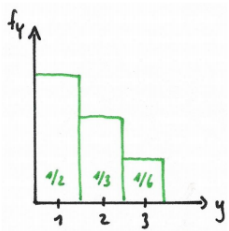
erhalten wir für X und Y folgende Dichten:

k	1	2	3
$f_X(k)$	1/6	1/3	1/2

k	1	2	3
$f_Y(k)$	1/2	1/3	1/6

Graphisch:



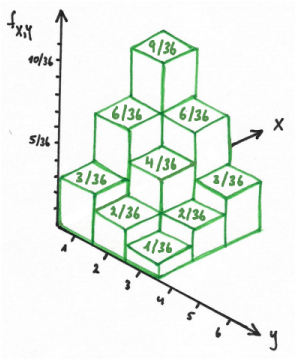


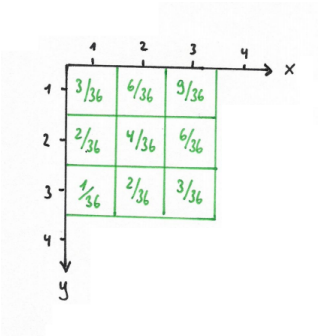
Beispiel

Die gemeinsame Dichte $f_{X,Y}(x, y)$ folgt ebenfalls aus

ω	(⚀, ⚅)	(⚁, ⚅)	(⚁, ⚆)	(⚂, ⚅)	(⚂, ⚆)	(⚂, ⚇)	(⚃, ⚅)	(⚃, ⚆)	(⚃, ⚆)
$\Pr\omega$	1/12	1/18	1/36	1/6	1/9	1/18	1/4	1/6	1/12

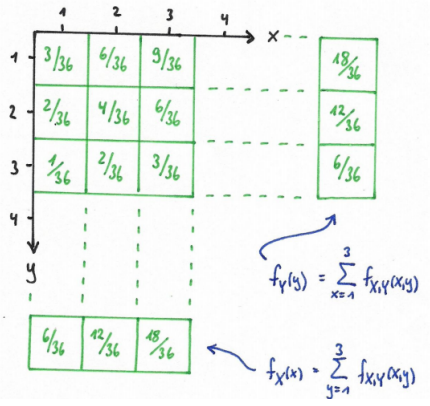
Graphisch:





Beispiel

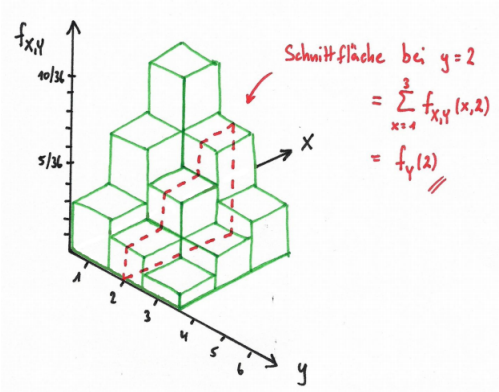
Daraus lassen sich die Randdichten f_X und f_Y bestimmen:



Wir erhalten dieselben Dichten wie vorher.

Beispiel

Graphische Bedeutung von z.B. $f_Y(2)$:



Wir betrachten wieder den Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ aus Folie 1757 mit

$$\Omega = \{bb, brb, brr, brs, bs, rbb, rbr, rbs, rr, rs, s\}$$

(siehe zwei Folien weiter im Beispiel) und

ω	bb	brb	brr	brs	bs	rbb	rbr	rbs	rr	rs	s
$\Pr\omega$	$1/5$	$1/10$	$1/20$	$1/20$	$1/10$	$1/10$	$1/20$	$1/20$	$1/15$	$1/15$	$1/6$

Dazu definieren wir folgende Zufallsvariablen:

X : Anzahl der b's in ω, also $|\omega|_b$,
Y : Anzahl der r's in ω, also $|\omega|_r$.

Was sind W_X, W_Y, f_X, f_Y und $f_{X,Y}$? (als Tabelle)

- Für X gilt $W_X = \{0, 1, 2\}$ und

x	0	1	2
$f_X(x)$	3/10	3/10	2/5

- Für Y gilt $W_Y = \{0, 1, 2\}$ und

y	0	1	2
$f_Y(y)$	7/15	11/30	1/6

- Für die gemeinsame Dichte $f_{X,Y}$ gilt:

$f_{X,Y}(x,y)$	$x = 0$	$x = 1$	$x = 2$
$y = 0$	1/6	1/10	1/5
$y = 1$	1/15	1/10	1/5
$y = 2$	1/15	1/10	0

Gemeinsame Verteilungsfunktion

Die gemeinsame Verteilungsfunktion zweier Zufallsvariablen X und Y definiert man analog:

$$F_{X,Y}(x, y) := \Pr[X \leq x, Y \leq y].$$

Gemeinsame Verteilungs- und Dichtefunktion

Für die gemeinsame Verteilungsfunktion gilt auch:

$$F_{X,Y}(x,y) = \sum_{k \leq x} \sum_{l \leq y} f_{X,Y}(k,l).$$

Themenübersicht

Unabhängigkeit zweier Ereignisse

Zwei Ereignisse sollen genau dann unabhängig sein, wenn sie sich gegenseitig „nicht beeinflussen“, d.h. wenn die Wahrscheinlichkeit des einen Ereignisses unverändert bleibet, wenn das andere Ereignis als bedingung vorkommt. Dies passiert wenn

$$\Pr[A|B] = \Pr[A] \quad \text{oder} \quad \Pr[B|A] = \Pr[B].$$

Wegen $\Pr[B] > 0$ und $\Pr[A] > 0$

$$\Pr[A|B] = \Pr[A] \iff \Pr[A \cap B] = \Pr[A] \cdot \Pr[B] \iff \Pr[B|A] = \Pr[B]$$

definieren wir Unabhängigkeit wie folgt.

Zwei beliebige Ereignisse $A, B \subseteq \Omega$ heißen unabhängig, falls gilt:

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B].$$

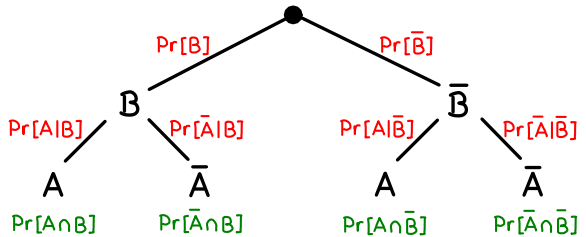
Dabei sind $\Pr[A] = 0$ oder $\Pr[B] = 0$ erlaubt.

Unabhängigkeit und Baumdiagramme

Die Unabhängigkeit zweier Ereignisse kann man auch sehr schön an einem Baumdiagramm erkennen. Damit A und B unabhängig sind muss nämlich gelten:

$$\begin{aligned}\Pr[A|B] = \Pr[A] &\Leftrightarrow \Pr[A|B] = \Pr[A|B] \cdot \Pr[B] + \Pr\left[A\middle|\overline{B}\right] \cdot \Pr\left[\overline{B}\right] \\ &\Leftrightarrow (1 - \Pr[B]) \cdot \Pr[A|B] = \Pr\left[A\middle|\overline{B}\right] \cdot \Pr\left[\overline{B}\right] \\ &\Leftrightarrow \Pr[A|B] = \Pr\left[A\middle|\overline{B}\right]\end{aligned}$$

D.h. die zwei Teilbäume an B und $\overline{B}$ müssen dieselben Wahrscheinlichkeiten haben!



Quizfrage

Sind disjunkte Ereignisse immer unabhängig?

Erinnerung: A und B sind disjunkt, falls $A \cap B = \emptyset$ gilt.

NEIN!!

Man kann sich sehr einfach durch folgende Intuition in die Irre führen lassen:

$$A, B \text{ disjunkt} \Rightarrow A \text{ hat nichts mit } B \text{ zu tun} \Rightarrow A, B \text{ unabhängig}$$

Das ist ein böser Fehler, denn in den seltensten Fällen ist es so!

Falls A und B disjunkt sind, dann gilt $\Pr[A \cap B] = \Pr[\emptyset] = 0$. D.h. die Gleichung $\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$ wird nur für $\Pr[A] = 0$ oder $\Pr[B] = 0$ erfüllt und sonst nicht.

Unabhängigkeit mehrerer Ereignisse (Definition)

Eine Menge $\{A_1, \ldots, A_n\}$ von Ereignissen ist genau dann unabhängig, wenn für jede Teilmenge $S \subseteq \{A_1, \ldots, A_n\}$ gilt:

$$\Pr\left[\bigcap_{i \in S} A_i\right] = \prod_{i \in S} \Pr[A_i].$$

Wichtig:

$$\Pr[A_{i_1} \cap \ldots \cap A_{i_k}] = \Pr[A_{i_1}] \cdot \ldots \cdot \Pr[A_{i_k}].$$

Beispiel

Die Ereignismenge $\{A, B, C\}$ ist genau dann unabhängig, wenn gilt:

$$\begin{aligned}
\Pr[A] &= \Pr[A], \\
\Pr[B] &= \Pr[B], \\
\Pr[C] &= \Pr[C], \\
\Pr[A \cap B] &= \Pr[A] \cdot \Pr[B], \\
\Pr[A \cap C] &= \Pr[A] \cdot \Pr[C], \\
\Pr[B \cap C] &= \Pr[B] \cdot \Pr[C], \\
\Pr[A \cap B \cap C] &= \Pr[A] \cdot \Pr[B] \cdot \Pr[C].
\end{aligned}$$

Unabhängigkeit mehrerer Ereignisse (Lemma)

Eine Menge $\{A_1, A_2, \ldots, A_n\}$ von Ereignissen ist genau dann unabhängig, wenn für alle $(s_1, \ldots, s_n) \in \{0,1\}^n$ gilt:

$$\Pr[A_1^{s_1} \cap \ldots \cap A_n^{s_n}] = \Pr[A_1^{s_1}] \cdot \ldots \cdot \Pr[A_n^{s_n}]$$

Dabei gilt $A_k^0 := \overline{A_k}$ und $A_k^1 := A_k$.

Beispiel

Die Ereignismenge $\{A, B, C\}$ ist genau dann unabhängig, wenn gilt:

$$
\begin{aligned}
\Pr\left[A^0 \cap B^0 \cap C^0\right] &= \Pr\left[A^0\right] \cdot \Pr\left[B^0\right] \cdot \Pr\left[C^0\right], \\
\Pr\left[A^0 \cap B^0 \cap C^1\right] &= \Pr\left[A^0\right] \cdot \Pr\left[B^0\right] \cdot \Pr\left[C^1\right], \\
\Pr\left[A^0 \cap B^1 \cap C^0\right] &= \Pr\left[A^0\right] \cdot \Pr\left[B^1\right] \cdot \Pr\left[C^0\right], \\
\Pr\left[A^0 \cap B^1 \cap C^1\right] &= \Pr\left[A^0\right] \cdot \Pr\left[B^1\right] \cdot \Pr\left[C^1\right], \\
\Pr\left[A^1 \cap B^0 \cap C^0\right] &= \Pr\left[A^1\right] \cdot \Pr\left[B^0\right] \cdot \Pr\left[C^0\right], \\
\Pr\left[A^1 \cap B^0 \cap C^1\right] &= \Pr\left[A^1\right] \cdot \Pr\left[B^0\right] \cdot \Pr\left[C^1\right], \\
\Pr\left[A^1 \cap B^1 \cap C^0\right] &= \Pr\left[A^1\right] \cdot \Pr\left[B^1\right] \cdot \Pr\left[C^0\right], \\
\Pr\left[A^1 \cap B^1 \cap C^1\right] &= \Pr\left[A^1\right] \cdot \Pr\left[B^1\right] \cdot \Pr\left[C^1\right].
\end{aligned}
$$

Beispiel

Die Ereignismenge $\{A, B, C\}$ ist genau dann unabhängig, wenn gilt:

$$
\begin{aligned}
\Pr\left[\overline{A} \cap \overline{B} \cap \overline{C}\right] &= \Pr\left[\overline{A}\right] \cdot \Pr\left[\overline{B}\right] \cdot \Pr\left[\overline{C}\right], \\
\Pr\left[\overline{A} \cap \overline{B} \cap C\right] &= \Pr\left[\overline{A}\right] \cdot \Pr\left[\overline{B}\right] \cdot \Pr[C], \\
\Pr\left[\overline{A} \cap B \cap \overline{C}\right] &= \Pr\left[\overline{A}\right] \cdot \Pr[B] \cdot \Pr\left[\overline{C}\right], \\
\Pr\left[\overline{A} \cap B \cap C\right] &= \Pr\left[\overline{A}\right] \cdot \Pr[B] \cdot \Pr[C], \\
\Pr\left[A \cap \overline{B} \cap \overline{C}\right] &= \Pr[A] \cdot \Pr\left[\overline{B}\right] \cdot \Pr\left[\overline{C}\right], \\
\Pr\left[A \cap \overline{B} \cap C\right] &= \Pr[A] \cdot \Pr\left[\overline{B}\right] \cdot \Pr[C], \\
\Pr\left[A \cap B \cap \overline{C}\right] &= \Pr[A] \cdot \Pr[B] \cdot \Pr\left[\overline{C}\right], \\
\Pr[A \cap B \cap C] &= \Pr[A] \cdot \Pr[B] \cdot \Pr[C].
\end{aligned}
$$

Unabhängigkeit bei Komplement, Schnitt und Vereinigung

Sei $\{A_1, \ldots, A_n\}$ eine unabhängige Menge von Ereignissen. Dann sind

$$\left\{\overline{A_1}, A_2, \ldots, A_n\right\}, \quad \{A_1 \cap A_2, A_3, \ldots, A_n\} \quad \textit{und} \quad \{A_1 \cup A_2, A_3, \ldots, A_n\}$$

auch unabhängig.

Verfahren zur Konstruktion unabhängiger Ereignisse

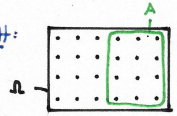
Das ist eine graphische Version zur Lösung von VA 1.2 auf Blatt 2.

Verfahren zur Konstruktion unabhängiger Ereignisse

Gegeben: W'keitsraum $\langle \Omega, Pr \rangle$ mit $|\Omega| = 24$ und $Pr[\omega] = \frac{1}{24}$ $(\forall \omega \in \Omega)$

Gesucht: unabhängige Ereignisse A, B und C mit $Pr[A] = \frac{1}{2}$, $Pr[B] = \frac{1}{3}$ und $Pr[C] = \frac{1}{4}$

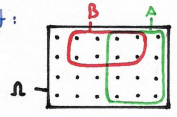
1. Schritt:



Wähle $\frac{1}{2}$ der Elementarereignisse für A.

$\rightsquigarrow$ Ω wird in 2 Mengen partitioniert: A und $\overline{A}$.

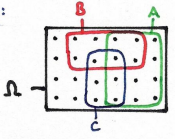
2. Schritt:



Wähle $\frac{1}{3}$ der Elementarereignisse von A und $\frac{1}{3}$ von $\overline{A}$ für B.

$\rightsquigarrow$ Ω wird in 4 partitioniert: $A \cap B$, $A \cap \overline{B}$, $\overline{A} \cap B$, $\overline{A} \cap \overline{B}$.

3. Schritt:



Wähle $\frac{1}{4}$ der Elementarereignisse von jedem der 4 Teile für C.

$\rightsquigarrow$ Ω wird in 8 Mengen partitioniert.

Unabhängigkeit von Zufallsvariablen

Die Zufallsvariablen $X_1, \ldots, X_n$ sind genau dann unabhängig, wenn

$$f_{X_1,\ldots,X_n}(x_1, \ldots, x_n) = f_{X_1}(x_1) \cdot \ldots \cdot f_{X_n}(x_n)$$

oder äquivalent dazu

$$F_{X_1,\ldots,X_n}(x_1, \ldots, x_n) = F_{X_1}(x_1) \cdot \ldots \cdot F_{X_n}(x_n)$$

für alle $(x_1, \ldots, x_n) \in W_{X_1} \times \ldots \times W_{X_n}$ gelten.

Gibt es also eine Kombination für die Werte von $x_1, \ldots, x_n$, so dass die Gleichungen oben nicht gelten, dann sind die Zufallsvariablen nicht unabhängig.

Beispiel

Für das Beispiel mit den zwei gezinkten Würfeln (Folie 1823) hatten wir für die Zufallsvariablen X und Y folgende Dichten für $x, y \in [3]$:

$$f_X(x) = \frac{x}{6}, \qquad f_Y(y) = \frac{4-y}{6}, \qquad f_{X,Y}(x,y) = \frac{x(4-y)}{36}.$$

X und Y sind unabhängig, da für alle $x, y \in [3]$ gilt:

$$f_X(x) \cdot f_Y(y) = \frac{x}{6} \cdot \frac{4-y}{6} = \frac{x(4-y)}{36} = f_{X,Y}(x,y)$$

Noch ein Beispiel

Für das Beispiel mit der Schubladen und den Socken (Folie 1757) hatten wir die Zufallsvariablen X (Anzahl der b's in ω) und Y (Anzahl der r's in ω) definiert. Für f_X, f_Y und $f_{X,Y}$ gilt:

x	0	1	2
$f_X(x)$	3/10	3/10	2/5

y	0	1	2
$f_Y(y)$	7/15	11/30	1/6

und

$f_{X,Y}(x,y)$	$x=0$	$x=1$	$x=2$
$y=0$	1/6	1/10	1/5
$y=1$	1/15	1/10	1/5
$y=2$	1/15	1/10	0

X und Y sind nicht unabhängig, da z.B. für $x=2, y=2$ gilt:

$$f_X(2) \cdot f_Y(2) = \frac{2}{5} \cdot \frac{1}{6} = \frac{1}{15} \neq 0 = f_{X,Y}(2,2)$$

Achtung!

falls X und Y unabhängig sind, dann gilt z.B. auch

$$\Pr[X = x \cap Y = n - x] = \Pr[X = x] \cdot \Pr[Y = n - x]$$

Intuitiv möchte man meinen, dass die Ereignisse $X = x$ und $Y = n - x$ nicht unabhängig sind, da beide ein x enthalten. Wenn aber X und Y unabhängig sind, dann gilt

$$\Pr[X = x \cap Y = y] = \Pr[X = x] \cdot \Pr[Y = y]$$

für alle $(x, y) \in W_X \times W_Y$, also auch für $(x, y) = (x, n - x)$.

Wichtige Rechenregel

Man kann unabhängige Zufallsvariablen $X_1, \ldots, X_n$ beliebig zu neuen Zufallsvariablen $Y_1, \ldots, Y_m$ „ kombinieren“. Falls keine Zufallsvariable X_i in zwei verschiedenen Zufallsvariablen Y_j, Y_k vorkommt, dann sind die Zufallsvariablen $Y_1, \ldots, Y_m$ auch unabhängig.

Beispiele

Seien X_1, X_2, X_3, X_4, X_5 unabhängige Zufallsvariablen. Folgende Zufallsvariablen sind ebenfalls unabhängig:

- $X_1^{X_2}$, $\sqrt{\frac{X_3}{X_4}}$ und X_5
- $\frac{X_1+X_2+X_3}{X_3^2}$, e^{X_4} und $(X_5-3)^{X_5}$
- $X_1+X_2+X_3+X_4$ und X_5

Nicht notwendigerweise unabhängig sind dagegen:

- $5(X_1+X_2)$, $\frac{1}{X_2+X_3}$ und $\log_{X_4} X_5$
- $\frac{X_1+X_2}{2}$, $\sqrt{\frac{X_3X_4}{2\pi}}$ und $X_1^{X_3^{X_5}}$
- X_1+X_2, X_2+X_3, X_3+X_4 und X_4+X_5

Indikatorvariablen

Sei A ein beliebiges Ereignis. Die Indikatorvariable I_A zu A ist wie folgt definiert:

$$I_A(\omega) := \begin{cases} 1 & \text{falls } \omega \in A \\ 0 & \text{falls } \omega \notin A \end{cases}.$$

„$I_A = 1$“ entspricht genau dem Ereignis A und „$I_A = 0$“ genau $\overline{A}$.

Beziehung zwischen Ereignissen und Zufallsvariablen

Eine Ereignismenge $\{A_1, A_2, \ldots, A_n\}$ ist genau dann unabhängig, wenn die entsprechenden Indikatorvariablen $I_{A_1}, I_{A_2}, \ldots, I_{A_n}$ unabhängig sind.

Rechenregeln

Hier sind einige coole Rechenregeln für eine Zufallsvariable Z, die aus zwei unabhängigen Zufallsvariablen X und Y zusammengesetzt ist.

- Für $Z = X + Y$:

$$f_Z(x) = \sum_{k \in W_x} \Pr[X = k \cap Y = x - k] = \sum_{k \in W_x} f_X(k) \cdot f_Y(x - k)$$

- Für $Z = X - Y$ (analog):

$$f_Z(x) = \sum_{k \in W_x} f_X(k) \cdot f_Y(k - x)$$

Daraus folgt z.B.:

$$\Pr[X = Y] = \Pr[X - Y = 0] = f_{X-Y}(0) = \sum_{k \in W_x} f_X(k) \cdot f_Y(k)$$

Rechenregeln

- Für $Z = \min(X, Y)$:

$$\begin{aligned} F_Z(k) &= \Pr[\min(X, Y) \leq k] \\ &= 1 - \Pr[\min(X, Y) > k] \\ &= 1 - \Pr[X > k \cap Y > k] \\ &= 1 - \Pr[X > k] \cdot \Pr[Y > k] \\ &= 1 - (1 - \Pr[X \leq k]) \cdot (1 - \Pr[Y \leq k]) \\ &= 1 - (1 - F_X(k)) \cdot (1 - F_Y(k)) \end{aligned}$$

- Für $Z = \max(X, Y)$:

$$\begin{aligned} F_Z(k) &= \Pr[\max(X, Y) \leq k] \\ &= \Pr[X \leq k \cap Y \leq k] \\ &= \Pr[X \leq k] \cdot \Pr[Y \leq k] \\ &= F_X(k) \cdot F_Y(k) \end{aligned}$$

min- und max-Trick

Seien $X_1, \ldots, X_n$ unabhängige Zufallsvariablen.

- Für $Z = \min\{X_1, \ldots, X_n\}$ gilt:

$$F_Z(k) = 1 - (1 - F_{X_1}(k)) \cdot \ldots \cdot (1 - F_{X_n}(k)).$$

- Für $Z = \max\{X_1, \ldots, X_n\}$ gilt:

$$F_Z(k) = F_{X_1}(k) \cdot \ldots \cdot F_{X_n}(k).$$

Die Herleitung verläuft analog zur vorherigen Folie.

Sei X eine Zufallsvariable, für die $F_X = F_{-X}$ gilt. Dann gilt für $Z = |X|$ und $k \in \mathbb{R}$:

$$F_Z(k) = F_{|X|}(k) = F_{\max\{X,-X\}}(k) = F_X(k) \cdot F_{-X}(k) = (F_X(k))^2.$$

Der Trick $|X| = \max\{X, -X\}$ ist schon richtig. Dumm ist nur, dass X und $-X$ alles andere als unabhängig sind ;-)

Im Allgemeinen gilt also:

$$F_Z(k) = F_{|X|}(k) = F_{\max\{X,-X\}}(k) \neq F_X(k) \cdot F_{-X}(k)$$

Themenübersicht

Zusammenfassung: Rechenregeln für den Erwartungswert

- **Erwartungswert (Definition)**
  Sei X eine diskrete Zufallsvariable. Dann gilt:

$$\mathbb{E}[X] := \sum_{k \in W_X} k \cdot f_X(k).$$

- **Monotonie des Erwartungswerts**
  Seien X und Y Zufallsvariablen mit $X(\omega) \leq Y(\omega)$ für alle $\omega \in \Omega$. Dann gilt $\mathbb{E}[X] \leq \mathbb{E}[Y]$.
- **Erwartungswert transformierter Zufallsvariablen**
  Sei X eine diskrete Zufallsvariable und $g : \mathbb{R} \to \mathbb{R}$ eine Funktion. Dann gilt:

$$\mathbb{E}[g(X)] = \sum_{k \in W_X} g(k) \cdot f_X(k).$$

Zusammenfassung: Rechenregeln für den Erwartungswert

- **Linearität des Erwartungswerts (einfache Version)**
  Sei X eine Zufallsvariable und $a, b \in \mathbb{R}$. Dann gilt:

$$\mathbb{E}[aX + b] = a\mathbb{E}[X] + b.$$

- **Erwartungswert von Zufallsvariablen mit natürlichem Wertebereich**
  Sei X eine diskrete Zufallsvariable mit $W_X \subseteq \mathbb{N}_0$. Dann gilt:

$$\mathbb{E}[X] = \sum_{k=1}^{\infty} \Pr[X \geq k].$$

- **Bedingter Erwartungswert**
  Sei X eine diskrete Zufallsvariable und $A \subseteq \Omega$ ein Ereignis mit $\Pr[A] > 0$. Dann gilt:

$$\mathbb{E}[X|A] = \sum_{k \in W_X} k \cdot f_{X|A}(k)$$

  mit $f_{X|A}(k) := \Pr[X = k|A]$.

Zusammenfassung: Rechenregeln für den Erwartungswert

- **Satz des totalen Erwartungswerts**
  Seien X eine Zufallsvariable und P eine Partition von Ω mit $\Pr[A] > 0$ für alle $A \in P$. Dann gilt:
  $$\mathbb{E}[X] = \sum_{A \in P} \mathbb{E}[X|A] \cdot \Pr[A].$$

- **Linearität des Erwartungswerts**
  Seien $X_1, \ldots, X_n$ Zufallsvariablen und $a_1, \ldots, a_n \in \mathbb{R}$. Dann gilt:
  $$\mathbb{E}[a_1 X_1 + \ldots + a_n X_n] = a_1 \mathbb{E}[X_1] + \ldots + a_n \mathbb{E}[X_n].$$

- **Multiplikativität des Erwartungswerts**
  Seien $X_1, \ldots, X_n$ unabhängige Zufallsvariablen. Dann gilt:
  $$\mathbb{E}[X_1 \cdot \ldots \cdot X_n] = \mathbb{E}[X_1] \cdot \ldots \cdot \mathbb{E}[X_n].$$

Zusammenfassung: Rechenregeln für die Varianz

- **Varianz (Definition)**
  Sei X eine diskrete Zufallsvariable. Dann gilt:

$$\mathrm{Var}[X] := \mathbb{E}\left[(X - \mathbb{E}[X])^2\right].$$

- **Verschiebungssatz**
  Seien X eine Zufallsvariable. Dann gilt:

$$\mathrm{Var}[X] = \mathbb{E}\left[X^2\right] - \mathbb{E}[X]^2.$$

- **Lineare Transformation der Varianz**
  Sei X eine diskrete Zufallsvariable und $a, b \in \mathbb{R}$. Dann gilt:

$$\mathrm{Var}[aX + b] = a^2 \,\mathrm{Var}[X].$$

- **Additivität der Varianz**
  Seien $X_1, \ldots, X_n$ unabhängige Zufallsvariablen. Dann gilt:

$$\mathrm{Var}[X_1 + \ldots + X_n] = \mathrm{Var}[X_1] + \ldots + \mathrm{Var}[X_n].$$

Sei X eine diskrete Zufallsvariable und $X_1, \ldots, X_n$ unabhängige Ausführungen von X. Dann gilt:

$$\mathrm{Var}[X_1 + \ldots + X_n] = \mathrm{Var}[n \cdot X] = n^2 \cdot \mathrm{Var}[X].$$

Was stimmt hier nicht?

Hinweis: Unabhängige Ausführungen einer Zufallsvariable X sind Zufallsvariablen $X_1, \ldots, X_n$, die unabhängig und identisch verteilt zu X sind.

Antwort

Der Fehler ist, dass man *identisch verteilt* mit *gleich* verwechselt hat.

- Falls $X_1, \ldots, X_n$ alle identisch verteilt sind, dann haben sie dieselben Dichtefunktionen und somit dieselben Verteilungsfunktionen, Erwartungswerte, Varianzen, usw. Man nennt deswegen $X_1, \ldots, X_n$ unabhängige Ausführungen desselben Experiments X. Beispiel: Wir würfeln n mal und addieren alle Augenzahlen zusammen.
- Falls $X_1, \ldots, X_n$ alle gleich sind, dann gilt wirklich $X_1 = \ldots = X_n$ und somit auch:

$$X_1 + \ldots + X_n = n \cdot X.$$

  Intuitiv stellen $X_1, \ldots, X_n$ n Kopien des Ausgangs eines einzigen Experiments dar. Beispiel: Wir würfeln einmal und multiplizieren das Ergebnis mit n.

Richtig wäre:

$$\mathrm{Var}[X_1 + \ldots + X_n] = \mathrm{Var}[X_1] + \ldots + \mathrm{Var}[X_n] = n \cdot \mathrm{Var}[X].$$

Mehr Quizfragen

Seien $X_1, \ldots, X_n$ Zufallsvariablen. Wann dürfen wir jede der folgenden vier Rechenregeln verwenden?

1. Additivität des Erwartungswerts:

$$\mathbb{E}[X_1 + \ldots + X_n] = \mathbb{E}[X_1] + \ldots + \mathbb{E}[X_n].$$

2. Multiplikativität des Erwartungswerts:

$$\mathbb{E}[X_1 \cdot \ldots \cdot X_n] = \mathbb{E}[X_1] \cdot \ldots \cdot \mathbb{E}[X_n].$$

3. Additivität der Varianz:

$$\mathrm{Var}[X_1 + \ldots + X_n] = \mathrm{Var}[X_1] + \ldots + \mathrm{Var}[X_n].$$

4. Multiplikativität der Varianz:

$$\mathrm{Var}[X_1 \cdot \ldots \cdot X_n] = \mathrm{Var}[X_1] \cdot \ldots \cdot \mathrm{Var}[X_n].$$

Antworten

1. Immer!
2. Nur falls $X_1, \ldots, X_n$ unabhängig sind.
3. Nur falls $X_1, \ldots, X_n$ unabhängig sind.
4. Nie! Die Regel existiert nicht.

min- und max-Trick für Erwartungswerte

Für unabhängige Zufallsvariablen $X_1, \ldots, X_n$ mit $W_{X_1}, \ldots, W_{X_n} \subseteq \mathbb{N}_0$ gilt nach dem Satz für den Erwartungswert für Zufallsvariablen mit natürlichem Wertebereich:

$$\mathbb{E}[Z] = \sum_{k=1}^{\infty} \Pr[Z \geq k] = \sum_{k=1}^{\infty} 1 - \Pr[Z < k] = \sum_{k=1}^{\infty} 1 - \Pr[Z \leq k-1] = \sum_{k=0}^{\infty} 1 - F_Z(k).$$

Mithilfe von Folie 1855 folgt:

$$\mathbb{E}[\min\{X_1, \ldots, X_n\}] = \sum_{k=0}^{\infty} (1 - F_{X_1}(k)) \cdot \ldots \cdot (1 - F_{X_n}(k))$$

$$\mathbb{E}[\max\{X_1, \ldots, X_n\}] = \sum_{k=0}^{\infty} (1 - F_{X_1}(k) \cdot \ldots \cdot F_{X_n}(k))$$

Themenübersicht

Was ist ein Markov-Diagramm?

Ein Markov-Diagramm $D = (Q, T, \delta)$ ist ein gewichteter Graph mit folgenden Eigenschaften:

- Q ist endlich.
- Jede Kante hat ein Gewicht aus $(0, 1]$.
- Für jeden Knoten gilt: Die Summe der Gewichte aller ausgehenden Kanten ist 1.

Wie kann man Pr mit Markov-Diagrammen definieren?

Für die Pfade eines Markov-Diagramms definieren wir Wahrscheinlichkeiten wie folgt:

1. Die Wahrscheinlichkeit eines Pfades $q_0 q_1 \dots q_k$ ist:

$$\Pr(q_0 q_1 \dots q_k) = \begin{cases} 1, & \text{falls } k = 0 \\ \prod_{i=0}^{k-1} \delta(q_i, q_{i+1}) & \text{sonst} \end{cases}$$

2. Falls Π eine präfix-freie Menge von Pfaden ist, dann gilt:

$$\Pr[\Pi] = \sum_{\pi \in \Pi} \Pr[\pi].$$

Info

Ein Pfad (ein Wort) u ist Präfix von w, falls $w = uv$ gilt für irgendein Pfad v. Π Präfix-frei heißt, dass kein Pfad in Π Präfix eines anderen Pfades ist.

Wie kann man Ω mit Markov-Diagrammen definieren?

Für zwei Zustände q_i und q_j enthält die Menge

$$[q_i \rightsquigarrow q_j]^{q_j=1}$$

alle Pfade von q_i nach q_j, die q_j genau einmal enthalten. Falls jeder Zustand vom Markov-Diagramm auf mindestens einem Pfad von q_i nach q_2 liegt, dann gilt nach Satz 32:

$$\Pr\left[[q_i \rightsquigarrow q_j]^{q_j=1}\right] = 1,$$

d.h. wir können z.B. $\Omega_{q_i} = [q_i \rightsquigarrow q_j]^{q_j=1}$ wählen.

Wo sind wir nach k Schritten?

Die Zufallsvariable Z_k gibt den Zustand an indem wir uns nach genau k Schritten befinden. Wir wollen die Dichte von Z_k für ein beliebiges k bestimmen.

Idee:

1. Kodiere das Markov-Diagramm als Übergangsmatrix M und die Dichte von Z_k als Vektor:

   $$\vec{z_k} = (\Pr[Z_k = q_1], \ldots, \Pr[Z_k = q_n]).$$

   Dann gilt für alle $i \geq 0$:

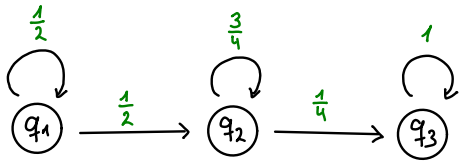
   $$\vec{z}_{i+1} = \vec{z}_i \cdot M.$$

2. Bestimme M^k.
3. Es gilt dann:

   $$\vec{z}_k = \vec{z}_0 \cdot M^k.$$

Beispiel

Gegeben sei folgendes Markov-Diagramm



mit $\Omega = [q_1 \rightsquigarrow q3]^{q_3=1}$. Was ist $\Pr[Z_k = q_i]$ für jeden Zustand q_i für ein beliebiges k?

1. Die Übergangsmatrix ist:

$$M = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{3}{4} & \frac{1}{4} \\ 0 & 0 & 1 \end{pmatrix}$$

Beispiel

2. Mit z.B. WolframAlpha lässt sich M^k bestimmen:

$$M^k = \begin{pmatrix} 2^{-k} & -2^{1-k} + 2^{1-2k}3^k & 1 + 2^{-k} - 2^{1-2k}3^k \\ 0 & \left(\frac{3}{4}\right)^k & 1 - \left(\frac{3}{4}\right)^k \\ 0 & 0 & 1 \end{pmatrix}$$

Beispiel

3. Daraus folgt für $\vec{z}_k$:

$$\vec{z}_k = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2^{-k} & -2^{1-k} + 2^{1-2k}3^k & 1 + 2^{-k} - 2^{1-2k}3^k \\ 0 & \left(\frac{3}{4}\right)^k & 1 - \left(\frac{3}{4}\right)^k \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \frac{1}{4^k} \begin{pmatrix} 2^k & 2 \cdot (3^k - 2^k) & 4^k + 2^k - 2 \cdot 3^k \end{pmatrix}$$

Es gilt also:

$$\Pr[Z_k = q_1] = \frac{2^k}{4^k}, \qquad \Pr[Z_k = q_2] = \frac{2 \cdot (3^k - 2^k)}{4^k}, \qquad \Pr[Z_k = q_3] = \frac{4^k + 2^k - 2 \cdot 3^k}{4^k}.$$

Das ist aber nicht die einzige Möglichkeit! Oft kann man die möglichen Pfade von q_i nach q_j auch einfach abzählen. Beim vorigen Markov-Diagramm hätte man auch z.B. wie folgt argumentieren können:

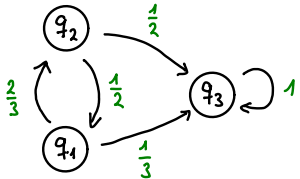
$$\Pr[X_k = q_1] = \Pr[q_1 q_1 q_1 \dots q_1] = \Pr\left[q_1^k\right] = \left(\frac{1}{2}\right)^k,$$

$$\Pr[X_k = q_2] = \Pr\left[\left\{ q_1^i q_2^{k+1-i} \right\} 0 < i \leq k \middle| =\right] \sum_{i=1}^{k} \left(\frac{1}{2}\right)^i \cdot \left(\frac{3}{4}\right)^{k-i} = \frac{2 \cdot (3^k - 2^k)}{4^k},$$

$$\Pr[X_k = q_3] = 1 - \Pr[X_k = q_1] - \Pr[X_k = q_2] = \frac{4^k + 2^k - 2 \cdot 3^k}{4^k}.$$

Beispiel

Gegeben sei folgendes Markov-Diagramm



mit $\Omega = [q_1 \rightsquigarrow q_3]^{q_3=1}$. Was ist $\Pr[Z_k = q_3]$ in Abhängigkeit von k?

Beispiel

An der Zeichnung erkennt man folgendes:

- Falls k gerade ist, so haben die Pfade von q_1 zu q_3 so aus:

$$q_1 \to q_2 \underbrace{\to q_1 \to q_2 \to q_1 \to \ldots \to q_2}_{k-2 \text{ Schritte}} \to q_3$$

- Falls k ungerade ist, so haben die Pfade von q_1 zu q_3 so aus:

$$q_1 \underbrace{\to q_2 \to q_1 \to q_2 \to \ldots \to q_1}_{k-1 \text{ Schritte}} \to q_3$$

Beispiel

Daraus folgt:

$$\Pr[Z_k = q_3] = \begin{cases} \frac{2}{3} \cdot \left(\frac{1}{2} \cdot \frac{2}{3}\right)^{\frac{k-2}{2}} \cdot \frac{1}{2} = \left(\frac{1}{3}\right)^{\frac{k}{2}}, & \text{falls } k \text{ gerade} \\ \left(\frac{2}{3} \cdot \frac{1}{2}\right)^{\frac{k-1}{2}} \cdot \frac{1}{3} = \left(\frac{2}{9}\right)^{\frac{k+1}{2}}, & \text{falls } k \text{ ungerade} \end{cases}$$

Analog kann man $\Pr[Z_k = q_1]$ und $\Pr[Z_k = q_2]$ berechnen.

Erreichen wir einen bestimmten Zustand?

Wir wollen jetzt die Wahrscheinlichkeit bestimmen, dass wir, bei q_i beginnend, irgendwann ein Zustand q_j erreichen, d.h.

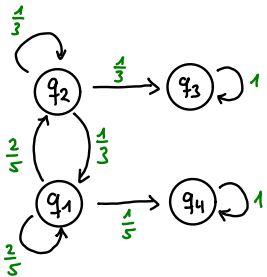
$$\Pr\left[[q_i \rightsquigarrow q_j]^{q_j=1}\right].$$

Idee:

1. Definiere Variablen $f_{k,j}$ für alle $k \in [n]$ als Abkürzung für $\Pr\left[[q_k \rightsquigarrow q_j]^{q_j=1}\right]$.
2. Benutze die Gleichung
$$f_{k,j} = \sum_{t \in kT} \delta(k,t) \cdot f_{t,j}$$
für $k \neq j$, um ein Gleichungssystem aufzustellen.
3. Löse das Gleichungssystem nach $f_{i,j}$

Beispiel

Gegeben sei folgendes Markov-Diagramm:



Was ist $\Pr\left[[q_1 \rightsquigarrow q_4]^{q_4=1}\right]$?

Beispiel

Gleichungen aufstellen:

$$
\begin{aligned}
f_{1,4} &= \frac{2}{5} f_{1,4} + \frac{2}{5} f_{2,4} + \frac{1}{5} f_{4,4} \\
f_{2,4} &= \frac{1}{3} f_{1,4} + \frac{1}{3} f_{2,4} + \frac{1}{3} f_{3,4} \\
f_{3,4} &= 0 \\
f_{4,4} &= 1
\end{aligned}
$$

Vereinfachen:

$$
\begin{aligned}
\frac{3}{5} f_{1,4} - \frac{2}{5} f_{2,4} &= \frac{1}{5} \\
\frac{1}{3} f_{1,4} - \frac{2}{3} f_{2,4} &= 0
\end{aligned}
$$

Die eindeutige Lösung lautet $f_{1,4} = \frac{1}{2}$ und $f_{2,4} = \frac{1}{4}$.

Info

Diese Methode funktioniert zwar immer, aber sie kann unübersichtlich werden. Vor allem wenn man viele Zustände hat. Analog zur Methode davor kann man oft die möglichen Pfaden von q_i nach q_j auch einfach abzählen.

Erreichen wir einen bestimmten Zustand? (2. Variante)

Wir wollen wieder $\Pr\left[[q_i \rightsquigarrow q_j]^{q_j=1}\right]$ bestimmen.

Zweite Idee:

1. Gib den Kanten irgendwelche Namen
2. Beschreibe die Menge aller Pfade von q_i nach q_j mit einem regulären Ausdruck:
   - $\alpha\beta$ ist die Konkatenation aller Pfade aus α mit allen aus β
   - $\alpha|\beta$ ist die Vereinigung aller Pfade aus α mit allen aus β. Wichtig: bei uns müssen α und β disjunkt sein! Aber das sind sie fast immer ;-)
   - α^* enthält alle Pfade die aus beliebig vielen Konkatenationen von Pfaden aus α bestehen.

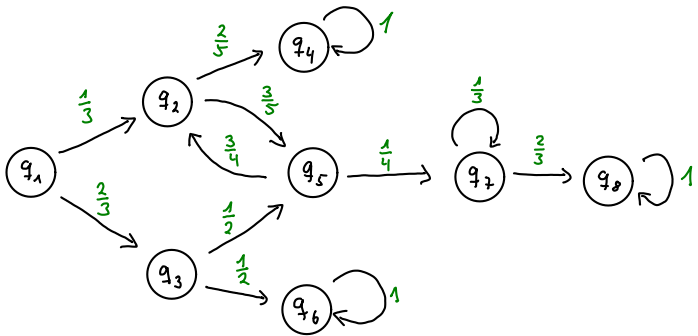
Erreichen wir einen bestimmten Zustand? (2. Variante)

3. Berechne die Wahrscheinlichkeit mit:

$$\Pr[\alpha\beta] = \Pr[\alpha] \cdot \Pr[\beta],$$
$$\Pr[\alpha|\beta] = \Pr[\alpha] + \Pr[\beta],$$
$$\Pr[\alpha^*] = \sum_{n=0}^{\infty} \Pr[\alpha]^n = \frac{1}{1 - \Pr[\alpha]}.$$

Beispiel

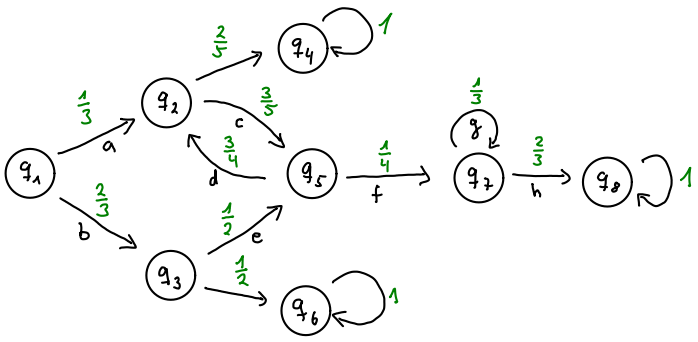
Gegeben sei folgendes Markov-Diagramm:



Was ist $\Pr\left[[q_1 \rightsquigarrow q_8]^{q_8=1}\right]$?

Beispiel

1. Kanten beschriften:



Beispiel

2. Regulärer Ausdruck:

$$\gamma = (ac|be)(dc)^* fg^* h$$

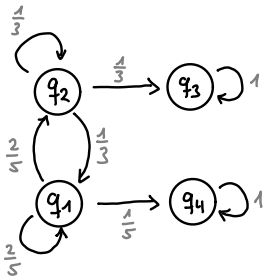
(ohne Ardens Lemma oder so, einfach scharf hinschauen! ;-))

Beispiel

3. Rechnung:

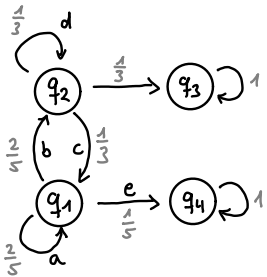
$$\begin{aligned}
\Pr\left[[q_1 \rightsquigarrow q_8]^{q_8=1}\right] &= \left(\frac{1}{3}\cdot\frac{3}{5}+\frac{2}{3}\cdot\frac{1}{2}\right)\cdot\left(\sum_{n=0}^{\infty}\left(\frac{3}{5}\cdot\frac{3}{4}\right)^n\right)\cdot\frac{1}{4}\cdot\left(\sum_{n=0}^{\infty}\left(\frac{1}{3}\right)^n\right)\cdot\frac{2}{3} \\
&= \left(\frac{5}{8}\right)\cdot\left(\sum_{n=0}^{\infty}\left(\frac{9}{20}\right)^n\right)\cdot\frac{1}{4}\cdot\left(\sum_{n=0}^{\infty}\left(\frac{1}{3}\right)^n\right)\cdot\frac{2}{3} \\
&= \left(\frac{5}{8}\right)\cdot\left(\frac{1}{1-\frac{9}{20}}\right)\cdot\frac{1}{4}\cdot\left(\frac{1}{1-\frac{1}{3}}\right)\cdot\frac{2}{3} \\
&= \frac{25}{88} \approx 0,28
\end{aligned}$$

Gegeben sei folgendes Markov-Diagramm:



Was ist $\Pr\left[[q_1 \rightsquigarrow q_4]^{q_4=1}\right]$?

1. Kanten beschriften:



2. Regulärer Ausdruck:

$$\gamma = a^*(bd^*ca^*)^*e$$

(Auch möglich: $\gamma = (a^*bd^*ca^*)^*a^*e$)

3. Rechnung:

$$
\begin{aligned}
\Pr\left[[q_1 \rightsquigarrow q_4]^{q_4=1}\right] &= \sum_{n=0}^{\infty}\left(\frac{2}{5}\right)^n \cdot \sum_{n=0}^{\infty}\left(\frac{2}{5}\cdot\sum_{m=0}^{\infty}\left(\frac{1}{3}\right)^m \cdot \frac{1}{3}\cdot\sum_{m=0}^{\infty}\left(\frac{2}{5}\right)^m\right)^n \cdot \frac{1}{5} \\
&= \frac{1}{1-\frac{2}{5}} \cdot \sum_{n=0}^{\infty}\left(\frac{2}{5}\cdot\frac{1}{1-\frac{1}{3}}\cdot\frac{1}{3}\cdot\frac{1}{1-\frac{2}{5}}\right)^n \cdot \frac{1}{5} \\
&= \frac{5}{3} \cdot \sum_{n=0}^{\infty}\left(\frac{1}{3}\right)^n \cdot \frac{1}{5} \\
&= \frac{5}{3} \cdot \frac{1}{1-\frac{1}{3}} \cdot \frac{1}{5} \\
&= \frac{1}{2}
\end{aligned}
$$

Wie viele Schritte brauchen wir im Mittel, um einen Zustand zu erreichen?

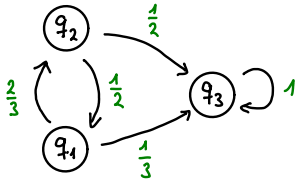
Wir haben $\Omega_{q_i} = [q_i \rightsquigarrow q_j]^{q_j=1}$. Die Zufallsvariable N zählt die Anzahl an Schritten bis man den Zustand q_j erreicht. Nun wollen wir $\mathbb{E}[N]$ wissen.

Idee:

1. Definiere Ω_{q_k} für jeden Zustand q_k. Somit ist $\mathbb{E}[N]$ die erwartete Anzahl an Schritten von q_k nach q_j.
2. Benutze die Gleichung
$$\mathbb{E}_k[N] = \sum_{t \in kT} \delta(k,t) \cdot \mathbb{E}_t[N+1]$$
für $k \neq j$, um ein Gleichungssystem aufzustellen.
3. Löse das Gleichungssystem nach $\mathbb{E}_{q_i}[N]$.

Beispiel

Gegeben sei wieder das Markov-Diagramm



mit $\Omega = [q_1 \rightsquigarrow q_3]^{q_3=1}$. Was ist $\mathbb{E}[N]$?

Beispiel

Gleichungen aufstellen:

$$\mathbb{E}_{q_1}[N] = \frac{2}{3}\mathbb{E}_{q_2}[N+1] + \frac{1}{3}\mathbb{E}_{q_3}[N+1]$$
$$\mathbb{E}_{q_2}[N] = \frac{1}{2}\mathbb{E}_{q_1}[N+1] + \frac{1}{2}\mathbb{E}_{q_3}[N+1]$$
$$\mathbb{E}_{q_3}[N] = 0$$

Mit der Linearität des Erwartungswertes folgt:

$$\mathbb{E}_{q_1}[N] = \frac{2}{3}\mathbb{E}_{q_2}[N] + \frac{2}{3} + \frac{1}{3}\mathbb{E}_{q_3}[N] + \frac{1}{3}$$
$$\mathbb{E}_{q_2}[N] = \frac{1}{2}\mathbb{E}_{q_1}[N] + \frac{1}{2} + \frac{1}{2}\mathbb{E}_{q_3}[N] + \frac{1}{2}$$
$$\mathbb{E}_{q_3}[N] = 0$$

Beispiel

Vereinfachen:

$$\mathbb{E}_{q_1}[N] - \frac{2}{3}\mathbb{E}_{q_2}[N] = 1$$
$$\mathbb{E}_{q_2}[N] - \frac{1}{2}\mathbb{E}_{q_1}[N] = 1$$

Die eindeutige Lösung lautet $\mathbb{E}_{q_1}[N] = \frac{5}{2} = 2,5$ und $\mathbb{E}_{q_2}[N] = \frac{9}{4} = 2,25$. Daraus folgt:

$$\mathbb{E}[N] = 2,5.$$

Info

Falls auch nach der Varianz Var[N] gefragt wird:

1. Bestimme $\mathbb{E}\left[N^2\right]$ analog zu $\mathbb{E}[N]$, aber mit der Formel:

$$\mathbb{E}_k\left[N^2\right] = \sum_{t \in kT} \delta(k,t) \cdot \mathbb{E}_t\left[(N+1)^2\right] = \sum_{t \in kT} \delta(k,t) \cdot \mathbb{E}_t\left[N^2 + 2N + 1\right]$$

2. Löse das Gleichungssystem und erhalte $\mathbb{E}\left[N^2\right]$.
3. Bestimme Var[N] mit

$$\mathrm{Var}[N] = \mathbb{E}\left[N^2\right] - \mathbb{E}[N]^2$$

Wahrscheinlichkeitserzeugende Funktionen in Markov-Diagrammen

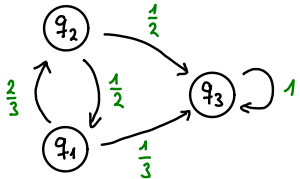
Bei Markov-Diagrammen haben wir Methoden für die Berechnung von $\mathbb{E}[N]$ und $\mathbb{E}\left[N^2\right]$ kennengelernt. ($N =$ Länge des Pfades). Man kann $G_N(z)$ analog mit der Formel

$$\mathbb{E}_k\left[z^N\right] = \sum_{t \in kT} \delta(k,t) \cdot \mathbb{E}_t\left[z^{N+1}\right] = \sum_{t \in kT} \delta(k,t) \cdot z \cdot \mathbb{E}_t\left[z^N\right]$$

bestimmen. Es gilt dann $G_N(z) = \mathbb{E}_s\left[z^N\right]$, wobei s der Startzustand ist.

Beispiel

Gegeben sei folgendes Markov-Diagramm



mit $\Omega = [q_1 \rightsquigarrow q_3]^{q_j=1}$. Was ist $G_N(z)$?

Beispiel

Es gilt:

$$\mathbb{E}_{q_1}\left[z^N\right] = \frac{2}{3} \cdot z \cdot \mathbb{E}_{q_2}\left[z^N\right] + \frac{1}{3} \cdot z \cdot \mathbb{E}_{q_3}\left[z^N\right]$$
$$\mathbb{E}_{q_2}\left[z^N\right] = \frac{1}{2} \cdot z \cdot \mathbb{E}_{q_1}\left[z^N\right] + \frac{1}{2} \cdot z \cdot \mathbb{E}_{q_3}\left[z^N\right]$$
$$\mathbb{E}_{q_3}\left[z^N\right] = z^0 = 1$$

Vereinfacht:

$$\mathbb{E}_{q_1}\left[z^N\right] = \frac{2}{3} \cdot z \cdot \mathbb{E}_{q_2}\left[z^N\right] + \frac{1}{3} \cdot z$$
$$\mathbb{E}_{q_2}\left[z^N\right] = \frac{1}{2} \cdot z \cdot \mathbb{E}_{q_1}\left[z^N\right] + \frac{1}{2} \cdot z$$

Beispiel

Durch einsetzen erhält man:

$$\mathbb{E}_{q_1}\left[z^N\right] = \frac{2}{3} \cdot z \cdot \left(\frac{1}{2} \cdot z \cdot \mathbb{E}_{q_1}\left[z^N\right] + \frac{1}{2} \cdot z\right) + \frac{1}{3} \cdot z$$

Daraus folgt:

$$G_N(z) = \mathbb{E}_{q_1}\left[z^N\right] = \frac{z^2 + z}{3 - z^2}$$

Daraus kann man z.B. die erwartete Länge bestimmen:

$$\mathbb{E}[N] = G'_N(1) = \frac{5}{2} = 2,5$$

Markov-Diagramme vs. Markov-Ketten

Bei Markov-Diagrammen hat unsere Ergebnismenge Ω_{q_i} immer dieselbe Gestalt:

$$\Omega_{q_i} = [q_i \rightsquigarrow q_j]^{q_j=1}$$

(falls jeder Zustand auf mindestens einen Pfad von q_i nach q_j liegt). D.h. wir haben immer genau einen Startzustand q_i und genau einen Endzustand q_j. Wahrscheinlichkeitsmaß ($\Pr_{q_1}[\ldots]$), Erwartungswerte ($\mathbb{E}_{q_i}[[]\ldots]$), Varianzen ($\mathrm{Var}_{q_i}[\ldots]$) und wahrscheinlichkeitserzeugende Funktionen ($G_{q_i}(z)$) haben wir mit dem Index q_i versehen, damit man weiß, in welcher Ergebnismenge wir rechnen, d.h. in welchem Zustand wir starten.

Markov-Ketten brauchen so was nicht. Bei Markov-Ketten beginnt man mit bestimmten Wahrscheinlichkeiten in bestimmten Zuständen.

Themenübersicht

Gleichverteilung

Eine gleichverteilte Zufallsvariable $X \sim \text{Uni}(a, b)$ gibt eine natürliche Zahl aus dem diskreten Intervall $\{a, \ldots, b\}$ aus. Dabei sind alle Zahlen gleich wahrscheinlich.

Der Wertebereich von X ist $W_X = \{a, \ldots, b\}$ und es gilt

$$f_X(k) = \begin{cases} \frac{1}{b-a+1}, & \text{falls } k \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info: Es gilt $|W_X| = b - a + 1$.

Info

Die Gleichverteilung bezieht sich immer auf den Wertebereich einer Zufallsvariable X. Sind die Elementarereignisse $\omega \in \Omega$ eines Wahrscheinlichkeitsraumes $W = (\Omega, \Pr)$ alle gleich wahrscheinlich, so spricht man von einer Laplace-Verteilung auf Ω. Dazu braucht man allerdings keine Zufallsvariable.

Dass ein Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ Laplace-verteilt ist, sagt nichts darüber aus, ob eine Zufallsvariable $X : \Omega \to \mathbb{R}$ gleichverteilt ist.

Beispiel

Wir betrachten nochmal den Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ aus Folie 1805 mit

$$\Omega = \{KKK, KKZ, KZK, KZZ, ZKK, ZKZ, ZZK, ZZZ\},$$

$\Pr[\omega] = \frac{1}{8}$ für alle $\omega \in \Omega$ und die Zufallsvariable

$$X: \quad \text{Anzahl der } \textit{Kopf}\text{-Würfe.}$$

Es gilt $W_X = \{0, 1, 2, 3\}$ und

$$\begin{array}{lcll} \Pr[X = 0] & = & \Pr[\{ZZZ\}] & = & 1/8, \\ \Pr[X = 1] & = & \Pr[\{KZZ, ZKZ, ZZK\}] & = & 3/8, \\ \Pr[X = 2] & = & \Pr[\{KKZ, KZK, ZKK\}] & = & 3/8, \\ \Pr[X = 3] & = & \Pr[\{KKK\}] & = & 1/8. \end{array}$$

X ist also nicht gleichverteilt, obwohl W Laplace-verteilt ist.

Bernoulli-Verteilung

Eine Bernoulli-verteilte Zufallsvariable $X \sim \text{Ber}(p)$ gibt das Ergebnis von einem Versuch an, wobei dieser mit Wahrscheinlichkeit p erfolgreich ($X = 1$) und mit Wahrscheinlichkeit $1 - p$ erfolglos ($X = 0$) ist.

Der Wertebereich von X ist $W_X = \{0, 1\}$ und für $k \in W_X$ gilt:

$$f_X(k) = \begin{cases} p, & \text{falls } k = 1 \\ 1 - p, & \text{falls } k = 0 \\ 0 & \text{sonst} \end{cases}$$

Zum Rechnen ist meistens dieser Ausdruck hilfreicher:

$$f_X(k) = \begin{cases} p^k \cdot (1 - p)^{1-k}, & \text{falls } k \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info

Jede Zufallsvariable mit Wertebereich $\{0, 1\}$, insbesondere also jede Indikatorvariable, ist automatisch Bernoulli-verteilt.

Binomialverteilung

Eine binomialverteilte Zufallsvariable $X \sim \text{Bin}(n, p)$ gibt die Anzahl der Erfolge bei n Versuchen an, wobei jeder Versuch, unabhängig von den anderen, mit Wahrscheinlichkeit p erfolgreich ist.

Der Wertebereich von X ist $W_X = \{0, 1, \ldots, n\}$ und es gilt

$$f_X(k) = \begin{cases} \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}, & \text{falls } k \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info

Die Binomialverteilung steht zur Bernoulli-Verteilung in folgender Beziehung:

- Sind $X_1, \ldots, X_n \sim \text{Ber}(p)$ unabhängige Zufallsvariablen und $X = X_1 + \ldots + X_n$, dann ist $X \sim \text{Bin}(n, p)$.
- Die Bernoulli-Verteilung ist ein Spezialfall der Binomialverteilung für $n = 1$.

Poisson-Verteilung

Eine binomialverteilte Zufallsvariable mit großem n und kleinem p kann durch eine Poisson-verteilte Zufallsvariable $X \sim \text{Poi}(\lambda)$ approximiert werden. Es gilt:

$$X \sim \text{Bin}(n, p) \overset{n \to \infty}{\longrightarrow} X \sim \text{Poi}(\lambda) \qquad (\text{für } \lambda = np).$$

Der Wertebereich von X ist $W_X = \mathbb{N}_0$ und es gilt

$$f_X(k) = \begin{cases} \frac{e^{-\lambda} \cdot \lambda^k}{k!}, & \text{falls } k \in W_X \\ 0 & \text{sonst} \end{cases}$$

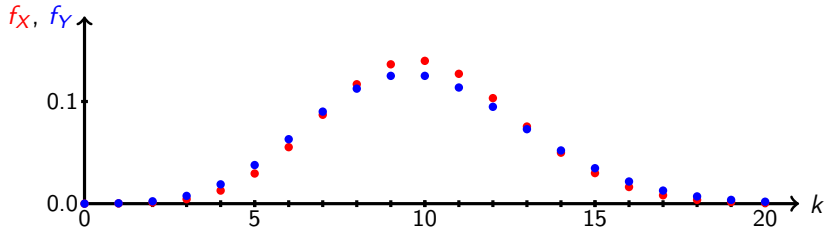
Info

Bei binomialverteilten Zufallsexperimenten benutzt man oft die Poisson-Verteilung, weil der Unterschied zwischen ihren Dichtefunktionen für großes n vernachlässigbar klein ist und die der Poisson-Verteilung viel einfacher zum Rechnen ist.

Binomialverteilung und Poisson-Verteilung sind nicht dasselbe! Nicht mal ist eine ein Spezialfall der anderen. Insbesondere ist keine Poisson-Verteilung mit $\lambda > 0$ eine Binomialverteilung!

Beispiel

Vergleicht man die Dichtefunktionen der Zufallsvariablen $X \sim \text{Bin}\left(50, \frac{1}{5}\right)$ (rote Kurve) und $Y \sim \text{Poi}(10)$ (blaue Kurve), so erkennt man, dass die Poisson-Verteilung schon für $n = 50$ eine recht gute Abschätzung der Binomialverteilung ist.



Der größte Unterschied liegt bei $k = 10$. Es gilt:

$$f_X(10) = \binom{50}{10} \cdot \left(\frac{1}{5}\right)^{10} \cdot \left(\frac{4}{5}\right)^{40} = 0.1398\ldots \quad \text{und} \quad f_Y(10) = \frac{e^{-10} \cdot 10^{10}}{10!} = 0.1251\ldots$$

Geometrische Verteilung

Eine geometrisch verteilte Zufallsvariable $X \sim \text{Geo}(p)$ gibt die Anzahl der benötigten Versuche bis zum ersten Erfolg an, wobei jeder Versuch, unabhängig von den anderen, mit Wahrscheinlichkeit p erfolgreich ist.

Der Wertebereich von X ist $W_X = \mathbb{N}$ und es gilt

$$f_X(k) = \begin{cases} p \cdot (1-p)^{k-1} & \text{falls } k \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info

Die geometrische Verteilung hat die tolle Eigenschaft gedächtnislos zu sein. D.h. sie „vergisst“ nach jeder Runde wie viele Misserfolge sie bis dahin schon hatte. Für $X \sim \text{Geo}(p)$ und alle $x, y \in W_X$ gilt nämlich:

$$\Pr[X > x + y | X > x] = \Pr[X > y].$$

Negative Binomialverteilung

Eine negativ Binomialverteilte Zufallsvariable $X \sim \text{NegBin}(n, p)$ gibt die Anzahl der benötigten Versuche bis zum n-ten Erfolg an, wobei jeder Versuch, unabhängig von den anderen, mit Wahrscheinlichkeit p erfolgreich ist.

Der Wertebereich von X ist $W_X = \{n, n+1, n+2, \ldots\}$ und es gilt

$$f_X(k) = \begin{cases} \binom{k-1}{n-1} \cdot p^n \cdot (1-p)^{k-n} & \text{falls } k \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info

Die negative Binomialverteilung steht zur geometrischen Verteilung in folgender Beziehung:

- Sind $X_1, \ldots, X_n \sim \text{Geo}(p)$ unabhängige Zufallsvariablen und $X = X_1 + \ldots + X_n$, dann ist $X \sim \text{NegBin}(n, p)$.
- Die geometrische Verteilung ist ein Spezialfall der negativen Binomialverteilung für $n = 1$.

Welche Verteilungen besitzen folgende Zufallsvariablen $X_1, \ldots, X_6$?

1. Wir würfeln gleichzeitig mit 10 fairen Würfeln. X_1 gibt die Anzahl der Würfel an, die ⚂ zeigen.
2. Wir würfeln mit einem fairen Würfel. X_2 gibt das Ergebnis des Würfels an.
3. Wir würfeln so lange mit einem fairen Würfel bis wir eine ⚀ bekommen. X_3 zählt die Gesamtanzahl der Würfe.
4. Wir würfeln mit einem fairen Würfel. X_4 ist 1, falls eine ⚅ gewürfelt wurde, sonst 0.
5. Wir würfeln so lange mit einem fairen Würfel, bis wir zum 10. mal eine ⚃ bekommen. X_5 zählt die Anzahl der Würfe insgesamt.
6. Wir würfeln gleichzeitig mit 10 fairen Würfeln und wiederholen dies 6^{11} mal. X_6 zählt, wie oft alle 10 Würfel ⚄ gezeigt haben.

1. $X_1 \sim \text{Bin}\left(10, \frac{1}{6}\right)$.
2. $X_2 \sim \text{Uni}\left(1, 6\right)$.
3. $X_3 \sim \text{Geo}\left(\frac{1}{6}\right)$ bzw. $X_3 \sim \text{NegBin}\left(1, \frac{1}{6}\right)$.
4. $X_4 \sim \text{Ber}\left(\frac{1}{6}\right)$ bzw. $X_4 \sim \text{Bin}\left(1, \frac{1}{6}\right)$.
5. $X_5 \sim \text{NegBin}\left(10, \frac{1}{6}\right)$.
6. $X_6 \sim \text{Bin}\left(6^{11}, \frac{1}{6^{10}}\right)$, also approximativ $X_6 \sim \text{Poi}\left(\lambda\right)$ mit $\lambda = 6^{11} \cdot \frac{1}{6^{10}} = 6$.

Hypergeometrische Verteilung

Gegeben sei eine Menge von $a + b$ Objekten, von denen b eine spezielle Eigenschaft haben und a nicht. Von dieser Menge werden zufällig n Elemente ohne Zurücklegen gezogen.

Die Anzahl an gezogenen Elementen, die die spezielle Eigenschaft besitzen, wird durch eine hypergeometrisch Verteilte Zufallsvariable $X \sim \text{Hyp}(n, a, b)$ modelliert.

Der Wertebereich von X ist $W_X = \{0, \ldots, n\}$ und es gilt

$$f_X(k) = \begin{cases} \frac{\binom{b}{k} \cdot \binom{a}{n-k}}{\binom{a+b}{n}} & \text{falls } k \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info

Die hypergeometrische Verteilung steht zur Binomialverteilung in folgender Beziehung:

- Werden beim Ziehen von Elementen, diese wieder zurückgelegt, dann gilt für die Anzahl X an gezogenen Elementen, die die spezielle Eigenschaft besitzen:

$$X \sim \text{Bin}\left(n, \frac{b}{a+b}\right).$$

- Der Unterschied zwischen beiden Verteilungen ist für große a und b vernachlässigbar klein. Es gilt nämlich:

$$X \sim \text{Hyp}(n, a, b) \overset{a,b\to\infty}{\longrightarrow} X \sim \text{Bin}(n, p) \qquad \left(\text{für } p = \frac{b}{a+b}\right).$$

  Intuitiv bedeutet das, dass es für eine große Anzahl an Elementen keine Rolle mehr spielt, ob diese wieder zurückgelegt werden oder nicht.

Negative Hypergeometrische Verteilung

Gegeben sei eine Menge von $a + b$ Objekten, von denen b eine spezielle Eigenschaft haben und a nicht. Von dieser Menge werden so lange Elemente ohne Zurücklegen gezogen, bis zum n-ten mal ein spezielles Element gezogen wurde.

Die Anzahl an benötigten Ziehungen wird durch eine negativ hypergeometrisch verteilte Zufallsvariable $X \sim \text{NegHyp}(n, a, b)$ modelliert.

Der Wertebereich von X ist $W_X = \{n, \ldots, a + b\}$ und es gilt

$$f_X(k) = \begin{cases} \frac{\binom{k-1}{n-1} \cdot \binom{a+b-k}{b-n}}{\binom{a+b}{b}} & \text{falls } k \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info

Die negative hypergeometrische Verteilung steht zur negativen Binomialverteilung in folgender Beziehung:

- Werden beim Ziehen von Elementen, diese wieder zurückgelegt, dann gilt für die Anzahl X an Ziehungen bis zum n-ten gezogenen Element mit der speziellen Eigenschaft:

$$X \sim \text{NegBin}\left(n, \frac{b}{a+b}\right).$$

- Der Unterschied zwischen beiden Verteilungen ist, analog zur Binomialverteilung und der hypergeometrischen Verteilung, für große a und b vernachlässigbar klein. Es gilt nämlich:

$$X \sim \text{NegHyp}(n, a, b) \overset{a,b\to\infty}{\longrightarrow} X \sim \text{NegBin}(n, p) \qquad \left(\text{für } p = \frac{b}{a+b}\right).$$

  Die Intuition ist dieselbe: für eine große Anzahl an Elementen spielt es keine Rolle mehr, ob diese wieder zurückgelegt werden oder nicht.

Es werden Bälle aus einer Urne mit 5 roten und 7 grünen Bällen gezogen. Mit den Zufallsvariablen X_1, X_2, X_3, X_4 wird folgendes gezählt:

X_1 : Ziehungen ohne Zurücklegen bis zum 3. mal ein grüner Ball gezogen wurde
X_2 : Ziehungen mit Zurücklegen bis zum 3. mal ein grüner Ball gezogen wurde
X_3 : Anzahl der gezogenen grünen Bälle nach 3 Ziehungen ohne Zurücklegen
X_4 : Anzahl der gezogenen grünen Bälle nach 3 Ziehungen mit Zurücklegen

Wie sind X_1, X_2, X_3, X_4 jeweils verteilt?

	X Erfolge bei n Versuchen	X Versuche bis n-ten Erfolg
ohne Zurücklegen	$X_3 \sim \text{Hyp}(3, 5, 7)$	$X_1 \sim \text{NegHyp}(3, 5, 7)$
mit Zurücklegen	$X_4 \sim \text{Bin}\left(3, \frac{7}{12}\right)$	$X_2 \sim \text{NegBin}\left(3, \frac{7}{12}\right)$

Beispiel

Beim Lotto werden zufällig 6 aus 49 Zahlen ohne Zurücklegen gewählt. Sei X die kleinste dieser 6 Zahlen.

Wir modellieren das Experiment ein bisschen um:

1. Wir gehen von einer Urne mit 43 roten und 6 grünen Kugeln aus.
2. Aus dieser Urne werden alle 49 Kugeln der Reihe nach gezogen und aufsteigend nummeriert (die i-te gezogene Kugel bekommt die Nummer i).
3. Die Nummern der 6 grünen Kugeln entsprechen den 6 gezogenen Zahlen beim Lotto.

X zählt dann die Anzahl an Ziehungen, bis die erste grüne Kugel gezogen wurde.

Daraus folgt:

$$X \sim \text{NegHyp}(1, 43, 6).$$

Sehr wichtig!

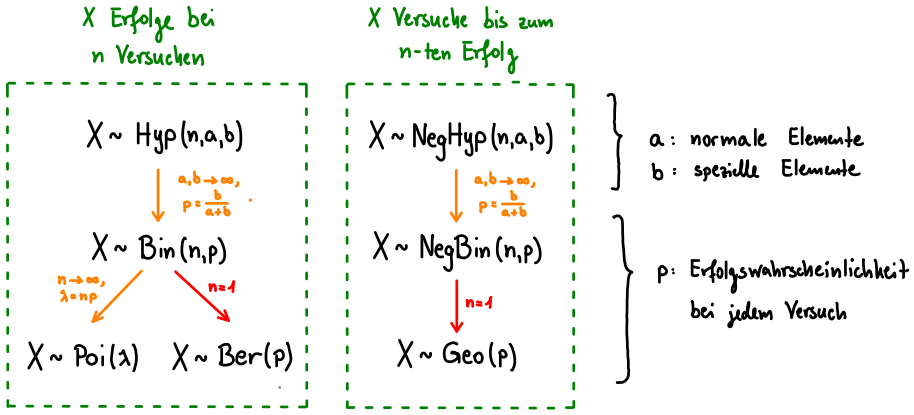
Die normale und die negative hypergeometrische Verteilungen werden üblicherweise nicht in der Vorlesung behandelt. Die Formeln habe ich zum Teil aus anderen Quellen und zum Teil selber hergeleitet. Bevor ihr sie benutzt, vergewissert euch bitte zuerst, dass ihr das dürft.

Übersicht: Wichtige diskrete Verteilungen

Verteilung	Experiment
$X \sim \text{Uni}(a, b)$	X gleichverteilt auf $\{a, \dots, b\}$.
$X \sim \text{Ber}(p)$	X Erfolge bei einem Versuch mit Erfolgswahrscheinlichkeit p.
$X \sim \text{Bin}(n, p)$	X Erfolge bei n Versuchen mit jeweils Erfolgswahrscheinlichkeit p.
$X \sim \text{Poi}(\lambda)$	Approximation für $X \sim \text{Bin}(n, p)$ für $n \to \infty$ und $\lambda = n \cdot p$.
$X \sim \text{Geo}(p)$	X Versuche, mit jeweils Erfolgswahrscheinlichkeit p, bis zum ersten Erfolg.
$X \sim \text{NegBin}(n, p)$	X Versuche, mit jeweils Erfolgswahrscheinlichkeit p, bis zum n-ten Erfolg.
$X \sim \text{Hyp}(n, a, b)$	a normale und b spezielle Elemente. X spezielle Elemente nach n Ziehungen ohne Zurücklegen.
$X \sim \text{NegHyp}(n, a, b)$	a normale und b spezielle Elemente. X Ziehungen ohne Zurücklegen bis zum n-ten speziellen Element.

Versuche vs. Erfolge

7 der 8 wichtigen Verteilungen kann man sehr schön wie folgt kategorisieren:



Rote Pfeile stellen Spezialfälle dar, **orangene** Pfeile Approximationen.

Tabelle: Formelsammlung für wichtige diskrete Verteilungen

Verteilung	W_X	$f_X(k)$	$F_X(k)$	$\mathbb{E}[X]$	$\mathrm{Var}[X]$
$X \sim \mathrm{Uni}(a, b)$	$\{a, \dots, b\}$	$\frac{1}{b-a+1}$	$\frac{k-a+1}{b-a+1}$	$\frac{a+b}{2}$	$\frac{(b-a)(b-a+2)}{12}$
$X \sim \mathrm{Ber}(p)$	$\{0, 1\}$	$p^k(1-p)^{1-k}$	$(1-p)^{1-k}$	p	$p(1-p)$
$X \sim \mathrm{Bin}(n, p)$	$\{0, \dots, n\}$	$\binom{n}{k} p^k (1-p)^{n-k}$	$\sum_{i=0}^{k} f_X(i)$	np	$np(1-p)$
$X \sim \mathrm{Poi}(\lambda)$	$\{0, \dots\}$	$\frac{e^{-\lambda} \lambda^k}{k!}$	$\sum_{i=0}^{k} f_X(i)$	λ	λ
$X \sim \mathrm{Geo}(p)$	$\{1, \dots\}$	$p(1-p)^{k-1}$	$1-(1-p)^k$	$\frac{1}{p}$	$\frac{1-p}{p^2}$
$X \sim \mathrm{NegBin}(n, p)$	$\{n, \dots\}$	$\binom{k-1}{n-1} p^n (1-p)^{k-n}$	$\sum_{i=n}^{k} f_X(i)$	$\frac{n}{p}$	$\frac{n(1-p)}{p^2}$
$X \sim \mathrm{Hyp}(n, a, b)$	$\{0, \dots, n\}$	$\frac{\binom{b}{k}\binom{a}{n-k}}{\binom{a+b}{n}}$	$\sum_{i=0}^{k} f_X(i)$	$\frac{bn}{a+b}$	$\frac{abn(a+b-n)}{(a+b-1)(a+b)^2}$
$X \sim \mathrm{NegHyp}(n, a, b)$	$\{n, \dots, a+b\}$	$\frac{\binom{k-1}{n-1}\binom{a+b-k}{b-n}}{\binom{a+b}{b}}$	$\sum_{i=n}^{k} f_X(i)$	$\frac{n(a+b+1)}{b+1}$	$\frac{na(a+b+1)(b+1-n)}{(b+1)^2(b+2)}$

Für die vollständige Tabelle mit wahrscheinlichkeitserzeugenden Funktionen siehe Folie 2005.

Infos

- Die Formeln für f_X und F_X gelten nur für $k \in W_X$.
- Für die Formeln in grau kennt man leider keine geschlossene Ausdrücke.
- Der Wert $f_X(k)$ der Dichtefunktion und der Wert $F_X(k)$ der Verteilungsfunktion sollten beide eigentlich für alle $k \in \mathbb{R}$ definiert werden. Das kostet aber Zeit, Tinte und Nerven. Deswegen schreibt das kein Mensch so formal hin.
- Falls $k \notin W_X$, dann gilt einerseits $f_X(k) = 0$ und andererseits ist $F_X(k) = F_X(k')$, für die nächstkleinere Zahl $k' \in W_X$.

Beispiel

Sei $X \sim \text{Uni}(1,6)$ beispielsweise das Ergebnis eines fairen Würfels mit $W_X = \{1, \ldots, 6\}$. Dann gilt unter anderem

$$F_X(3.75) = \Pr[X \leq 3.75] = \Pr[X \leq 3] = F_X(3),$$

da X keine Werte zwischen 3 und 4 annehmen kann.

Für $k \in W_X$ gilt bekanntlich $f_X(k) = \frac{1}{6}$ und $F_X(k) = \frac{k}{6}$. Möchte man sehr formal sein, dann müsste man folgendes schreiben:

$$f_X(k) = \begin{cases} \frac{1}{6} & \text{falls } k \in W_X \\ 0 & \text{falls } k \notin W_X \end{cases} \qquad \text{und} \qquad F_X(k) = \begin{cases} 0 & \text{falls } k < 1 \\ \frac{\lfloor k \rfloor}{6}, & \text{falls } 1 \leq k \leq 6 \\ 1 & \text{falls } k > 6. \end{cases}$$

Das macht jedoch, wie gesagt, kein Mensch!

Übungsaufgabe

Wir betrachten zwei Varianten von einem Spiel, bei denen 3 Zahlen aus der Menge $\{1, 2, 3, 4, 5\}$ mit bzw. ohne Zurücklegen gewählt werden. Seien X_1, X_2, X_3 die Ergebnisse der 3 Ziehungen und Z_1, Z_2 wie folgt:

Z_1 : größte gezogene Zahl mit Zurücklegen
Z_2 : größte gezogene Zahl ohne Zurücklegen

1. Berechne $\mathbb{E}[Z_1]$ mithilfe der Formeln auf Folie 1867.
2. Berechne $\mathbb{E}[Z_2]$ mithilfe der Modellierung aus Folie 1927.

1. Zieht man mit Zurücklegen, dann sind X_1, X_2, X_3 unabhängig mit $X_1, X_2, X_3 \sim \text{Uni}(1,5)$. Es folgt nach Folie 1867:

$$\begin{aligned}\mathbb{E}[Z_1] = \mathbb{E}[\max\{X_1, X_2, X_3\}] &= \sum_{k=1}^{5}(1 - F_{X_1}(k) \cdot F_{X_2}(k) \cdot F_{X_3}(k)) \\ &= \sum_{k=1}^{5}\left(1 - \left(\frac{k}{5}\right)^3\right) = 5 - \sum_{k=1}^{5}\left(\frac{k}{5}\right)^3 \\ &= 5 - \frac{1^3 + 2^3 + 3^3 + 4^3 + 5^3}{5^3} = 3.2.\end{aligned}$$

2. Zieht man ohne Zurücklegen, dann sind X_1, X_2, X_3 alles andere als unabhängig.
   Analog zum Beispiel auf Folie 1927 gilt aber:

$$Z_2 \sim \text{NegHyp}(3, 2, 3).$$

   Daraus folgt mithilfe der Tabelle auf Folie 1931:

$$\mathbb{E}[Z_2] = \frac{3 \cdot (2 + 3 + 1)}{3 + 1} = \frac{18}{4} = 4.5.$$

Fritz hat einen neuen Schrott-Laptop gekauft, um mit ihm online Musik hören zu können. Allerdings funktionieren bei jedem Neustart mit Wahrscheinlichkeit $\frac{2}{3}$ die Lautsprecher nicht und - unabhängig davon - geht die Internetverbindung mit Wahrscheinlichkeit $\frac{3}{4}$ nicht.

Wie oft muss Fritz im Schnitt seinen Laptop neustarten, bis er endlich online Musik hören kann?

Antwort

Sei X die Anzahl der notwendigen Neustarts. X ist geometrisch verteilt mit Parameter $p = (1 - \frac{2}{3})(1 - \frac{3}{4}) = \frac{1}{12}$. Somit ist die erwartete Anzahl der Neustarts $\mathbb{E}[X] = \frac{1}{1/12} = 12$.

Rechenregeln

1. Gedächtnislosigkeit der geometrischen Verteilung.
   Eine Zufallsvariable X ist genau dann geometrisch verteilt, wenn $W_X = \mathbb{N}$ gilt und sie gedächtnislos ist, d.h. wenn für alle $x, y \in W_X$ gilt:

$$\Pr[X > x + y | X > x] = \Pr[X > y].$$

2. Binomial-Prozess.
   Falls $T_1, T_2, T_3, \ldots \sim \text{Geo}(p)$ unabhängig und

$$X(t) := \max\{n \in \mathbb{N}_0 \mid T_1 + \ldots + T_n \leq t\}$$

   für jedes $t \in \mathbb{N}$. Dann gilt:

$$X(t) \sim \text{Bin}(t, p).$$

Rechenregeln

3. Für zusammengesetzte Zufallsvariablen gilt:

$$X \sim \text{Uni}(a, b) \qquad \Longrightarrow \qquad X + c \sim \text{Uni}(a + c, b + c) \qquad (c \in \mathbb{Z})$$

4. Für aus mehreren unabhängigen Zufallsvariablen $X_1, \ldots, X_k$ zusammengesetzte Zufallsvariablen gilt:

$$\begin{aligned}
X_i \sim \text{Ber}(p) &\Longrightarrow X_1 + \ldots + X_k \sim \text{Bin}(k, p) \\
X_i \sim \text{Bin}(n_i, p) &\Longrightarrow X_1 + \ldots + X_k \sim \text{Bin}(n_1 + \ldots + n_k, p) \\
X_i \sim \text{Poi}(\lambda_i) &\Longrightarrow X_1 + \ldots + X_k \sim \text{Poi}(\lambda_1 + \ldots + \lambda_k) \\
X_i \sim \text{Geo}(p) &\Longrightarrow X_1 + \ldots + X_k \sim \text{NegBin}(k, p) \\
X_i \sim \text{NegBin}(n_i, p) &\Longrightarrow X_1 + \ldots + X_k \sim \text{NegBin}(n_1 + \ldots + n_k, p) \\
X_i \sim \text{Geo}(p_i) &\Longrightarrow \min\{X_1, \ldots, X_k\} \sim \text{Geo}(1 - (1 - p_1) \cdot \ldots \cdot (1 - p_k))
\end{aligned}$$

Seien $p_1, \ldots, p_k \in [0,1]$ und $X_1, \ldots, X_k$ unabhängige Zufallsvariablen mit $X_i \sim \text{Ber}(p_i)$. Wir definieren Zufallsvariablen Z_1, Z_2, Z_3 wie folgt:

$$Z_1 := \min\{X_1, \ldots, X_k\}, \qquad Z_2 := \max\{X_1, \ldots, X_k\}, \qquad Z_3 := X_1 \cdot \ldots \cdot X_k.$$

1. Wie ist Z_1 verteilt?
2. Wie ist Z_2 verteilt?
3. Wie ist Z_3 verteilt?

Hinweise: Welche Werte können Z_1, Z_2, Z_3 annehmen? Wie hängen diese Werte von den Werten von $X_1, \ldots, X_k$ ab? Wenn du keinen Lösungsansatz hast, schau dir die Lösung zu 1. auf der nächsten Folie an und versuch 2. und 3. analog dazu zu lösen.

1. Für $Z_1 = \min\{X_1, \ldots, X_k\}$ gilt:

$$Z_1 = \begin{cases} 1 & \text{falls } X_1 = 1, \ldots, X_k = 1 \\ 0 & \text{sonst} \end{cases}$$

Daraus folgt:

$$\begin{aligned} \Pr[Z_1 = 1] &= \Pr[X_1 = 1, \ldots, X_k = 1] \\ &= \Pr[X_1 = 1] \cdot \ldots \cdot \Pr[X_k = 1] \\ &= p_1 \cdot \ldots \cdot p_k \end{aligned}$$

D.h.:

$$Z_1 \sim \text{Ber}(p_1 \cdot \ldots \cdot p_k).$$

2. Für $Z_2 = \max\{X_1, \ldots, X_k\}$ gilt:

$$Z_2 = \begin{cases} 0 & \text{falls } X_1 = 0, \ldots, X_k = 0 \\ 1 & \text{sonst} \end{cases}$$

Daraus folgt:

$$\begin{aligned} \Pr[Z_2 = 1] &= 1 - \Pr[Z_2 = 0] \\ &= 1 - \Pr[X_1 = 0, \ldots, X_k = 0] \\ &= 1 - \Pr[X_1 = 0] \cdot \ldots \cdot \Pr[X_k = 0] \\ &= 1 - (1 - p_1) \cdot \ldots \cdot (1 - p_k) \end{aligned}$$

D.h.:

$$Z_2 \sim \text{Ber}(1 - (1 - p_1) \cdot \ldots \cdot (1 - p_k)).$$

3. Für $Z_3 = X_1 \cdot \ldots \cdot X_k$ gilt:

$$Z_3 = \begin{cases} 1 & \text{falls } X_1 = 1, \ldots, X_k = 1 \\ 0 & \text{sonst} \end{cases}$$

D.h. es gilt $Z_3 = Z_1$ und somit:

$$Z_3 \sim \text{Ber}(p_1 \cdot \ldots \cdot p_k).$$

Das Coupon-Collector-Problem

Das Coupon-Collector-Problem befasst sich mit der Frage, wie viele zufällig ausgewählte Bilder einer Serie von n Sammelbildern zu kaufen sind, um jedes Bild mindestens einmal zu haben.

Annahmen:

- Bei jedem Kauf erhalten wir genau eine der n Figuren und
- sie sind alle gleich wahrscheinlich.

Frage: Wie groß ist die erwartete Anzahl an gekauften Bildern bis man alle n hat?

Das Coupon-Collector-Problem

Lösung: Wir teilen das Experiment in n Phasen auf. Die i-te Phase beginnt nach dem Erwerb des $(i-1)$-ten und endet mit dem Erwerb des i-ten Bildes. Für die Gesamtanzahl X der Käufe gilt

$$X = X_1 + \ldots + X_n$$

für unabhängige Zufallsvariablen $X_1, \ldots, X_n$ mit $X_i \sim \text{Geo}\left(\frac{n+1-i}{n}\right)$ für alle $i = 1, \ldots, n$.

Es folgt:

$$\mathbb{E}[X] = \sum_{i=1}^{n} \mathbb{E}[X_i] = \sum_{i=1}^{n} \frac{n}{n+1-i} = \sum_{i=1}^{n} \frac{n}{i} = n \cdot \sum_{i=1}^{n} \frac{1}{i} = nH_n,$$

wobei $H_n := \sum_{i=1}^{n} \frac{1}{i}$ die *n-te harmonische Zahl* genannt wird.

Beispiel

Ein Glücksrad besteht aus 12 gleichgroßen Feldern, die von 1 bis 12 durchnummeriert sind. Sei jede Zahl gleichwahrscheinlich und sei X die Anzahl an benötigten Drehungen, bis jede Zahl mindestens einmal vorgekommen ist.

Die erwartete Anzahl an Drehungen ist dann:

$$\mathbb{E}[X] = 12 \cdot \left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{12}\right) = 37.2385\ldots$$

Quizfrage

Ein Glücksrad besteht aus 8 gleichgroßen Felder, die von 1 bis 8 durchnummeriert sind. Sei jede Zahl gleichwahrscheinlich und sei X die Anzahl an benötigten Drehungen, bis jede gerade Zahl mindestens einmal vorgekommen ist.

Was ist die erwartete Anzahl $\mathbb{E}[X]$ an Drehungen?

Wir teilen das Experiment in 4 unabhängigen Phasen X_1, X_2, X_3, X_4 mit

$$X_1 \sim \text{Geo}\left(\frac{4}{8}\right), \qquad X_2 \sim \text{Geo}\left(\frac{3}{8}\right), \qquad X_3 \sim \text{Geo}\left(\frac{2}{8}\right), \qquad X_4 \sim \text{Geo}\left(\frac{1}{8}\right)$$

auf. Dann erhalten wir:

$$\mathbb{E}[X] = \frac{8}{4} + \frac{8}{3} + \frac{8}{2} + \frac{8}{1} = 8 \cdot \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}\right) = \frac{50}{3} = 16.\overline{6}.$$

Übungsaufgabe

Es werden Kugeln aus einer Urne mit 3 roten und 3 grünen Kugeln gezogen. Dabei werden rote Kugeln wieder zurückgelegt und grüne Kugeln nicht. Die Zufallsvariable X zählt die Anzahl an Ziehungen bis die letzte grüne Kugel gezogen wurde.

Bestimme $\mathbb{E}[X]$ und $\mathrm{Var}[X]$.

Wir teilen das Experiment, analog zur Lösung des Coupon-Collector-Problems, in drei Phasen auf:

1. X_1 zählt die Ziehungen bis der erste grüne Ball gezogen wird.
2. X_2 zählt die Ziehungen nach dem ersten grünen Ball bis zum zweiten.
3. X_3 zählt die Ziehungen nach dem zweiten grünen Ball bis zum dritten.

Dann gilt

$$X = X_1 + X_2 + X_3$$

für unabhängige Zufallsvariablen X_1, X_2, X_3 mit $X_1 \sim \text{Geo}\left(\frac{1}{2}\right)$, $X_2 \sim \text{Geo}\left(\frac{2}{5}\right)$ und $X_3 \sim \text{Geo}\left(\frac{1}{4}\right)$. Es folgt:

$$\mathbb{E}[X] = \mathbb{E}[X_1] + \mathbb{E}[X_2] + \mathbb{E}[X_3] = \frac{1}{1/2} + \frac{1}{2/5} + \frac{1}{1/4} = 8.5$$

$$\text{Var}[X] \overset{\text{unabh.}}{=} \text{Var}[X_1] + \text{Var}[X_2] + \text{Var}[X_3] = \frac{1/2}{(1/2)^2} + \frac{3/5}{(2/5)^2} + \frac{3/4}{(1/4)^2} = 17.75.$$

Themenübersicht

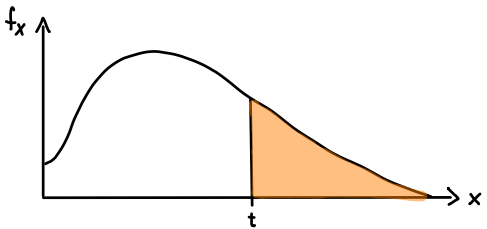
Abschätzen von Wahrscheinlichkeiten

Gegeben sei eine Zufallsvariable X mit unbekannter Dichtefunktion f_X. Das Ziel dieses Abschnittes ist es, Wahrscheinlichkeiten abzuschätzen, wenn nur wenige Informationen über X (wie z.B. $\mathbb{E}[X]$ oder $\mathrm{Var}[X]$) zur Verfügung stehen.

Markov-Ungleichung

Sei X eine Zufallsvariable mit $X \geq 0$ und $t \in \mathbb{R}$ mit $t > 0$. Dann gilt:

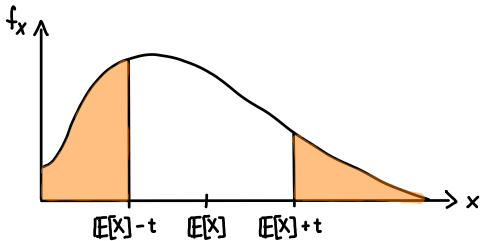
$$\Pr[X \geq t] \leq \frac{\mathbb{E}[X]}{t}$$



Chebyshev-Ungleichung

Sei X eine Zufallsvariable und $t \in \mathbb{R}$ mit $t > 0$. Dann gilt:

$$\Pr[|X - \mathbb{E}[X]| \geq t] \leq \frac{\mathrm{Var}[X]}{t^2}$$



Mit Trick:

$$\underbrace{\Pr[X \leq \mathbb{E}[X] - t]}_{\text{linke Fläche}} + \underbrace{\Pr[X \geq \mathbb{E}[X] + t]}_{\text{rechte Fläche}} \overset{\text{Trick}}{=} \underbrace{\Pr[|X - \mathbb{E}[X]| \geq t]}_{\text{beide Flächen}} \overset{\text{Cheb.}}{\leq} \frac{\mathrm{Var}[X]}{t^2}.$$

Info

Möchte man eine Wahrscheinlichkeit der Form $\Pr[X \geq \ldots]$ oder $\Pr[X \leq \ldots]$ abschätzen, dann kann man mit diesem Trick zwei coole Sachen machen:

1. Eine Fläche einfach ignorieren, z.B.:

$$\Pr[X \geq \mathbb{E}[X] + t] \overset{\text{Trick}}{\leq} \Pr[|X - \mathbb{E}[X]| \geq t] \overset{\text{Cheb.}}{\leq} \frac{\text{Var}[X]}{t^2}.$$

   Dadurch wird die Abschätzung schlechter, aber was solls!

2. Wenn beide Flächen gleich groß sind, einfach zweimal eine von beiden nehmen, z.B.:

$$\Pr[X \geq \mathbb{E}[X] + t] \overset{\text{Trick}}{=} \frac{1}{2} \Pr[|X - \mathbb{E}[X]| \geq t] \overset{\text{Cheb.}}{\leq} \frac{1}{2} \cdot \frac{\text{Var}[X]}{t^2}.$$

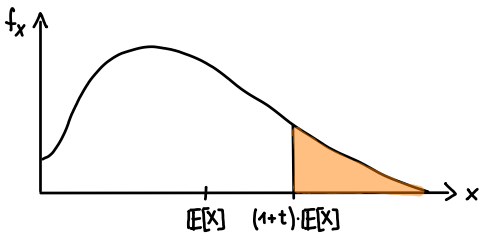
   Das kann man machen, wenn f_X achsensymmetrisch zu $\mathbb{E}[X]$ ist (z.B. $X \sim \text{Bin}(n, \frac{1}{2})$).

Beide Fälle funktionieren auch für $\Pr[X \leq \mathbb{E}[X] - t]$ statt $\Pr[X \geq \mathbb{E}[X] + t]$.

Chernoff-Schranken (upper tail)

Sei $X = X_1 + \ldots + X_n$ die Summe von unabhängigen Zufallsvariablen mit $X_i \sim \text{Ber}(p_i)$ und $t \in \mathbb{R}$ mit $t > 0$. Dann gilt:

$$\Pr[X \geq (1+t)\mathbb{E}[X]] \leq \left(\frac{e^t}{(1+t)^{1+t}} \right)^{\mathbb{E}[X]}.$$



Chernoff-Schranken (lower tail)

Sei $X = X_1 + \ldots + X_n$ die Summe von unabhängigen Zufallsvariablen mit $X_i \sim \text{Ber}(p_i)$ und $t \in \mathbb{R}$ mit $0 < t < 1$. Dann gilt:

$$\Pr[X \leq (1-t)\mathbb{E}[X]] \leq \left(\frac{e^{-t}}{(1-t)^{1-t}} \right)^{\mathbb{E}[X]}.$$

Infos

- Die Chernoff-Schranken gelten auch für $X \sim \text{Bin}(n, p)$ oder $X \sim \text{Poi}(\lambda)$ (wird üblicherweise in den Tutorübungen bewiesen).
- Damit die Chernoff-Schranken anwendbar sind, muss X nicht notwendigerweise Binomialverteilt sein! Die Zufallsvariablen $X_1, \ldots, X_n$ sind zwar alle unabhängig und Bernoulli-verteilt, aber sie dürfen verschiedene Erfolgswahrscheinlichkeiten $p_1, \ldots, p_n$ besitzen!
- Der Erwartungswert $\mathbb{E}[X]$ lässt sich ganz einfach berechnen. Wegen $X_i \sim \text{Ber}(p_i)$ für alle $1 \leq i \leq n$ gilt:

$$\mathbb{E}[X] = \mathbb{E}[X_1 + \ldots + X_n] = \mathbb{E}[X_1] + \ldots + \mathbb{E}[X_n] = p_1 + \ldots + p_n.$$

Untere Schranken

Die vier Ungleichungen haben die Form „$\Pr[\ldots \geq a] \leq b$“ bzw. „$\Pr[\ldots \leq a] \leq b$“, d.h. sie geben eine obere Schranke b für gewisse Wahrscheinlichkeiten an. Möchte man eine untere Schranke finden, dann kann aus jeder oberen Schranke eine entsprechende untere Schranke für das Gegenereignis gefunden werden.

Es gilt:

$$\Pr[\ldots < a] \geq 1 - b \quad \Longleftrightarrow \quad \Pr[\ldots \geq a] \leq b,$$

$$\Pr[\ldots > a] \geq 1 - b \quad \Longleftrightarrow \quad \Pr[\ldots \leq a] \leq b.$$

Gesetz der großen Zahlen

Seien $X_1, \ldots, X_n$ die Ergebnisse von n unabhängigen Ausführungen eines Zufallsexperiments X und

$$\overline{X} = \frac{X_1 + \ldots + X_n}{n}$$

der Mittelwert aller X_i. Dann gilt für alle $s, t > 0$:

$$n \geq \frac{\mathrm{Var}[X]}{st^2} \qquad \Longrightarrow \qquad \Pr\left[|\overline{X} - \mathbb{E}[X]| \geq t\right] \leq s.$$

Daraus folgt für ein beliebiges $t > 0$:

$$\lim_{n \to \infty} \Pr\left[|\overline{X} - \mathbb{E}[X]| \geq t\right] = 0.$$

Der Ausdruck $\Pr\left[|\overline{X} - \mathbb{E}[X]| \geq t\right] \leq s$ ist äquivalent zu

$$\Pr\left[|\overline{X} - \mathbb{E}[X]| < t\right] > 1 - s.$$

D.h. wenn man ein Experiment oft genug wiederholt (mindestens $\mathrm{Var}[X]/st^2$ mal), dann kann man die Abweichung $|\overline{X} - \mathbb{E}[X]|$ zwischen dem erwarteten Ergebnis $\mathbb{E}[X]$ und dem Mittelwert $\overline{X}$ der Ergebnisse mit beliebig großer Wahrscheinlichkeit beliebig klein halten.

t ist eine obere Grenze für die Abweichung zwischen $\mathbb{E}[X]$ und $\overline{X}$ und $1 - s$ eine untere Grenze für die Wahrscheinlichkeit.

Das Arithmetische Mittel

Für unabhängige Ausführungen $X_1, \ldots, X_n$ einer Zufallsvariable X ist das *arithmetische Mittel* definiert als

$$\overline{X} := \frac{X_1 + \ldots + X_n}{n}.$$

Diese ist eine sehr wichtige zusammengesetzte Zufallsvariable, die beim Gesetz der großen Zahlen zum ersten mal auftaucht, aber ab jetzt ständig wieder vorkommen wird. Für sie gilt:

$$\mathbb{E}\left[\overline{X}\right] = \mathbb{E}[X] \qquad \text{und} \qquad \mathrm{Var}\left[\overline{X}\right] = \frac{\mathrm{Var}[X]}{n}.$$

Die Herleitung dieser zwei Formeln ist auf der nächsten Folie. In Zukunft dürft ihr sie direkt verwenden!

Hier ist die Herleitung beider Formeln:

$$
\begin{aligned}
\mathbb{E}\left[\overline{X}\right] &= \mathbb{E}\frac{X_1 + \ldots + X_n}{n} \\
&= \frac{1}{n} \cdot \mathbb{E}[X_1 + \ldots + X_n] \\
&= \frac{1}{n} \cdot (\mathbb{E}[X_1] + \ldots + \mathbb{E}[X_n]) \\
&= \frac{1}{n} \cdot n \cdot \mathbb{E}[X] \\
&= \mathbb{E}[X],
\end{aligned}
\qquad
\begin{aligned}
\mathrm{Var}\left[\overline{X}\right] &= \mathrm{Var}\left[\frac{X_1 + \ldots + X_n}{n}\right] \\
&= \left(\frac{1}{n}\right)^2 \cdot \mathrm{Var}[X_1 + \ldots + X_n] \\
&= \left(\frac{1}{n}\right)^2 \cdot (\mathrm{Var}[X_1] + \ldots + \mathrm{Var}[X_n]) \\
&= \left(\frac{1}{n}\right)^2 \cdot n \cdot \mathrm{Var}[X] \\
&= \frac{\mathrm{Var}[X]}{n}.
\end{aligned}
$$

$\mathrm{Var}[X_1 + \ldots + X_n] = \mathrm{Var}[X_1] + \ldots + \mathrm{Var}[X_n]$ gilt nur, weil $X_1, \ldots, X_n$ unabhängig sind.

Beispiel

Wie oft muss man mit einem fairen Würfel würfeln, damit der Durchschnitt $\overline{X}$ aller gewürfelten Augenzahlen mit mindestens 95% Wahrscheinlichkeit echt zwischen 3 und 4 liegt?

Gesucht ist also das kleinste n, das die Ungleichung

$$\Pr\left[3 < \overline{X} < 4\right] \geq 0.95$$

mit $\overline{X} = \frac{X_1 + \ldots + X_n}{n}$ für unabhängige Ausführungen $X_1, \ldots, X_n$ von $X \sim \mathrm{Uni}(1, 6)$ erfüllt.

Beispiel

Gesucht ist also das kleinste $n_0 \in \mathbb{N}$, so dass für alle $n \geq n_0$ die obere Ungleichung gilt. Aus

$$a - b < x < a + b \qquad \Longleftrightarrow \qquad -b < x - a < b \qquad \Longleftrightarrow \qquad |x - a| < b$$

folgt, dass die zu beweisende Ungleichung äquivalent zu

$$\Pr\left[|\overline{X} - 3.5| < 0.5\right] \geq 0.95$$

ist. Aus Folie 1961 folgt wiederum, dass folgende Ungleichung gelten muss:

$$\Pr\left[|\overline{X} - 3.5| \geq 0.5\right] \leq 0.05.$$

Beispiel

Mithilfe von Folie 1964 und $X \sim \mathrm{Uni}(1,6)$ erhalten wir:

$$\mathbb{E}\big[\overline{X}\big] = \mathbb{E}[X] = \frac{7}{2} \qquad \text{und} \qquad \mathrm{Var}\big[\overline{X}\big] = \frac{\mathrm{Var}[X]}{n} = \frac{35}{12n}.$$

Mit der Chebyshev-Ungleichung erhalten wir:

$$\Pr\big[|\overline{X} - 3.5| \geq 0.5\big] = \Pr\big[|\overline{X} - \mathbb{E}\big[\overline{X}\big]| \geq 0.5\big] \overset{\text{Cheb.}}{\leq} \frac{\mathrm{Var}\big[\overline{X}\big]}{0.5^2} = \frac{35/12n}{0.5^2} = \frac{35}{3n} \overset{!}{\leq} 0.05.$$

Die letzte Ungleichung liefert

$$n \overset{!}{\geq} \frac{35}{3 \cdot 0.05} = 233.333\ldots$$

D.h. wir müssen mindestens $n_0 = 234$ mal würfeln.

Übrigens: Das Ausrufezeichen über dem $\geq$-Zeichen beudetet „soll sein“.

Übungsaufgabe

Die Übungsleitung einer gewissen Vorlesungen erstellt eine Klausur mit 160 Fragen zum Ankreuzen.

- 80 davon sind Wahr-oder-Falsch-Fragen, d.h. sie haben nur zwei Antwortmöglichkeiten.
- Die restlichen 80 sind Multiple-Choice-Fragen mit vier Antwortmöglichkeiten, wobei genau eine der vier richtig ist.

Zum Bestehen muss man mindestens 60% der insgesamt 160 Fragen richtig beantwortet haben, d.h. 96 oder mehr. Die Fragen sind natürlich so schwer, dass man nur raten kann.

Welche Chancen zum Bestehen versprechen die Ungleichungen von Markov, Chebyshev und von Chernoff?

Wir definieren unabhängige Zufallsvariablen $X_1, \ldots, X_{80}, Y_1, \ldots, Y_{80}$ mit $X_i \sim \text{Ber}(\frac{1}{2})$ und $Y_i \sim \text{Ber}(\frac{1}{4})$, wobei:

$$X_i = \begin{cases} 1 & \text{falls } i\text{-te Wahr-oder-Falsch-Frage richtig geraten wurde} \\ 0 & \text{sonst} \end{cases}$$

und

$$Y_i = \begin{cases} 1 & \text{falls } i\text{-te Multiple-Choice-Frage richtig geraten wurde} \\ 0 & \text{sonst} \end{cases}$$

Für die gesamte Anzahl an richtigen Fragen Z gilt:

$$Z = X_1 + \ldots + X_{80} + Y_1 + \ldots + Y_{80}$$

Erinnerung: Für $X_i \sim \text{Ber}(p_i)$ gilt $\mathbb{E}[X_i] = p_i$ und $\text{Var}[X_i] = p_i(1 - p_i)$.

Für den Erwartungswert $\mathbb{E}[Z]$ gilt:

$$\begin{aligned}
\mathbb{E}[Z] &= \mathbb{E}[X_1 + \ldots + X_{80} + Y_1 + \ldots + Y_{80}] \\
&= \mathbb{E}[X_1] + \ldots + \mathbb{E}[X_{80}] + \mathbb{E}[Y_1] + \ldots + \mathbb{E}[Y_{80}] \\
&= 80 \cdot \mathbb{E}[X_i] + 80 \cdot \mathbb{E}[Y_i] \\
&= 80 \cdot \frac{1}{2} + 80 \cdot \frac{1}{4} \\
&= 60
\end{aligned}$$

Für die Varianz $\mathrm{Var}[Z]$ gilt:

$$\begin{aligned}
\mathrm{Var}[Z] &= \mathrm{Var}[X_1 + \ldots + X_{80} + Y_1 + \ldots + Y_{80}] \\
&\overset{\text{unabh.}}{=} \mathrm{Var}[X_1] + \ldots + \mathrm{Var}[X_{80}] + \mathrm{Var}[Y_1] + \ldots + \mathrm{Var}[Y_{80}] \\
&= 80 \cdot \mathrm{Var}[X_i] + 80 \cdot \mathrm{Var}[Y_i] \\
&= 80 \cdot \frac{1}{2} \cdot \frac{1}{2} + 80 \cdot \frac{1}{4} \cdot \frac{3}{4} \\
&= 35
\end{aligned}$$

Markov:

$$\Pr[Z \geq 96] \leq \frac{\mathbb{E}[Z]}{96} = \frac{60}{96} = 62.5\%$$

Chebyshev:

$$\Pr[Z \geq 96] = \Pr[Z \geq 60 + 36] \overset{\text{Trick}}{\leq} \Pr[|Z - 60| \geq 36] \leq \frac{\mathrm{Var}[Z]}{36^2} = \frac{35}{36^2} \approx 2.7\%$$

Chernoff:

$$\Pr[Z \geq 96] = \Pr[Z \geq (1 + 0.6) \cdot 60] \leq \left(\frac{e^{0.6}}{(1 + 0.6)^{1+0.6}} \right)^{60} \approx 0.01\%$$

Die Wahrscheinlichkeit zum Bestehen ist also höchstens 0.01%.

Zusammenfassung: Ungleichungen

- **Markov-Ungleichung**
  Sei X eine Zufallsvariable mit $X \geq 0$ und $t \in \mathbb{R}$ mit $t > 0$. Dann gilt:

$$\Pr[X \geq t] \leq \frac{\mathbb{E}[X]}{t}.$$

- **Chebyshev-Ungleichung**
  Sei X eine Zufallsvariable und $t \in \mathbb{R}$ mit $t > 0$. Dann gilt:

$$\Pr[|X - \mathbb{E}[X]| \geq t] \leq \frac{\mathrm{Var}[X]}{t^2}.$$

  Trick:

$$\Pr[|X - \mathbb{E}[X]| \geq t] = \Pr[X \leq \mathbb{E}[X] - t] + \Pr[X \geq \mathbb{E}[X] + t].$$

- **Chernoff-Schranke (upper tail)**
  Falls X eine Summe unabhängiger, Bernoulli-verteilter Zufallsvariablen ist, dann gilt für jedes $t \in \mathbb{R}$ mit $t > 0$:

$$\Pr[X \geq (1+t)\mathbb{E}[X]] \leq \left(\frac{e^t}{(1+t)^{1+t}}\right)^{\mathbb{E}[X]}.$$

Zusammenfassung: Ungleichungen

- **Chernoff-Schranke (lower tail)**
  Falls X eine Summe unabhängiger, Bernoulli-verteilter Zufallsvariablen ist, dann gilt für jedes $t \in \mathbb{R}$ mit $0 < t < 1$:

$$\Pr[X \leq (1-t)\mathbb{E}[X]] \leq \left(\frac{e^{-t}}{(1-t)^{1-t}} \right)^{\mathbb{E}[X]}.$$

- **Gesetz der großen Zahlen**
  Seien $X_1, \ldots, X_n$ unabhängig und identisch verteilt zu X und

$$\overline{X} = \frac{X_1 + \ldots + X_n}{n}.$$

  Dann gilt für alle $s, t > 0$:

$$n \geq \frac{\mathrm{Var}[X]}{st^2} \qquad \Longrightarrow \qquad \Pr\left[|\overline{X} - \mathbb{E}[X]| \geq t\right] \leq s.$$

  Daraus folgt für ein beliebiges $t > 0$:

$$\lim_{n \to \infty} \Pr\left[|\overline{X} - \mathbb{E}[X]| \geq t\right] = 0.$$

Themenübersicht

Wahrscheinlichkeitserzeugende Funktion

Zu einer Zufallsvariable X mit $W_X \subseteq \mathbb{N}_0$ ist die wahrscheinlichkeitserzeugende Funktion G_X von X definiert als

$$G_X(s) := \mathbb{E}\left[s^X\right].$$

Mit dem Satz für den Erwartungswert transformierter Zufallsvariablen erhalten wir

$$G_X(s) = \sum_{k=0}^{\infty} f_X(k) \cdot s^k.$$

Erinnerung

Der Satz für den Erwartungswert transformierter Zufallsvariablen besagt für eine beliebige Funktion $g : \mathbb{R} \to \mathbb{R}$:

$$\mathbb{E}[g(X)] = \sum_{k \in W_X} g(k) \cdot f_X(k).$$

Für $g(x) = s^x$ erhalten wir:

$$G_X(s) = \mathbb{E}\left[s^X\right] = \sum_{k=0}^{\infty} s^k \cdot f_X(k).$$

Wir schreiben aber s^k rechts neben $f_X(k)$, damit $G_X(s)$ die Form eines Polynoms bzw. einer Potenzreihe hat.

Beispiel

Sei X eine Zufallsvariable mit $W_X = \{0, 1, 3, 6\}$ und folgender Dichtefunktion:

k	0	1	3	6
$f_X(k)$	1/2	1/4	1/6	1/12

Dann gilt:

$$G_X(s) = \frac{1}{2} + \frac{1}{4}s + \frac{1}{6}s^3 + \frac{1}{12}s^6$$

Noch ein Beispiel

Sei $X \sim \text{Geo}\left(\frac{1}{2}\right)$ eine geometrisch verteilte Zufallsvariable. Dann gilt $W_X = \mathbb{N}$ und:

$$\begin{aligned} G_X(s) = \sum_{k=0}^{\infty} f_X(k) \cdot s^k &= \sum_{k=1}^{\infty} \frac{1}{2} \left(1 - \frac{1}{2}\right)^{k-1} \cdot s^k \\ &= \sum_{k=1}^{\infty} \left(\frac{1}{2}\right)^k \cdot s^k \\ &= \sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^{k+1} \cdot s^{k+1} \\ &= \frac{1}{2}s \cdot \sum_{k=0}^{\infty} \left(\frac{1}{2}s\right)^k \\ &\overset{(*)}{=} \frac{1}{2}s \cdot \frac{1}{1 - \frac{1}{2}s} = \frac{s}{2 - s} \end{aligned}$$

Bei $(*)$ wurde wieder die geometrische Reihe benutzt (s. Folie 1730).

Infos

- Damit eine Zufallsvariable überhaupt eine wahrscheinlichkeitserzeugende Funktionen besitzt, benötigen wir die Annahme $W_X \subseteq \mathbb{N}_0$.
- Wegen $W_X \subseteq \mathbb{N}_0$, ist es auch egal, ob man immer „$\sum_{k \in W_X}$“ oder „$\sum_{k=0}^{\infty}$“ schreibt.
- Die Annahme $W_X \subseteq \mathbb{N}_0$ schränkt uns zum Glück minimal ein, denn die meisten diskreten Zufallsvariablen in DWT erfüllen sie.
- Ein Beispiel einer diskreten Zufallsvariable mit $W_X \nsubseteq \mathbb{N}_0$ ist X mit $W_X = \{1, \sqrt{2}, \sqrt{3}, 2\}$ und f_X beliebig. Wegen $\sqrt{2}, \sqrt{3} \notin \mathbb{N}_0$ besitzt X keine wahrscheinlichkeitserzeugende Funktion .

Zu einer Zufallsvariable X mit $W_X \subseteq \mathbb{N}_0$ seien ihre wahrscheinlichkeitserzeugende Funktion $G_X(s)$ und deren Ableitung $G'_X(s)$ wie folgt gegeben.

$$G_X(s) = f_X(0) + f_X(1)s + f_X(2)s^2 + f_X(3)s^3 + f_X(4)s^4 + \dots$$
$$G'_X(s) = f_X(1) + 2f_X(2)s + 3f_X(3)s^2 + 4f_X(4)s^3 + \dots$$

1. Was sind $G_X(0)$, $G'_X(0)$, $G_X(1)$ und $G'_X(1)$?
2. Was ist $G''''(0)$?
3. Wie kann man $f_X(k)$ mithilfe von $G^{(k)}(s)$ bestimmen?

Hinweis: Mit $G^{(k)}(s)$ ist die k-te Ableitung von G_X nach s gemeint, also $\frac{\mathrm{d}^k G_X}{\mathrm{d}s^k}$.

1. Es gilt:

$$\begin{array}{rcll} G_X(0) & = & f_X(0) & = \Pr[X=0] \\ G'_X(0) & = & f_X(1) & = \Pr[X=1] \\ G_X(1) & = & f_X(0)+f_X(1)+f_X(2)+f_X(3)+f_X(4)+\ldots & = 1 \\ G'_X(1) & = & f_X(1)+2f_X(2)+3f_X(3)+4f_X(4)+\ldots & = \mathbb{E}[X] \end{array}$$

2. Für $G''''(0)$ gilt:

$$G''''(0) = 4! \cdot f_X(4).$$

3. Für ein beliebiges $k \in \mathbb{N}_0$ gilt $G^{(k)}(0) = k! \cdot f_X(k)$. Daraus folgt:

$$f_X(k) = \frac{G^{(k)}(0)}{k!}.$$

Noch eine Quizfrage

Sei $f : \mathbb{R} \to \mathbb{R}$ mit

$$f(s) = \frac{2}{2 - s}$$

für alle $s \neq 2$. Gibt es eine Zufallsvariable X mit wahrscheinlichkeitserzeugender Funktion $G_X = f$?

Antwort

Nö. Dazu müsste unter anderem $f(1) = 1$ gelten. Es gilt aber $f(1) = \frac{2}{2-1} = 2$.

- Für die ersten n Ableitungen von G_X gilt:

$$G_X(s) = \sum_{k=0}^{\infty} f_X(k) \cdot s^k$$

$$G'_X(s) = \sum_{k=0}^{\infty} k \cdot f_X(k) \cdot s^{k-1}$$

$$G''_X(s) = \sum_{k=0}^{\infty} k \cdot (k-1) \cdot f_X(k) \cdot s^{k-2}$$

$$\vdots$$

$$G_X^{(n)}(s) = \sum_{k=0}^{\infty} k^{\underline{n}} \cdot f_X(k) \cdot s^{k-n}$$

- Für $s = 1$ erhalten wir:

$$G_X^{(n)}(1) = \sum_{k=0}^{\infty} k^{\underline{n}} \cdot f_X(k) = \mathbb{E}\left[X^{\underline{n}}\right].$$

Für die zweite Gleichung wurde wieder der Satz für den Erwartungswert transformierter Zufallsvariablen $\mathbb{E}[g(X)] = \sum_{k \in W_X} g(k) \cdot f_X(k)$ mit $g(x) = x^{\underline{n}}$ benutzt.

- Mithilfe von

$$G_X^{(n)}(1) = \mathbb{E}\left[X^{\underline{n}}\right]$$

erhalten wir für den Erwartungswert von X:

$$\mathbb{E}[X] = \mathbb{E}\left[X^{\underline{1}}\right] = G_X'(1).$$

Für die Varianz folgt:

$$\begin{aligned}
\mathrm{Var}[X] &= \mathbb{E}\left[X^2\right] - \mathbb{E}[X]^2 \\
&= \mathbb{E}[X^2 - X + X] - \mathbb{E}[X]^2 \\
&= \mathbb{E}[X(X-1) + X] - \mathbb{E}[X]^2 \\
&= \mathbb{E}[X^{\underline{2}} + X] - \mathbb{E}[X]^2 \\
&= \mathbb{E}[X^{\underline{2}}] + \mathbb{E}[X] - \mathbb{E}[X]^2 \\
&= G_X''(1) + G_X'(1) - G_X'(1)^2
\end{aligned}$$

Übungsaufgabe

Gegeben sei eine Zufallsvariable X mit wahrscheinlichkeitserzeugender Funktion

$$G_X(s) = \left(\frac{s+1}{2}\right)^8.$$

1. Bestimme $G_X'(s)$.
2. Bestimme $G_X''(s)$.
3. Berechne $\mathbb{E}[X]$.
4. Berechne $\mathrm{Var}[X]$.

Erinnerung: Die Kettenregel lautet:

$$(f(g(x)))' = f'(g(x)) \cdot g'(x).$$

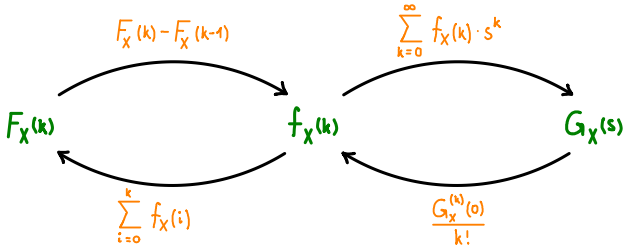
Lösung

1. $G'_X(s) = 8\left(\frac{s+1}{2}\right)^7 \cdot \frac{1}{2} = 4\left(\frac{s+1}{2}\right)^7$.
2. $G''_X(s) = 28\left(\frac{s+1}{2}\right)^6 \cdot \frac{1}{2} = 14\left(\frac{s+1}{2}\right)^6$.
3. $\mathbb{E}[X] = G'_X(1) = 4$.
4. $\mathrm{Var}[X] = G''_X(1) + G'_X(1) - G'_X(1)^2 = 14 + 4 - 4^2 = 2$.

Eindeutigkeit wahrscheinlichkeitserzeugender Funktionen

Die Dichtefunktion f_X und die Verteilungsfunktion F_X einer Zufallsvariable X mit $W_X \subseteq \mathbb{N}_0$ sind durch die wahrscheinlichkeitserzeugende Funktion von X eindeutig bestimmt.

- Nach diesem Satz bestimmt $G_X(s)$ die Dichtefunktion f_X und die Verteilungsfunktion F_X von X eindeutig. D.h. man kann aus einer der Funktionen F_X, f_X und G_X alle anderen berechnen:



- Identisch verteilte Zufallsvariablen X und Y mit $W_X, W_Y \subseteq \mathbb{N}_0$ haben also auch dieselben wahrscheinlichkeitserzeugende Funktionen, d.h.: $G_X(k) = G_Y(k)$.

  Aber (again and again and again): X, Y *identisch verteilt* heißt nicht, dass $X = Y$ gelten muss!

Summen von Zufallsvariablen

Für unabhängige Zufallsvariablen $X_1, \ldots, X_n$ mit $W_{X_1}, \ldots, W_{X_n} \subseteq \mathbb{N}_0$ und $Z = X_1 + \ldots + X_n$ gilt:

$$G_Z(s) = G_{X_1}(s) \cdot \ldots \cdot G_{X_n}(s).$$

Übungsaufgabe

Für eine Poisson-verteilte Zufallsvariable X gilt:

$$X \sim \text{Poi}(\lambda) \quad \Longleftrightarrow \quad G_X(s) = e^{\lambda(s-1)}.$$

Seien nun

$$X_1 \sim \text{Poi}(1), \quad X_2 \sim \text{Poi}(2), \quad X_3 \sim \text{Poi}(3), \quad X_4 \sim \text{Poi}(4)$$

unabhängige Zufallsvariablen und $Z := X_1 + X_2 + X_3 + X_4$.

Wie ist Z verteilt? (*Hinweis:* Bestimme $G_Z(s)$.)

Nach dem Satz über Summen von Zufallsvariablen gilt:

$$\begin{aligned} G_Z(s) &= G_{X_1}(s) \cdot G_{X_2}(s) \cdot G_{X_3}(s) \cdot G_{X_4}(s) \\ &= e^{s-1} \cdot e^{2(s-1)} \cdot e^{3(s-1)} \cdot e^{4(s-1)} \\ &= e^{s-1+2(s-1)+3(s-1)+4(s-1)} \\ &= e^{10(s-1)} \end{aligned}$$

Für Z gilt also $Z \sim \text{Poi}(10)$.

- Diesen Satz kann man sehr einfach mit der Multiplikativität des Erwartungswerts beweisen:

$$\begin{aligned} G_Z(s) = \mathbb{E}\left[s^Z\right] &= \mathbb{E}\left[s^{X_1+\ldots+X_n}\right] \\ &= \mathbb{E}\left[s^{X_1} \cdot \ldots \cdot s^{X_n}\right] \\ &= \mathbb{E}\left[s^{X_1}\right] \cdot \ldots \cdot \mathbb{E}\left[s^{X_n}\right] \qquad \text{(da } X_1, \ldots, X_n \text{ unabhängig)} \\ &= G_{X_1}(s) \cdot \ldots \cdot G_{X_n}(s) \end{aligned}$$

- Wahrscheinlichkeitserzeugende Funktionen sind sehr unintuitiv. Dem Graph von G_X kann kaum was über die Wahrscheinlichkeitsverteilung von X entnommen werden. Man kann höchstens erkennen, ob G_X keine wahrscheinlichkeitserzeugende Funktion ist, indem man $G_X(1) \neq 1$ überprüft. $G_X(1) = 1$ impliziert aber wiederum nicht, dass G_X schon eine wahrscheinlichkeitserzeugende Funktion ist.

- Nützlich sind wahrscheinlichkeitserzeugende Funktionen vor allem, wenn wir mit Summen von Zufallsvariablen hantieren müssen.

  Die Formel

  $$G_{X+Y}(s) = G_X(s) \cdot G_Y(s)$$

  ist viel einfacher als

  $$f_{X+Y}(k) = \sum_{i \in W_x} f_X(i) \cdot f_Y(k-i).$$

  Spätestens wenn es nicht nur um zwei, sondern um mehrere Zufallsvariablen geht, merkt man wie viel einfacher es ist $G_{X_1+\ldots+X_n}(s)$ zu bestimmen als $f_{X_1+\ldots+X_n}(k)$.

Zufällige Summen

Seien X und N zwei Zufallsvariablen, $X_1, X_2, X_3, \ldots$ unabhängige Ausführungen von X und

$$Z = \sum_{i=1}^{N} X_i.$$

Dann gilt:

$$G_Z(s) = G_N(G_X(s)) \qquad \text{und} \qquad \mathbb{E}[Z] = \mathbb{E}[N] \cdot \mathbb{E}[X].$$

Info

In der Vorlesung wurde die erste Aussage bewiesen. Hier ist die Herleitung der Folgerung $\mathbb{E}[Z] = \mathbb{E}[N] \cdot \mathbb{E}[X]$, falls sie euch interessiert.

Mithilfe der Kettenregel folgt für die Ableitung G'_Z von G_Z:

$$G'_Z(s) = G'_N(G_X(s)) \cdot G'_X(s).$$

Setzt man $s = 1$ ein, so erhält man:

$$\underbrace{G'_Z(1)}_{\mathbb{E}[Z]} = G'_N(\underbrace{G_X(1)}_{=1}) \cdot G'_X(1) = \underbrace{G'_N(1)}_{\mathbb{E}[N]} \cdot \underbrace{G'_X(1)}_{\mathbb{E}[X]}.$$

Übrigens: Eine Zusammenfassung aller wichtigen Ableitungsregeln findet ihr im AI Trainer.

Wichtig!

Ihr dürft beide Aussagen über zufällige Summen ohne Beweis benutzen. Versucht bitte nicht eine von ihnen in der Klausur zu beweisen oder begründen. Aussagen wie

$$Z = N \cdot X, \qquad \mathbb{E}[Z] = N \cdot \mathbb{E}[X], \qquad \mathbb{E}[Z] = \sum_{i=1}^{\mathbb{E}[N]} \mathbb{E}[X_i] \qquad \text{oder} \qquad Z \sim \text{Bin}(\mathbb{E}[N], p)$$

machen alle keinen Sinn und können nur zu Punktabzügen führen. Schreibt BITTE ganz einfach:

$$G_Z(s) = G_N(G_X(s)) = \dots \qquad \text{bzw.} \qquad \mathbb{E}[Z] = \mathbb{E}[N] \cdot \mathbb{E}[X] = \dots$$

und überlasst den Beweis der Vorlesung/Zentralübung.

Seien X und N zwei Zufallsvariablen, $X_1, X_2, X_3, \ldots$ unabhängige Ausführungen von X und $Z = X_1 + \ldots + X_N$. Was ist an folgender Argumentation faul?

Es gilt:

$$\mathbb{E}[Z] = \mathbb{E}[X_1 + \ldots + X_N] = \mathbb{E}[X_1] + \ldots + \mathbb{E}[X_N] = N \cdot \mathbb{E}[X].$$

$\mathbb{E}[]$ *auf beiden Seiten liefert:*

$$\mathbb{E}[\mathbb{E}[Z]] = \mathbb{E}[N \cdot \mathbb{E}[X]].$$

Wegen $\mathbb{E}[\mathbb{E}[Z]] = \mathbb{E}[Z]$ *und* $\mathbb{E}[N \cdot \mathbb{E}[X]] = \mathbb{E}[N] \cdot \mathbb{E}[X]$ *folgt:*

$$\mathbb{E}[Z] = \mathbb{E}[N] \cdot \mathbb{E}[X].$$

In dieser Argumentation gibt es zwei gravierende Fehler:

1. $\mathbb{E}[Z]$ sollte eine Zahl liefern. $N \cdot \mathbb{E}[X]$ ist aber keine Zahl, sondern eine Zufallsvariable, die aus einer Zahl $\mathbb{E}[X]$ und einer Zufallsvariable N zusammengesetzt ist.
2. Die Ausdrücke $\mathbb{E}[\mathbb{E}[Z]]$ und $\mathbb{E}[\mathbb{E}[X]]$ sind nicht definiert. Man kann $\mathbb{E}[]$ nur auf Zufallsvariablen anwenden. $\mathbb{E}[Z]$ und $\mathbb{E}[X]$ sind aber keine Zufallsvariablen, sondern Zahlen.

Der Schritt $\mathbb{E}[N \cdot \mathbb{E}[X]] = \mathbb{E}[N] \cdot \mathbb{E}[X]$ ist richtig. Da wurde die Linearität des Erwartungswertes benutzt.

Fazit:

$\mathbb{E}[]$ ist eine Funktion, die immer eine Zufallsvariable als Eingabeparameter erwartet und eine reelle Zahl als Ergebnis liefert!

Zusammenfassung: Wahrscheinlichkeitserzeugende Funktionen

- **Wahrscheinlichkeitserzeugende Funktionen**
  Für eine Zufallsvariable X mit $W_X \subseteq \mathbb{N}_0$ gilt:

$$G_X(s) := \mathbb{E}\left[s^X\right] \qquad \text{bzw.} \qquad G_X(s) = \sum_{k=0}^{\infty} f_X(k) \cdot s^k.$$

- **Beobachtungen**
  Für eine Zufallsvariable X mit $W_X \subseteq \mathbb{N}_0$ gilt:

s	$G_X(s)$	$G_X'(s)$	$G_X''(s)$	$G_X'''(s)$	$\ldots$	$G_X^{(n)}(s)$
0	$f_X(0)$	$f_X(1)$	$2f_X(2)$	$6f_X(3)$	$\ldots$	$n!f_X(n)$
1	1	$\mathbb{E}[X]$	$\mathbb{E}[X^{\underline{2}}]$	$\mathbb{E}[X^{\underline{3}}]$	$\ldots$	$\mathbb{E}[X^{\underline{n}}]$

Daraus folgt für die Varianz von X:

$$\mathrm{Var}[X] = G_X''(1) + G_X'(1) - G_X'(1)^2.$$

Zusammenfassung: Wahrscheinlichkeitserzeugende Funktionen

- **Eindeutigkeit wahrscheinlichkeitserzeugender Funktionen**
  Die Dichtefunktion f_X und die Verteilungsfunktion F_X einer Zufallsvariable mit $W_X \subseteq \mathbb{N}_0$ sind durch ihre wahrscheinlichkeitserzeugende Funktion eindeutig bestimmt.

- **Summen von Zufallsvariablen**
  Für unabhängige Zufallsvariablen $X_1, \ldots, X_n$ gilt:

$$G_{X_1+\ldots+X_n}(s) = G_{X_1}(s) \cdot \ldots \cdot G_{X_n}(s).$$

- **Zufällige Summen**
  Seien X und N zwei Zufallsvariablen, $X_1, X_2, X_3, \ldots$ unabhängige Ausführungen von X und $Z = X_1 + \ldots + X_N$. Dann gilt:

$$G_Z(s) = G_N(G_X(s)).$$

  Daraus folgt:

$$\mathbb{E}[Z] = \mathbb{E}[N] \cdot \mathbb{E}[X].$$

Tabelle: Formelsammlung für wichtige diskrete Verteilungen

Verteilung	W_X	$f_X(k)$	$F_X(k)$	$\mathbb{E}[X]$	$\mathrm{Var}[X]$	$G_X(s)$
$X \sim \mathrm{Uni}(a, b)$	$\{a, \dots, b\}$	$\frac{1}{b-a+1}$	$\frac{k-a+1}{b-a+1}$	$\frac{a+b}{2}$	$\frac{(b-a)(b-a+2)}{12}$	$\sum_{k=a}^{b} f_X(k)s^k$
$X \sim \mathrm{Ber}(p)$	$\{0, 1\}$	$p^k(1-p)^{1-k}$	$(1-p)^{1-k}$	p	$p(1-p)$	$1-p+ps$
$X \sim \mathrm{Bin}(n, p)$	$\{0, \dots, n\}$	$\binom{n}{k} p^k (1-p)^{n-k}$	$\sum_{i=0}^{k} f_X(i)$	np	$np(1-p)$	$(1-p+ps)^n$
$X \sim \mathrm{Poi}(\lambda)$	$\{0, \dots\}$	$\frac{e^{-\lambda}\lambda^k}{k!}$	$\sum_{i=0}^{k} f_X(i)$	λ	λ	$e^{\lambda(s-1)}$
$X \sim \mathrm{Geo}(p)$	$\{1, \dots\}$	$p(1-p)^{k-1}$	$1-(1-p)^k$	$\frac{1}{p}$	$\frac{1-p}{p^2}$	$\frac{ps}{1-(1-p)s}$
$X \sim \mathrm{NegBin}(n, p)$	$\{n, \dots\}$	$\binom{k-1}{n-1} p^n (1-p)^{k-n}$	$\sum_{i=n}^{k} f_X(i)$	$\frac{n}{p}$	$\frac{n(1-p)}{p^2}$	$\left(\frac{ps}{1-(1-p)s}\right)^n$
$X \sim \mathrm{Hyp}(n, a, b)$	$\{0, \dots, n\}$	$\frac{\binom{b}{k}\binom{a}{n-k}}{\binom{a+b}{n}}$	$\sum_{i=0}^{k} f_X(i)$	$\frac{bn}{a+b}$	$\frac{abn(a+b-n)}{(a+b-1)(a+b)^2}$	$\sum_{k=0}^{n} f_X(k)s^k$
$X \sim \mathrm{NegHyp}(n, a, b)$	$\{n, \dots, a+b\}$	$\frac{\binom{k-1}{n-1}\binom{a+b-k}{b-n}}{\binom{a+b}{b}}$	$\sum_{i=n}^{k} f_X(i)$	$\frac{n(a+b+1)}{b+1}$	$\frac{na(a+b+1)(b+1-n)}{(b+1)^2(b+2)}$	$\sum_{k=n}^{a+b} f_X(k)s^k$

Infos

- Die Formeln für f_X und F_X gelten nur für $k \in W_X$. Beispielsweise gilt für $X \sim \text{Ber}(p)$: $f_X(0) = 1 - p$, $f_X(1) = p$ und $f_X(k) = 0$ für alle $k \notin \{0, 1\}$.
- Für die Formeln in grau kennt man leider keine geschlossene Ausdrücke.
- Manchmal findet man für $X \sim \text{Uni}(a, b)$ die Formel

$$G_X(s) = \frac{s^a - s^{b+1}}{(b - a + 1)(1 - s)}.$$

Die sieht zwar schön aus, aber sie hat zwei große Macken:

1. Sie ist nur für $s \neq 1$ definiert und $s = 1$ ist, genauso wie $s = 0$, ein sehr wichtiger Wert für uns.
2. Man müsste die Quotientenregel benutzen, um sie anzuleiten.

Die Formel $G_X(s) = \sum_{k=a}^{b} f_X(k) s^k = \frac{s^a + \ldots + s^b}{b-a+1}$ ist viel schöner und einfacher!

Zu einer Zufallsvariable X mit $W_X \subseteq \mathbb{N}_0$ sei ihre wahrscheinlichkeitserzeugende Funktion $G_X(s)$ bekannt. Wie kann man die wahrscheinlichkeitserzeugende Funktion G_Y von $Y := 3X + 5$ mithilfe von G_X darstellen?

Hinweis: Benutze die Definition: $G_Y(s) = \mathbb{E}\left[s^Y\right]$.

$$G_Y(s) = \mathbb{E}\left[s^Y\right] = \mathbb{E}\left[s^{3X+5}\right] = \mathbb{E}\left[s^{3X} \cdot s^5\right] = \mathbb{E}\left[s^{3X}\right] \cdot s^5 = \mathbb{E}\left[(s^3)^X\right] \cdot s^5 = G_X(s^3) \cdot s^5.$$

Themenübersicht

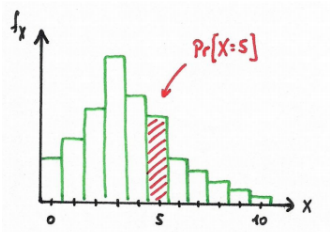
Themenübersicht

Stetige Zufallsvariablen

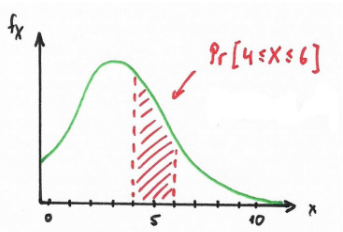
Ab jetzt werden wir unsere Wahrscheinlichkeitskeitsräume durch Zufallsvariablen definieren. Für jede Zufallsvariable wird meistens $W_X = \mathbb{R}$ gelten und:

$$\int_{-\infty}^{\infty} f_X(x)\,\mathrm{d}x = 1$$

Früher: Summe aller Balken war 1



Ab jetzt: Fläche unterhalb der Kurve ist 1



Infos

- Im Kontinuierlichen gilt zwar $F_X(x) = \Pr[X \leq x]$ aber es gibt keine Beziehung zwischen $f_X(x)$ und $\Pr[X = x]$! Für jedes $x \in \mathbb{R}$ gilt nämlich $\Pr[X = x] = 0$, was für $f_X(x)$ nicht unbedingt der Fall sein soll.
- f_X kann jetzt sogar größer als 1 sein. Wichtig ist, dass sie nicht negativ ist und dass das Integral, also die Fläche unter ihrem Graph, gleich 1 ist.
- Wahrscheinlichkeiten werden meistens die Form $\Pr[a \leq X \leq b]$ haben. Diese berechnet man durch einfaches Integrieren:

$$\Pr[a \leq X \leq b] = \int_a^b f_X(x)\,\mathrm{d}x.$$

- Im Kontinuierlichen gilt:

$$\Pr[a \leq X \leq b] = \Pr[a < X \leq b] = \Pr[a \leq X < b] = \Pr[a < X < b].$$

D.h. wir brauchen hier keine Tricks wie $\Pr[X > k] = \Pr[X \geq k + 1]$.

Erinnerung

Hier ist eine unwichtige Bemerkung, die meiner Meinung nach sehr interessant ist!

Wer bei Prof. Mayr DS gehört hat (also vemutlich keiner von euch), erinnert sich bestimmt an folgende Definition aus dem Abschnitt *Diskrete Analysis*:

$$\nabla f(n) = f(n) - f(n-1).$$

Wir lernten damals folgende Begriffe kennen:

- $\nabla f(n)$ wurde eine der zwei möglichen *diskreten Ableitungen* von $f(n)$ genannt.
- Jede Funktion $F(n)$ mit $\nabla F(n) = f(n)$, insbesondere auch $F(n) = \sum_{k=0}^{n} f(k)$, wird eine *diskrete Stammfunktion* von $f(n)$ genannt.

Für eine diskrete Zufallsvariable X mit $W_X \subseteq \mathbb{N}_0$ gilt:

$$F_X(x) = \sum_{k=0}^{x} f_X(k) \quad \text{und} \quad f_X(x) = F_X(x) - F_X(x-1).$$

Somit ist F_X eine diskrete Stammfunktion von f_X und f_X eine diskrete Ableitung von F_X.

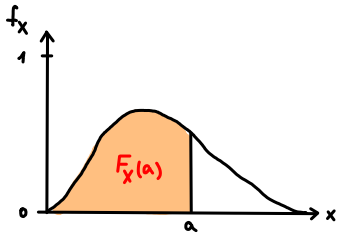
Dichte und Verteilung

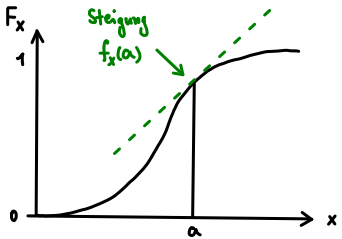
Für eine stetige Zufallsvariable X gilt:

$$F_X(x) = \int_{-\infty}^{x} f_X(u)\,\mathrm{d}u \qquad \text{und} \qquad f_X(x) = F_X'(x)$$

mit F_X' wieder als Abkürzung für die Ableitung $\frac{\mathrm{d}F_X}{\mathrm{d}x}$. Das heißt:

1. Der Wert von $F_X(a)$ ist also die Fläche unterhalb von $f_X(x)$ zwischen $-\infty$ und a.
2. $f_X(a)$ ist die Steigung von $F_X(x)$ an der Stelle a.





Infos

- Üblicherweise bestimmt man zuerst $F_X(x) = \Pr[X \leq x]$ und berechnet danach (durch ableiten) $f(x)$.
- Für stetige Zufallsvariablen gilt immer:

$$\lim_{x \to -\infty} f_X(x) = 0, \quad \lim_{x \to \infty} f_X(x) = 0, \quad \lim_{x \to -\infty} F_X(x) = 0 \quad \text{und} \quad \lim_{x \to \infty} F_X(x) = 1.$$

- F_X ist immer monoton steigend und stetig, f_X kann auch unstetig sein.
- Wegen

$$\int_{-\infty}^{\infty} f_X(x)\,\mathrm{d}x = \lim_{x \to \infty} \int_{-\infty}^{x} f_X(u)\,\mathrm{d}u = \lim_{x \to \infty} F_X(x)$$

gilt für jede stetige Zufallsvariable $\lim_{x \to \infty} F_X(x) = 1$.

- Weil F_X eine Stammfunktion von f_X ist, wird immer gelten:

$$\Pr[a \leq X \leq b] = F_X(b) - F_X(a).$$

Gemeinsame Dichte

Was eine gemeinsame Dichte $f_{X,Y}$ ist und in welcher Beziehung sie zu den Randdichten f_X und f_Y steht, funktioniert in kontinuierlichen Wahrscheinlichkeitsräumen analog zu den diskreten. Es gilt

$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{X,Y}(x,y) \, \mathrm{d}x \, \mathrm{d}y = 1$$

und:

$$f_X(x) = \sum_{y \in W_Y} f_{X,Y}(x,y) \qquad \rightsquigarrow \qquad f_X(x) = \int_{-\infty}^{\infty} f_{X,Y}(x,y) \, \mathrm{d}y,$$

$$f_Y(y) = \sum_{x \in W_X} f_{X,Y}(x,y) \qquad \rightsquigarrow \qquad f_Y(y) = \int_{-\infty}^{\infty} f_{X,Y}(x,y) \, \mathrm{d}x.$$

Die Formeln für die Randdichten von diskreten Zufallsvariablen müssen also nur auf stetige Zufallsvariablen „angepasst“ werden.

Gemeinsame Verteilung

- Analog zu diskreten Zufallsvariablen gilt für die gemeinsame Verteilung $F_{X,Y}$:

$$F_{X,Y}(x,y) = \Pr[X \leq x, Y \leq y].$$

- Zwischen $f_{X,Y}$ und $F_{X,Y}$ besteht folgende Beziehung:

$$F_{X,Y}(x,y) = \int_{-\infty}^{y} \int_{-\infty}^{x} f_{X,Y}(u,v)\, \mathrm{d}u\, \mathrm{d}v \quad \text{und} \quad f_{X,Y}(x,y) = \frac{\mathrm{d}}{\mathrm{d}y} \frac{\mathrm{d}}{\mathrm{d}x} F_{X,Y}(x,y).$$

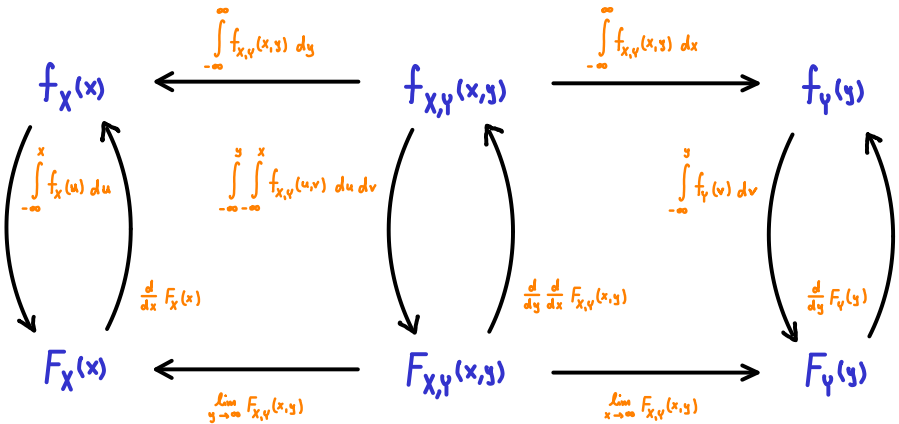
- Daraus folgt für die Randverteilungen F_X und F_Y:

$$F_X(x) = \lim_{y \to \infty} F_{X,Y}(x,y) \qquad \text{und} \qquad F_Y(y) = \lim_{x \to \infty} F_{X,Y}(x,y).$$

Info

Analog zu dem Fall mit nur einer Zufallsvariable, kommt man im Kontinuierlichen am einfachsten über die gemeinsame Verteilung $F_{X,Y}$ auf die gemeinsame Dichte $f_{X,Y}$.

Übersicht: $f_{X,Y}$, f_X, f_Y, $F_{X,Y}$, F_X und F_Y



Nicht vergessen!

- Damit $f_{X,Y}$ zulässig ist, muss $f_{X,Y}(x,y) \geq 0$ für alle $x, y \in \mathbb{R}$ gelten und:

$$\int_{-\infty}^{\infty} \underbrace{\int_{-\infty}^{\infty} f_{X,Y}(x,y)\,\mathrm{d}x}_{f_Y(y)}\,\mathrm{d}y = 1 \qquad \text{bzw.} \qquad \int_{-\infty}^{\infty} \underbrace{\int_{-\infty}^{\infty} f_{X,Y}(x,y)\,\mathrm{d}y}_{f_X(x)}\,\mathrm{d}x = 1.$$

- Die Reihenfolge der Variablen, nach denen man integriert, ist egal. Wer das wieder auffrischen will:

`de.wikipedia.org/wiki/Satz_von_Fubini`

- X und Y sind genau dann unabhängig wenn für alle $x, y \in \mathbb{R}$ gilt:

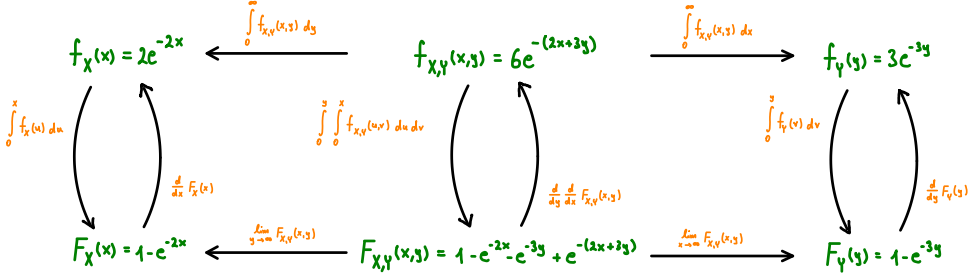
$$f_{X,Y}(x,y) = f_X(x) \cdot f_Y(y) \qquad \text{bzw.} \qquad F_{X,Y}(x,y) = F_X(x) \cdot F_Y(y).$$

Beispiel

Seien X und Y stetige Zufallsvariablen mit gemeinsamer Dichte

$$f_{X,Y}(x,y) = \begin{cases} 6e^{-(2x+3y)} & \text{falls } x, y \geq 0 \\ 0 & \text{sonst} \end{cases}$$

Für $x, y \geq 0$ erhalten wir:



Übungsaufgabe

Sei $f_{X,Y}$ gegeben durch:

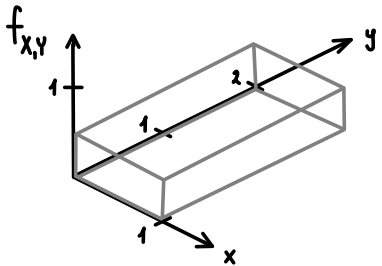
$$f_{X,Y}(x,y) = \begin{cases} \frac{1}{2} & \text{falls } 0 \leq x \leq 1 \text{ und } 0 \leq y \leq 2 \\ 0 & \text{sonst} \end{cases}$$

Überprüfe anhand einer Zeichnung, dass $f_{X,Y}$ wohldefiniert ist und bestimme dann f_X, f_Y, $F_{X,Y}$, F_X und F_Y für $0 \leq x \leq 1$ und $0 \leq y \leq 2$.

Intuitiv beschreibt $f_{X,Y}$ das zufällige Wählen eines Punktes aus dem rechteckförmigen Bereich

$$B = \left\{(x, y) \in \mathbb{R}^2 \,\middle|\, 0 \leq x \leq 1 \text{ und } 0 \leq y \leq 2\right\}.$$

Der Graph von $f_{X,Y}$ ist konstant $\frac{1}{2}$ über B und 0 sonst. Es ergibt sich der folgende Quader:

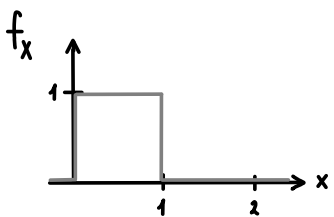


Das Volumen unter dem Graph ist $1 \cdot 2 \cdot \frac{1}{2} = 1$. Somit ist $f_{X,Y}$ wohldefiniert.

Für $0 \leq x \leq 1$ gilt:

$$f_X(x) = \int_{-\infty}^{\infty} f_{X,Y}(x,y)\ \mathrm{d}y = \int_0^2 \frac{1}{2}\ \mathrm{d}y = 1.$$

Graphisch:

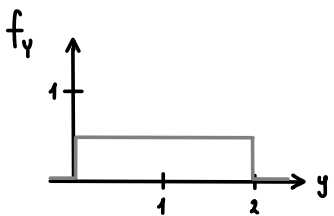


Info: Die Fläche unter dem Graph ist (wie erwartet) $1 \cdot 1 = 1$.

Für $0 \leq y \leq 2$ gilt:

$$f_Y(y) = \int_{-\infty}^{\infty} f_{X,Y}(x,y)\,\mathrm{d}x = \int_0^1 \frac{1}{2}\,\mathrm{d}x = \frac{1}{2}.$$

Graphisch:

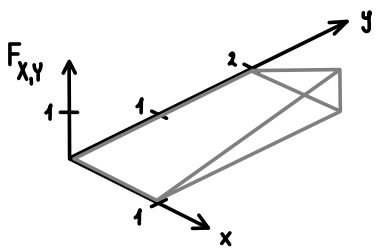


Info: Die Fläche unter dem Graph ist (wie erwartet) $2 \cdot \frac{1}{2} = 1$.

Für $0 \leq x \leq 1$ und $0 \leq y \leq 2$ gilt:

$$F_{X,Y}(x,y) = \int_{-\infty}^{y} \int_{-\infty}^{x} f_{X,Y}(u,v)\,\mathrm{d}u\,\mathrm{d}v = \int_{0}^{y} \int_{0}^{x} \frac{1}{2}\,\mathrm{d}u\,\mathrm{d}v = \int_{0}^{y} \frac{x}{2}\,\mathrm{d}v = \frac{xy}{2}.$$

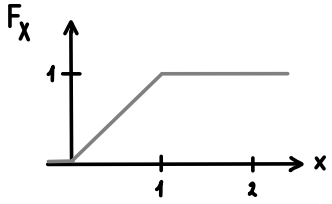
Graphisch:



Für $0 \leq x \leq 1$ gilt:

$$F_X(x) = \int_{-\infty}^{x} f_X(u)\,\mathrm{d}u = \int_{0}^{x} 1\,\mathrm{d}u = x.$$

Graphisch:



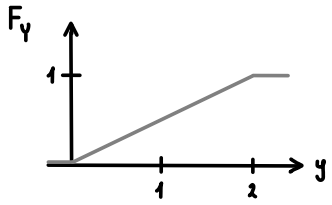
Alternativ:

$$F_X(x) = \lim_{y\to\infty} F_{X,Y}(x,y) = F_{X,Y}(x,2) = \frac{x\cdot 2}{2} = x.$$

Für $0 \leq y \leq 2$ gilt:

$$F_Y(y) = \int_{-\infty}^{y} f_X(v)\,\mathrm{d}v = \int_0^y \frac{1}{2}\,\mathrm{d}v = \frac{y}{2}.$$

Graphisch:

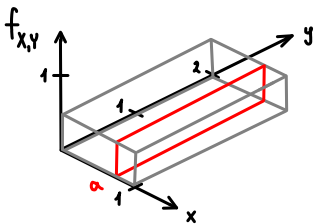


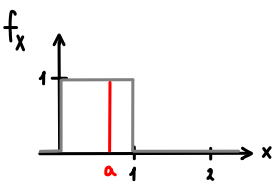
Alternativ:

$$F_Y(y) = \lim_{x\to\infty} F_{X,Y}(x,y) = F_{X,Y}(1,y) = \frac{1\cdot y}{2} = \frac{y}{2}.$$

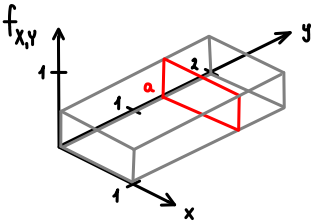
In diesem Beispiel kann man die graphische Bedeutung der Randdichten sehr schön erkennen.

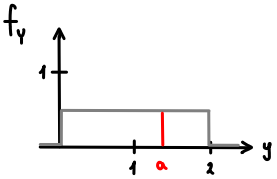
$f_X(a)$ gibt die Schnittfläche der Kurve von $f_{X,Y}(x, y)$ an der Stelle $x = a$ an:





Analog dazu gibt $f_Y(a)$ die Schnittfläche der Kurve von $f_{X,Y}(x, y)$ an der Stelle $y = a$ an:





Rechenregeln recyclen

So wie die Formeln der Randdichten können wir im Kontinuierlichen alle Rechenregeln, die wir im Diskreten kennengelernt haben, entweder genau so oder mit kleinen Veränderungen verwenden.

Es müssen diejenigen Rechenregeln angepasst werden, bei denen über alle Werte im Wertebereich einer Zufallsvariable summiert wird. Bei ihnen ersetzen wir „$\sum_{x \in W_x} \ldots$“ durch „$\int_{-\infty}^{\infty} \ldots \mathrm{d}x$“.

Auf den nächsten Folien sind alle Anpassungen aufgelistet. Die müsst ihr euch nicht extra aufschreiben, denn sie wurden alle nach demselben Schema angepasst. Es reicht sich das Schema zu merken!

Zusammenfassung: Angepasste Rechenregeln

Folgende Rechenregeln für diskrete Zufallsvariablen müssen auf stetige Zufallsvariablen angepasst werden:

$$\mathbb{E}[X] = \sum_{x \in W_X} x \cdot f_X(x) \quad \rightsquigarrow \quad \mathbb{E}[X] = \int_{-\infty}^{\infty} x \cdot f_X(x)\, \mathrm{d}x,$$

$$\mathbb{E}[X|B] = \sum_{x \in W_X} x \cdot f_{X|B}(x) \quad \rightsquigarrow \quad \mathbb{E}[X|B] = \int_{-\infty}^{\infty} x \cdot f_{X|B}(x)\, \mathrm{d}x,$$

$$\mathbb{E}[g(X)] = \sum_{x \in W_X} g(x) \cdot f_X(x) \quad \rightsquigarrow \quad \mathbb{E}[g(X)] = \int_{-\infty}^{\infty} g(x) \cdot f_X(x)\, \mathrm{d}x,$$

$$\mathrm{Var}[X] = \sum_{x \in W_X} (x - \mathbb{E}[X])^2 \cdot f_X(x) \quad \rightsquigarrow \quad \mathrm{Var}[X] = \int_{-\infty}^{\infty} (x - \mathbb{E}[X])^2 \cdot f_X(x)\, \mathrm{d}x,$$

Zusammenfassung: Angepasste Rechenregeln

$$f_X(x) = \sum_{y \in W_Y} f_{X,Y}(x,y) \qquad \rightsquigarrow \qquad f_X(x) = \int_{-\infty}^{\infty} f_{X,Y}(x,y)\,\mathrm{d}y,$$

$$f_Y(y) = \sum_{x \in W_X} f_{X,Y}(x,y) \qquad \rightsquigarrow \qquad f_Y(y) = \int_{-\infty}^{\infty} f_{X,Y}(x,y)\,\mathrm{d}x,$$

$$f_{X+Y}(x) = \sum_{k \in W_x} f_X(k) \cdot f_Y(x-k) \qquad \rightsquigarrow \qquad f_{X+Y}(x) = \int_{-\infty}^{\infty} f_X(u) \cdot f_Y(x-u)\,\mathrm{d}u,$$

$$f_{X-Y}(x) = \sum_{k \in W_x} f_X(k) \cdot f_Y(k-x) \qquad \rightsquigarrow \qquad f_{X-Y}(x) = \int_{-\infty}^{\infty} f_X(u) \cdot f_Y(u-x)\,\mathrm{d}u.$$

Dies sind, meiner bescheidenen Meinung nach, alle Regeln die angepasst werden müssen. Falls ihr die Vermutung habt, dass ich welche vergessen habe, dann meldet euch bitte!

Info

Aus Folie 1998 wissen wir, dass für unabhängige Zufallsvariablen X und N und unabhängige Ausführungen $X_1, X_2, X_3, \ldots$ von X gilt:

$$Z = X_1 + \ldots + X_N \qquad \Longrightarrow \qquad \mathbb{E}[Z] = \mathbb{E}[N] \cdot \mathbb{E}[X].$$

Diese Regel wurde in der Zentralübung zwar mithilfe wahrscheinlichkeitserzeugender Funktionen bewiesen (s. Folie 1999), das heißt aber nicht, dass die Existenz einer wahrscheinlichkeitserzeugenden Funktion eine notwendige Voraussetzung dafür ist.

Mann kann diese Aussage auch wie folgt beweisen:

Für $Z = X_1 + \ldots + X_N$ gilt:

$$\begin{aligned}
\mathbb{E}[Z] &= \sum_{n \in W_N} \mathbb{E}[Z|N=n] \cdot \Pr[N=n] \\
&= \sum_{n \in W_N} \underbrace{\mathbb{E}[X_1 + \ldots + X_N | N=n]}_{\mathbb{E}[X_1|N=n] + \ldots + \mathbb{E}[X_N|N=n]} \cdot \Pr[N=n] \\
&= \sum_{n \in W_N} n \cdot \underbrace{\mathbb{E}[X|N=n]}_{\mathbb{E}[X], \text{ da unabh.}} \cdot \Pr[N=n] \\
&= \mathbb{E}[X] \cdot \underbrace{\sum_{n \in W_N} n \cdot \Pr[N=n]}_{\mathbb{E}[N]}
\end{aligned}$$

D.h., diese Regel gilt für beliebige Zufallsvariablen. X darf sogar stetig sein!

Themenübersicht

Gleichverteilung

Eine gleichverteilte Zufallsvariable $X \sim \text{Uni}(a, b)$ gibt eine natürliche Zahl aus dem Intervall $[a, b]$ aus. Dabei sind alle Zahlen gleich wahrscheinlich.

Der Wertebereich von X ist $W_X = [a, b]$ und es gilt:

$$f_X(x) = \begin{cases} \frac{1}{b-a}, & \text{falls } x \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info

Je nach Anwendung kann a oder b vom Wertebereich von X ausgeschlossen werden. Das ändert jedoch nichts an den Formeln!

Exponentialverteilung

Eine exponentialverteilte Zufallsvariable $X \sim \text{Exp}(\lambda)$ stellt die Wartezeit bis zum ersten Auftreten eines Ereignisses („Erfolg“), wobei

$$\lambda = \frac{\text{Durchschnittliche Anzahl an Erfolgen in einem Zeitintervall}}{\text{Länge des Zeitintervalls}}$$

die Erfolgsrate ist. Die Exponentialverteilung ist das kontinuierliche Analogon zur geometrischen Verteilung.

Der Wertebereich von X ist $W_X = \mathbb{R}_0^+$ und es gilt:

$$f_X(x) = \begin{cases} \lambda \cdot e^{-\lambda x}, & \text{falls } x \in W_X \\ 0 & \text{sonst} \end{cases}$$

Infos

- Die Exponentialverteilung hat, wie die geometrische Verteilung, die tolle Eigenschaft gedächtnislos zu sein. D.h. sie „vergisst“ nach jeder Runde wie viele Misserfolge sie bis dahin schon hatte. Für $X \sim \text{Exp}(\lambda)$ und alle $x, y \in W_X$ gilt nämlich:

$$\Pr[X > x + y \mid X > x] = \Pr[X > y].$$

  Erinnerung: „$>$“ und „$\geq$“ machen im Kontinuierlichen keinen Unterschied!

- Die Summe $X_1 + \ldots + X_n$ von unabhängigen Zufallsvariablen $X_1, \ldots, X_n \sim \text{Exp}(\lambda)$ ist Erlang-verteilt. Man schreibt:

$$X_1 + \ldots + X_n \sim \text{Erl}(n, \lambda).$$

Sehr wichtig!

Die Erlang-Verteilung wird üblicherweise nicht in der Vorlesung behandelt, aber sie kann in Tutor- oder Hausaufgaben vorkommen. Hilfreiche Formeln dazu sind auf den Folien 2044 und 2047. Bevor ihr sie benutzt, vergewissert euch bitte zuerst, dass ihr das dürft.

Normalverteilung

Eine normalverteilte Zufallsvariable $X \sim \mathcal{N}(\mu, \sigma^2)$ besitzt approximativ dieselbe Verteilung wie die Summe von vielen unabhängigen, beliebig (aber identisch) verteilten Zufallsvariablen.

Der Wertebereich von X ist $W_X = \mathbb{R}$ und es gilt:

$$f_X(x) = \begin{cases} \frac{1}{\sqrt{2\pi}\sigma} \cdot e^{-\frac{(x-\mu)^2}{2\sigma^2}}, & \text{falls } x \in W_X \\ 0 & \text{sonst} \end{cases}$$

Info

Für $X_1, \ldots, X_n$ unabhängig und identisch verteilt, $Y_n = X_1 + \ldots + X_n$ und großes n gilt approximativ:

$$Y_n \sim \mathcal{N}(\mathbb{E}[Y_n], \mathrm{Var}[Y_n]).$$

Dass man Summen unabhängiger Zufallsvariablen durch die Normalverteilung approximieren kann, ist die Aussage des Zentralen Grenzwertsatzes.

Für die Verteilungsfunktion F_X einer normalverteilten Zufallsvariable X gibt es leider keine geschlossene Formel, da f_X nicht geschlossen integrierbar ist.

Tabelle: Formelsammlung für wichtige stetige Verteilungen

Verteilung	W_X	$f_X(x)$	$F_X(x)$	$\mathbb{E}[X]$	$\mathrm{Var}[X]$
$X \sim \mathrm{Uni}(a,b)$	$[a,b]$	$\frac{1}{b-a}$	$\frac{x-a}{b-a}$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$
$X \sim \mathrm{Exp}(\lambda)$	$[0,\infty)$	$\lambda e^{-\lambda x}$	$1-e^{-\lambda x}$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$
$X \sim \mathrm{Erl}(n,\lambda)$	$[0,\infty)$	$\frac{\lambda^n x^{n-1}}{(n-1)!}e^{-\lambda x}$	$1-\left(\sum_{k=0}^{n-1}\frac{(\lambda x)^k}{k!}\right)e^{-\lambda x}$	$\frac{n}{\lambda}$	$\frac{n}{\lambda^2}$
$X \sim \mathcal{N}(\mu,\sigma^2)$	$(-\infty,\infty)$	$\frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$	$\int_{-\infty}^{x} f_X(u)\,\mathrm{d}u$	μ	σ^2

Für die vollständige Tabelle mit momenterzeugenden Funktionen siehe Folie 2091.

Infos

- Die Formeln für f_X und F_X gelten nur für $x \in W_X$.
- Für die Verteilungsfunktion der Normalverteilung gibt es leider keine geschlossene Formel.
- Je nach Situation kann man bei der Gleichverteilung a oder b ausschließen. Man bekommt dann für W_X entweder $(a, b]$, $[a, b)$ oder (a, b). Die Formeln bleiben aber, wie gesagt, alle gleich!
- Für $x \notin W_X$ gilt immer $f_X(x) = 0$. Ist x kleiner als alle Werte in W_X, dann ist $F_X(x) = 0$. Ist x, dagegen, größer als alle Werte in W_X, dann ist $F_X(x) = 1$.

Rechenregeln

1. Gedächtnislosigkeit der Exponentialverteilung.
   Eine Zufallsvariable X ist genau dann exponentialverteilt, wenn $W_X = \mathbb{R}_0^+$ gilt und sie gedächtnislos ist, d.h. wenn für alle $x, y \in W_X$ gilt:

$$\Pr[X > x + y \mid X > x] = \Pr[X > y].$$

2. Poisson-Prozess.
   Falls $T_1, T_2, T_3, \ldots \sim \text{Exp}(\lambda)$ unabhängig und

$$X(t) := \max\{n \in \mathbb{N}_0 \mid T_1 + \ldots + T_n \leq t\}$$

   für jedes $t > 0$. Dann gilt:

$$X(t) \sim \text{Poi}(t\lambda).$$

Rechenregeln

3. Für zusammengesetzte Zufallsvariablen gilt:

$$
\begin{aligned}
X \sim \mathrm{Uni}(a,b) &\quad\Longrightarrow\quad rX+s \sim \mathrm{Uni}(ra+s, rb+s) && (r,s \in \mathbb{R}, r \neq 0)\\
X \sim \mathrm{Exp}(\lambda) &\quad\Longrightarrow\quad aX \sim \mathrm{Exp}\left(\frac{\lambda}{a}\right) && (a \in \mathbb{R}, a > 0)\\
X \sim \mathcal{N}(\mu,\sigma^2) &\quad\Longrightarrow\quad aX+b \sim \mathcal{N}(a\mu+b, a^2\sigma^2) && (a,b \in \mathbb{R}, a \neq 0)
\end{aligned}
$$

4. Für aus mehreren unabhängigen Zufallsvariablen $X_1, \ldots, X_k$ zusammengesetzte Zufallsvariablen gilt:

$$
\begin{aligned}
X_i \sim \mathcal{N}(\mu_i,\sigma_i^2) &\quad\Longrightarrow\quad X_1+\ldots+X_k \sim \mathcal{N}(\mu_1+\ldots+\mu_k, \sigma_1^2+\ldots+\sigma_k^2)\\
X_i \sim \mathrm{Exp}(\lambda_i) &\quad\Longrightarrow\quad \min\{X_1,\ldots,X_k\} \sim \mathrm{Exp}(\lambda_1+\ldots+\lambda_k)\\
X_i \sim \mathrm{Exp}(\lambda) &\quad\Longrightarrow\quad X_1+\ldots+X_k \sim \mathrm{Erl}(k,\lambda)
\end{aligned}
$$

Themenübersicht

Simulation von Zufallsvariablen

Gegeben seien eine auf $[0, 1]$ gleichverteilte, stetige Zufallsvariable U und eine beliebige stetige Zufallsvariable X mit streng monoton wachsender Verteilungsfunktion F_X. Dann besitzt F_X eine eindeutige Umkehrfunktion F_X^{-1} und für $Y = F_X^{-1}(U)$ und alle $x \in \mathbb{R}$ gilt:

$$F_Y(x) = F_X(x).$$

D.h. Y und X sind identisch verteilt.

- F_X muss streng monoton steigend sein damit eine Umkehrfunktion überhaupt existiert.
- Weil F_X nur Werte in $[0, 1]$ annehmen kann, kann F_X^{-1} auch nur für Werte in $[0, 1]$ definiert sein. Deswegen muss der Wertebereich von U in $[0, 1]$ sein.
- Der Beweis von $F_Y(x) = F_X(x)$ für $U \sim \text{Uni}(0, 1)$ und $Y = F_X^{-1}(U)$ ist ganz einfach. Es gilt nämlich:

$$F_Y(x) = \Pr[Y \leq x] = \Pr\left[F_X^{-1}(U) \leq x\right] = \Pr[U \leq F_X(x)] = F_U(F_X(x)) = F_X(x).$$

Beispiel

Wir wollen eine Java-Methode `exp(double lambda)` implementieren, welche das Ergebnis einer exponentialverteilten Zufallsvariable $X \sim \text{Exp}(\lambda)$ simuliert. Zur Verfügung haben wir die Methode `Math.random()`, welche eine auf $[0, 1)$ gleichverteilte reelle Zahl ausgibt.

Seien also $U \sim \text{Uni}(0, 1)$, $X \sim \text{Exp}(\lambda)$ zwei stetige Zufallsvariablen. Für X gilt $F_X(x) = 1 - e^{-\lambda x}$. Wir rechnen:

$$\begin{aligned} y = 1 - e^{-\lambda x} &\iff y + e^{-\lambda x} = 1 \\ &\iff e^{-\lambda x} = 1 - y \\ &\iff -\lambda x = \ln(1 - y) \\ &\iff x = -\frac{\ln(1 - y)}{\lambda} \end{aligned}$$

Die Umkehrfunktion von F_X ist also $F_X^{-1}(y) = -\frac{\ln(1-y)}{\lambda}$.

Beispiel

Somit sind X und Y mit $Y = F_X^{-1}(U) = -\frac{\ln(1-U)}{\lambda}$ identisch verteilt und die Methode `exp(double lambda)` kann wie folgt implementiert werden:

```
double exp(double lambda) {
   return -Math.log(1-Math.random())/lambda;
}
```

Eine Zufallsvariable X nennt man *dreiecksverteilt* mit Parametern $a, b, c \in \mathbb{R}$ $(0 \leq a \leq b \leq c)$, falls sie folgende Dichtefunktion besitzt:

$$f_X(x) = \begin{cases} \frac{2(x-a)}{(c-a)(b-a)}, & \text{falls } a \leq x \leq b \\ \frac{2(c-x)}{(c-a)(c-b)}, & \text{falls } b < x \leq c \\ 0 & \text{sonst} \end{cases}$$

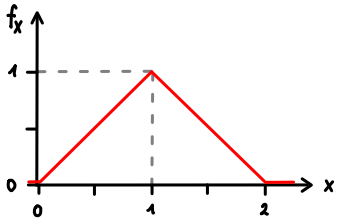
Für diese Aufgabe seien $a = 0$, $b = 1$ und $c = 2$ fest, d.h.

$$f_X(x) = \begin{cases} x & \text{falls } 0 \leq x \leq 1 \\ 2 - x & \text{falls } 1 < x \leq 2 \\ 0 & \text{sonst} \end{cases}$$

Übungsaufgabe

1. Zeichne den Graph von f_X und begründe anhand der Zeichnung, wieso f_X eine gültige Dichtefunktion ist.
2. Berechne die Verteilungsfunktion F_X von X. Beachte, dass $F_X(x)$ für alle $x \in \mathbb{R}$ definiert sein soll.
3. Definiere eine Funktion $g : [0, 1] \to [0, 2]$, so dass $g(U)$ und X für $U \sim \text{Uni}(0, 1)$ identisch verteilt sind und implementiere sie als Java-Methode `dreieck()`.
4. Seien $X_1, X_2 \sim \text{Uni}(0, 1)$ zwei unabhängige, gleichverteilte Zufallsvariablen. Zeige, dass X und $X_1 + X_2$ identisch verteilt sind. Was heißt das für unsere Methode `dreieck()`?

1. Zeichnung:



Man erkennt an dem Bild, dass die Funktion ein Dreieck mit Grundseite 2 und Höhe 1 beschreibt. Somit ist die Fläche unterhalb von f_X genau 1. Alternativ rechnet man:

$$\int_0^2 f_X(x)\,\mathrm{d}x = \int_0^1 x\,\mathrm{d}x + \int_1^2 2 - x\,\mathrm{d}x = 1.$$

2. Für $0 \leq x \leq 1$ gilt:

$$F_X(x) = \int_{-\infty}^{x} f_X(u)\,\mathrm{d}u = \int_0^x u\,\mathrm{d}u = \left[\frac{u^2}{2}\right]_{u=0}^{x} = \frac{x^2}{2}$$

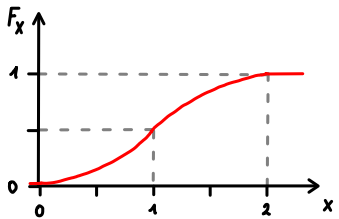
Für $1 < x \leq 2$ gilt:

$$\begin{aligned} F_X(x) &= \int_{-\infty}^{x} f_X(u)\,\mathrm{d}u = \int_0^1 f_X(u)\,\mathrm{d}u + \int_1^x f_X(u)\,\mathrm{d}u = \frac{1}{2} + \int_1^x 2 - x\,\mathrm{d}u \\ &= \frac{1}{2} + \left[2u - \frac{u^2}{2}\right]_{u=1}^{x} = \frac{1}{2} + \left(\left(2x - \frac{x^2}{2}\right) - \left(2 - \frac{1}{2}\right)\right) \\ &= \frac{1}{2} + 2x - \frac{x^2}{2} - \frac{3}{2} = 1 - \frac{(2-x)^2}{2} \end{aligned}$$

Daraus folgt für F_X:

$$F_X(x) = \begin{cases} 0 & \text{falls } x < 0 \\ \frac{x^2}{2}, & \text{falls } 0 \leq x \leq 1 \\ 1 - \frac{(2-x)^2}{2} & \text{falls } 1 < x \leq 2 \\ 1 & \text{falls } 2 < x \end{cases}$$

Graphisch:



3. Als nächstes bestimmen wir die Umkehrfunktion von F_X. Sei hierfür $y := F_X(x)$. An dem Graph von F_X erkennen wir:

$$0 \leq x \leq 1 \iff 0 \leq y \leq \frac{1}{2} \qquad \text{und} \qquad 1 < x \leq 2 \iff \frac{1}{2} < y \leq 1.$$

Für $0 \leq x \leq 1$ bzw. $0 \leq y \leq \frac{1}{2}$ gilt:

$$y = \frac{x^2}{2} \iff x^2 = 2y \iff x = \sqrt{2y}.$$

Für $m < x \leq 1$ bzw. $m < y \leq 1$ gilt:

$$y = 1 - \frac{(2-x)^2}{2} \iff (2-x)^2 = 2(1-y) \iff x = 1 - \sqrt{2(1-y)}$$

Daraus folgt, dass $g(U)$ mit

$$g(y) = \begin{cases} \sqrt{2y} & \text{falls } 0 \leq y \leq \frac{1}{2} \\ 1 - \sqrt{2(1-y)} & \text{falls } \frac{1}{2} < y \leq 1 \end{cases}$$

identisch verteilt zu X ist. D.h., dass X, analog zum Beispiel auf Folie 2051, durch folgende Java-Methode simuliert werden kann:

```
double dreieck() {
   double y = Math.random();
   if (y <= 0.5)
      return Math.sqrt(2*y);
   else
      return 1-Math.sqrt(2*(1-y));
}
```

4. Für unabhängige, gleichverteilte Zufallsvariablen $X_1, X_2 \sim \text{Uni}(0,1)$ berechnen wir $f_{X_1+X_2}$ nach Folie 2032. Für $0 \leq x \leq 1$ gilt:

$$f_{X_1+X_2}(x) = \int_{-\infty}^{\infty} f_{X_1}(u) \cdot f_{X_2}(x-u)\,\mathrm{d}u \overset{(1)}{=} \int_0^x 1 \cdot 1\,\mathrm{d}u = [u]_{u=0}^{x} = x$$

An der Stelle (1) gilt die Überlegung, dass $f_{X_1}(u)$ und $f_{X_2}(x-u)$ nur für $0 \leq u \leq x$ beide 1 sind und sonst 0. Für $1 < x \leq 2$ gilt analog:

$$f_{X_1+X_2}(x) = \int_{-\infty}^{\infty} f_{X_1}(u) \cdot f_{X_2}(x-u)\,\mathrm{d}u \overset{(2)}{=} \int_{x-1}^{1} 1 \cdot 1\,\mathrm{d}u = [u]_{u=x-1}^{1} = 2 - x$$

An der Stelle (2) gilt die Überlegung, dass $f_{X_1}(u)$ und $f_{X_2}(x-u)$ nur für $x-1 \leq u \leq 1$ beide 1 sind und sonst 0. Daraus ergibt sich:

$$f_{X_1,X_2}(x) = \begin{cases} x & \text{falls } 0 \leq x \leq 1 \\ 2-x & \text{falls } 1 < x \leq 2 \\ 0 & \text{sonst} \end{cases}.$$

Also sind X und $X_1 + X_2$ identisch verteilt.

Wir könnten also unsere Java-Methode `dreieck()` auch wie folgt implementieren:

```
double dreieck() {
   return Math.random() + Math.random();
}
```

Cool, oder?

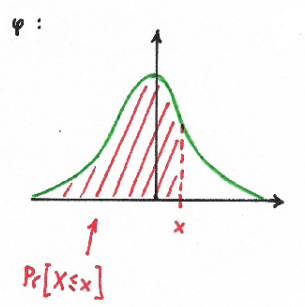
Themenübersicht

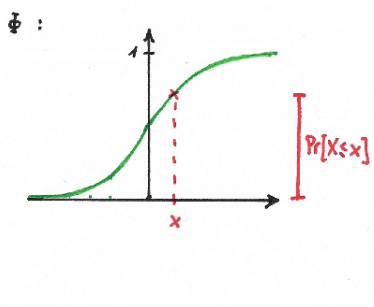
Standardnormalverteilung

Eine normalverteilte Zufallsvariable $X \sim \mathcal{N}(\mu, \sigma^2)$ mit $\mu = 0$ und $\sigma^2 = 1$ heißt standardnormalverteilt. Für sie gilt:

$$\varphi(x) = \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{x^2}{2}}, \qquad \Phi(x) = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{x} e^{-\frac{t^2}{2}} \, \mathrm{d}t.$$

Graphisch:





Infos

Folgendes sollte man für $X \sim \mathcal{N}(0,1)$ wissen.

- Weil diese Verteilung so wichtig ist, haben die Dichte- und die Verteilungsfunktion spezielle Namen. Wir definieren: $\varphi(x) := f_X(x)$ (klein-Phi) und $\Phi(x) := F_X(x)$ (groß-Phi).
- An der Formel für die Dichtefunktion erkennt man, dass $\varphi(-x) = \varphi(x)$ gilt. D.h. $\varphi(x)$ ist achsensymmetrisch zu $x = 0$ ist. Es gilt also $\Pr[X \geq x] = \Pr[X \leq -x]$ für alle $x \in \mathbb{R}$ und somit $\Phi(-x) = 1 - \Phi(x)$.

Der Zentrale Grenzwertsatz

Seien X eine beliebige Zufallsvariable, $X_1, \ldots, X_n$ unabhängige Ausführungen von X, $Y = X_1 + \ldots + X_n$ und

$$Z := \frac{Y - \mathbb{E}[Y]}{\sqrt{\mathrm{Var}[Y]}}.$$

Dann konvergiert die Verteilung von Z gegen die Standardnormalverteilung, d.h. es gilt approximativ $Z \sim \mathcal{N}(0, 1)$.

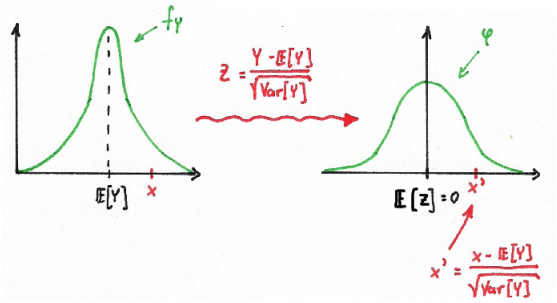
- Der Grenzwertsatz von de Moivre aus der Vorlesung ist nur ein Spezialfall vom Zentralen Grenzwertsatz für $X_i \sim \text{Ber}(p)$, also $Y \sim \text{Bin}(n, p)$.
- Oft wird auch
$$Z := \frac{Y - \mu_Y}{\sigma_Y} \qquad \text{bzw.} \qquad Z := \frac{Y - n\mu_X}{\sqrt{n}\sigma_X}$$
geschrieben, wobei μ_X, σ_X, μ_Y und σ_Y entsprechend den Erwartungswert und die Standardabweichung von X und Y bezeichnen:
$$\mu_Y := \mathbb{E}[Y], \qquad \sigma_Y := \sqrt{\text{Var}[Y]}, \qquad \mu_X := \mathbb{E}[X] \qquad \text{und} \qquad \sigma_X := \sqrt{\text{Var}[X]}.$$
- Für μ_Y und σ_Y gilt:
$$\begin{aligned}\mu_Y &= \mathbb{E}[Y] = \mathbb{E}[X_1 + \ldots + X_n] = n\mathbb{E}[X] = n\mu_X,\\ \sigma_Y &= \sqrt{\text{Var}[Y]} = \sqrt{\text{Var}[X_1 + \ldots + X_n]} = \sqrt{n\,\text{Var}[X]} = \sqrt{n}\sigma_X.\end{aligned}$$

Standardisierung

Für $Y = X_1 + \ldots + X_n$ gilt approximativ $Y \sim \mathcal{N}(\mu, \sigma^2)$. Der Zentrale Grenzwertsatz „standardisiert“ Y damit $\mu = 0$ und $\sigma^2 = 1$ gilt. Es folgt:

$$\Pr[Y \leq x] = \Pr\left[\underbrace{\frac{Y - \mathbb{E}[Y]}{\sqrt{\mathrm{Var}[Y]}}}_{=:Z \sim \mathcal{N}(0,1)} \leq \frac{x - \mathbb{E}[Y]}{\sqrt{\mathrm{Var}[Y]}}\right] \approx \Phi\left(\frac{x - \mathbb{E}[Y]}{\sqrt{\mathrm{Var}[Y]}}\right).$$

Graphisch:



Info

Für die Verteilungsfunktion einer normalverteilten Zufallsvariable gibt es keinen abgeschlossenen Ausdruck. Mittels Interpolation hat man einige approximative Werte für die Verteilungsfunktion der Standardnormalverteilung (also für Φ) in einer Tabelle aufgelistet. Diese ist überall zu finden, z.B. unter

`de.wikipedia.org/wiki/Tabelle_Standardnormalverteilung`.

Die Tabelle auf den nächsten Folien habe ich aus den Vorlesungsfolien von Prof. Esparza genommen.

Verteilungstabelle Standardnormalverteilung

Für $x \geq 0$ kann man folgender Tabelle den Wert von $\Phi(x)$ entnehmen. Es gilt z.B. $\Phi(1.53) \approx 0.937$ bzw. $z_{0.937} \approx 1.53$.

	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0	0.5000	0.5040	0.5080	0.5120	0.5160	0.5199	0.5239	0.5279	0.5319	0.5359
0.1	0.5398	0.5438	0.5478	0.5517	0.5557	0.5596	0.5636	0.5675	0.5714	0.5753
0.2	0.5793	0.5832	0.5871	0.5910	0.5948	0.5987	0.6026	0.6064	0.6103	0.6141
0.3	0.6179	0.6217	0.6255	0.6293	0.6331	0.6368	0.6406	0.6443	0.6480	0.6517
0.4	0.6554	0.6591	0.6628	0.6664	0.6700	0.6736	0.6772	0.6808	0.6844	0.6879
0.5	0.6915	0.6950	0.6985	0.7019	0.7054	0.7088	0.7123	0.7157	0.7190	0.7224
0.6	0.7257	0.7291	0.7324	0.7357	0.7389	0.7422	0.7454	0.7486	0.7517	0.7549
0.7	0.7580	0.7611	0.7642	0.7673	0.7704	0.7734	0.7764	0.7794	0.7823	0.7852
0.8	0.7881	0.7910	0.7939	0.7967	0.7995	0.8023	0.8051	0.8078	0.8106	0.8133
0.9	0.8159	0.8186	0.8212	0.8238	0.8264	0.8289	0.8315	0.8340	0.8365	0.8389
1.0	0.8413	0.8438	0.8461	0.8485	0.8508	0.8531	0.8554	0.8577	0.8599	0.8621
1.1	0.8643	0.8665	0.8686	0.8708	0.8729	0.8749	0.8770	0.8790	0.8810	0.8830
1.2	0.8849	0.8869	0.8888	0.8907	0.8925	0.8944	0.8962	0.8980	0.8997	0.9015
1.3	0.9032	0.9049	0.9066	0.9082	0.9099	0.9115	0.9131	0.9147	0.9162	0.9177
1.4	0.9192	0.9207	0.9222	0.9236	0.9251	0.9265	0.9279	0.9292	0.9306	0.9319
1.5	0.9332	0.9345	0.9357	0.9370	0.9382	0.9394	0.9406	0.9418	0.9429	0.9441
1.6	0.9452	0.9463	0.9474	0.9484	0.9495	0.9505	0.9515	0.9525	0.9535	0.9545
1.7	0.9554	0.9564	0.9573	0.9582	0.9591	0.9599	0.9608	0.9616	0.9625	0.9633
1.8	0.9641	0.9649	0.9656	0.9664	0.9671	0.9678	0.9686	0.9693	0.9699	0.9706

Verteilungstabelle Standardnormalverteilung

1.9	0.9713	0.9719	0.9726	0.9732	0.9738	0.9744	0.9750	0.9756	0.9761	0.9767
2.0	0.9772	0.9778	0.9783	0.9788	0.9793	0.9798	0.9803	0.9808	0.9812	0.9817
2.1	0.9821	0.9826	0.9830	0.9834	0.9838	0.9842	0.9846	0.9850	0.9854	0.9857
2.2	0.9861	0.9864	0.9868	0.9871	0.9875	0.9878	0.9881	0.9884	0.9887	0.9890
2.3	0.9893	0.9896	0.9898	0.9901	0.9904	0.9906	0.9909	0.9911	0.9913	0.9916
2.4	0.9918	0.9920	0.9922	0.9925	0.9927	0.9929	0.9931	0.9932	0.9934	0.9936
2.5	0.9938	0.9940	0.9941	0.9943	0.9945	0.9946	0.9948	0.9949	0.9951	0.9952
2.6	0.9953	0.9955	0.9956	0.9957	0.9959	0.9960	0.9961	0.9962	0.9963	0.9964
2.7	0.9965	0.9966	0.9967	0.9968	0.9969	0.9970	0.9971	0.9972	0.9973	0.9974
2.8	0.9974	0.9975	0.9976	0.9977	0.9977	0.9978	0.9979	0.9979	0.9980	0.9981
2.9	0.9981	0.9982	0.9982	0.9983	0.9984	0.9984	0.9985	0.9985	0.9986	0.9986
3.0	0.9987	0.9987	0.9987	0.9988	0.9988	0.9989	0.9989	0.9989	0.9990	0.9990
3.1	0.9990	0.9991	0.9991	0.9991	0.9992	0.9992	0.9992	0.9992	0.9993	0.9993
3.2	0.9993	0.9993	0.9994	0.9994	0.9994	0.9994	0.9994	0.9995	0.9995	0.9995
3.3	0.9995	0.9995	0.9995	0.9996	0.9996	0.9996	0.9996	0.9996	0.9996	0.9997
3.4	0.9997	0.9997	0.9997	0.9997	0.9997	0.9997	0.9997	0.9997	0.9997	0.9998
3.5	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998	0.9998

Quelle: `www7.in.tum.de/um/courses/dwt/ss12/folien/tabelle.pdf`.

Das α-Quantil

- Die Umkehrfunktion von Φ heißt z. Es gilt nämlich:

$$\Phi(x) = \alpha \qquad \Longleftrightarrow \qquad z(\alpha) = x$$

  Man nennt $z(\alpha)$ das α-Quantil. Meistens wird z_α statt $z(\alpha)$ geschrieben.

- Weil die Dichtefunktion φ achsensymmetrisch zu $x = 0$ ist (s. Folie 2064), werden nur die Werte $\Phi(x)$ für $x \geq 0$ aufgelistet. Es gilt:

$$\Phi(-x) = 1 - \Phi(x) \qquad \text{und} \qquad z_{1-\alpha} = -z_\alpha.$$

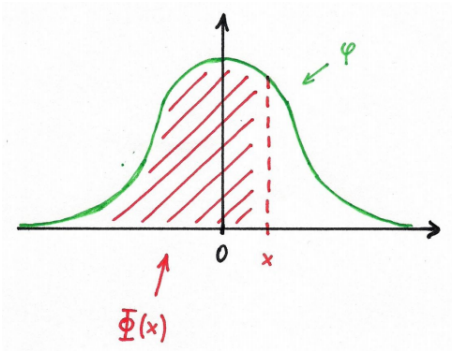
  Beispielsweise gilt:

$$\Phi(-1.96) = 1 - \Phi(1.96) \approx 1 - 0.975 = 0.025$$

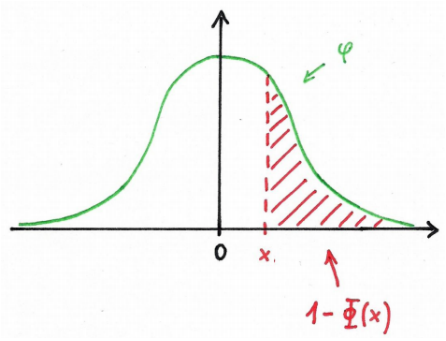
  bzw.

$$z_{0.025} = -z_{0.975} \approx -1.96.$$

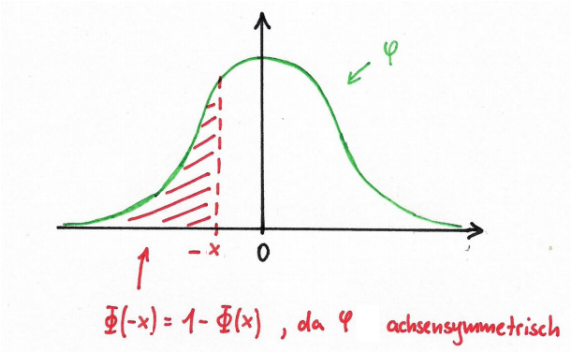
Das α-Quantil



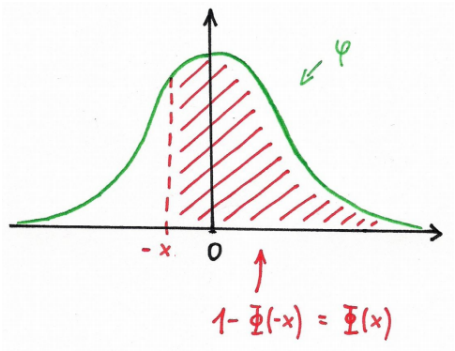
Das α-Quantil



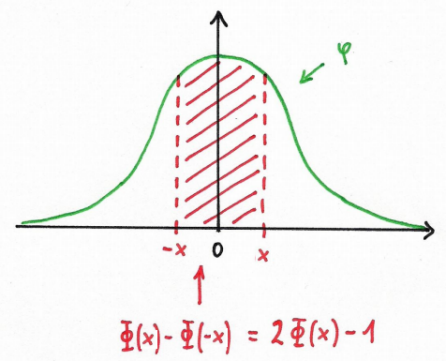
Das α-Quantil



Das α-Quantil



Das α-Quantil



Beispiel

Wir würfeln mit 120 fairen Würfeln. Mit welcher Wahrscheinlichkeit liegt die Summe der Augenzahlen zwischen 410 und 430?

Seien $X_1, \ldots, X_{120}$ unabhängige Ausführungen von $X \sim \text{Uni}(1,6)$ und $Y = X_1 + \ldots + X_{120}$. Gesucht ist

$$\Pr[410 \leq Y \leq 430].$$

Für $\mathbb{E}[X]$ und $\text{Var}[X]$ gilt nach der Tabelle auf Folie 1931:

$$\mathbb{E}[X] = \frac{1+6}{2} = \frac{7}{2} \qquad \text{und} \qquad \text{Var}[X] = \frac{(6-1+1)^2 - 1}{12} = \frac{35}{12}.$$

Daraus folgt für $\mathbb{E}[Y]$ und $\text{Var}[Y]$:

$$\mathbb{E}[Y] = 120 \cdot \frac{7}{2} = 420 \qquad \text{und} \qquad \text{Var}[Y] = 120 \cdot \frac{35}{12} = 350.$$

Beispiel

Es folgt:

$$\begin{aligned}
\Pr[410 \leq Y \leq 430] &= \Pr\left[\frac{410 - \mathbb{E}[Y]}{\sqrt{\mathrm{Var}[Y]}} \leq \frac{Y - \mathbb{E}[Y]}{\sqrt{\mathrm{Var}[Y]}} \leq \frac{430 - \mathbb{E}[Y]}{\sqrt{\mathrm{Var}[Y]}}\right] \\
&= \Pr\left[\frac{410 - 420}{\sqrt{350}} \leq Z \leq \frac{430 - 420}{\sqrt{350}}\right] \\
&= \Pr\left[-\frac{10}{\sqrt{350}} \leq Z \leq \frac{10}{\sqrt{350}}\right] \\
&\approx \Phi\left(\frac{10}{\sqrt{350}}\right) - \Phi\left(-\frac{10}{\sqrt{350}}\right) \approx 2 \cdot \Phi\Bigg(\underbrace{\frac{10}{\sqrt{350}}}_{\approx 0.53}\Bigg) - 1 \approx 0.4038.
\end{aligned}$$

Damit eine Zufallsvariable standardisiert werden kann muss sie nicht notwendigerweise nur eine Summe von Zufallsvariablen $X_1, \ldots, X_n$ sein. Sie kann auch eine lineare Transformation davon sein. Für $Y = X_1 + \ldots + X_n$ und $Y' = aY + b$ gilt:

$$\frac{Y' - \mathbb{E}[Y']}{\sqrt{\mathrm{Var}[Y']}} = \frac{aY + b - (a\mathbb{E}[Y] + b)}{\sqrt{a^2 \,\mathrm{Var}[Y]}} = \frac{a(Y - \mathbb{E}[Y]) + b - b}{a\sqrt{\mathrm{Var}[Y]}} = \frac{Y - \mathbb{E}[Y]}{\sqrt{\mathrm{Var}[Y]}}$$

D.h. man kann den zentralen Grenzwertsatz direkt auf Y' anwenden.

Beispiel

Wir können beispielsweise das arithmetische Mittel

$$\overline{X} = \frac{X_1 + \ldots + X_n}{n}$$

aus Folie 1964 direkt standardisieren, weil es eine lineare Transformation $aY + b$ von

$$Y := X_1 + \ldots + X_n$$

mit $a = \frac{1}{n}$ und $b = 0$ ist. Es folgt:

$$\Pr[\overline{X} \leq x] = \Pr\left[\frac{\overline{X} - \mathbb{E}[\overline{X}]}{\sqrt{\mathrm{Var}[\overline{X}]}} \leq \frac{x - \mathbb{E}[\overline{X}]}{\sqrt{\mathrm{Var}[\overline{X}]}}\right] \approx \Phi\left(\frac{x - \mathbb{E}[\overline{X}]}{\sqrt{\mathrm{Var}[\overline{X}]}}\right).$$

Dies ist wohl das üblichste Beispiel für diesen Trick und es wird sehr oft vorkommen. Ihr dürft das in Zukunft natürlich auch so machen!

Normalverteilung vs. Poisson-Verteilung

Weil eine binomialverteilte Zufallsvariable X aus n zusammenaddierten, unabhängigen, Bernoulli-verteilten Zufallsvariablen besteht, kann sie nicht nur durch die Poisson-Verteilung approximiert werden, sondern auch durch die Normalverteilung. Es entsteht die Frage wann man welche Approximation benutzt:

$$\mathrm{Bin}(n,p) \overset{n\to\infty}{\longrightarrow} \mathrm{Poi}(np) \qquad \text{oder} \qquad \mathrm{Bin}(n,p) \overset{n\to\infty}{\longrightarrow} \mathcal{N}(np, np(1-p)).$$

Der wesentliche Unterschied ist, dass die Poisson-Verteilung diskret ist und die Normalverteilung stetig

Normalverteilung vs. Poisson-Verteilung

D.h.:

- Wir benutzen die Poisson-Verteilung, falls wir an $\Pr[X = k]$ interessiert sind und setzen:

$$\Pr[X = k] = \frac{e^{-\lambda}\lambda^k}{k!} = \frac{e^{-np}(np)^k}{k!}.$$

- Die Normalverteilung benutzen wir, falls wir an $\Pr[a \leq X \leq b]$ interessiert sind und setzen (mit dem Zentralen Grenzwertsatz):

$$\Pr[a \leq X \leq b] = \Phi\left(\frac{b - np}{\sqrt{np(1-p)}}\right) - \Phi\left(\frac{a - np}{\sqrt{np(1-p)}}\right).$$

Themenübersicht

Momenterzeugende Funktion

Momenterzeugendefunktionen gibt es sowohl für diskrete wie auch für kontinuierliche Zufallsvariablen. Für eine beliebige Zufallsvariable X gilt:

$$M_X(s) := \mathbb{E}\left[e^{Xs}\right].$$

Daraus folgt

$$M_X(s) = \sum_{k \in W_X} e^{ks} \cdot f_X(k)$$

falls X diskret ist und

$$M_X(s) = \int_{-\infty}^{\infty} e^{ts} \cdot f_X(t)\ dt$$

falls X stetig ist.

Beispiel (diskrete Zufallsvariable)

Sei X eine diskrete Zufallsvariable mit $W_X = \mathbb{N}$ und Dichtefunktion $f_X(x) = \left(\frac{1}{2}\right)^x$ für alle $x \in W_X$. Dann gilt:

$$M_X(s) = \sum_{k \in W_X} e^{ks} \cdot f_X(k) = \sum_{k=1}^{\infty} e^{ks} \cdot \left(\frac{1}{2}\right)^k = \sum_{k=1}^{\infty} \left(\frac{e^s}{2}\right)^k = \sum_{k=0}^{\infty} \left(\frac{e^s}{2}\right)^k - 1$$
$$\overset{(*)}{=} \frac{1}{1 - \frac{e^s}{2}} - 1 = \frac{\frac{e^s}{2}}{1 - \frac{e^s}{2}} = \frac{e^s}{2 - e^s}.$$

$(*)$ und schon wieder die geometrische Reihe!

Beispiel (stetige Zufallsvariable)

Sei X eine stetige Zufallsvariable mit Wertebereich $W_X = \mathbb{R}_0^+$ und Dichtefunktion $f_X(x) = \frac{1}{e^x}$ für alle $x \in W_X$. Dann gilt:

$$M_X(s) = \int_{-\infty}^{\infty} e^{ts} \cdot f_X(t)\ dt = \int_0^{\infty} e^{ts} \cdot \frac{1}{e^t}\ \mathrm{d}t = \int_0^{\infty} e^{t(s-1)}\ \mathrm{d}t = \frac{1}{1-s}.$$

Beobachtung

Mit $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ und der Linearität des Erwartungswerts bekommt man:

$$M_X(s) = \mathbb{E}\left[e^{Xs}\right] = \mathbb{E}\left[\sum_{k=0}^{\infty} \frac{(Xs)^k}{k!}\right] = \sum_{k=0}^{\infty} \frac{\mathbb{E}\left[X^k\right]}{k!} s^k.$$

Leitet man $M_X(s)$ nach s ab, so erhält man:

$$M'_X(s) = \sum_{k=1}^{\infty} \frac{\mathbb{E}\left[X^k\right]}{k!} k s^{k-1},$$

$$M''_X(s) = \sum_{k=2}^{\infty} \frac{\mathbb{E}\left[X^k\right]}{k!} k(k-1) s^{k-2},$$

$$M'''_X(s) = \sum_{k=3}^{\infty} \frac{\mathbb{E}\left[X^k\right]}{k!} k(k-1)(k-2) s^{k-3},$$

usw.

Beobachtung

Für ein allgemeines $n \in \mathbb{N}_0$ gilt

$$M_X^{(n)}(s) = \sum_{k=n}^{\infty} \frac{\mathbb{E}\left[X^k\right]}{k!} k^{\underline{n}} s^{k-n}$$

und somit

$$M_X^{(n)}(0) = \mathbb{E}[X^n].$$

Erinnerung: Die fallende Faktorielle

$$k^{\underline{n}} = k \cdot (k-1) \cdot (k-2) \cdot \ldots \cdot (k-n+1)$$

kennen wir aus der Kombinatorik.

Achtung!

Nicht jede Zufallsvariable X besitzt eine Momenterzeugende Funktion M_X! Damit M_X existiert muss sie in einer beliebig kleinen Umgebung von 0 definiert sein, d.h.:

$$\exists \epsilon \in \mathbb{R}^+ \ \forall s \in (-\epsilon, \epsilon) : M_X(s) < \infty.$$

Sonst könnte man M_X an der Stelle $s = 0$ nicht ableiten und unsere Herleitung aus den letzten Folien würde nicht mehr funktionieren.

Bei dem Beispiel auf Folie 2085 durfte man an der Stelle $(*)$ die geometrische Reihe nur dann benutzen, falls $\left|\frac{e^s}{2}\right| < 1$, d.h. $s < \ln 2 = 0.6931\ldots$. Das ist kein Problem, weil wir dann M_X beispielsweise auch nur im Intervall $(-\ln 2, \ln 2)$ definieren können.

Zusammenfassung: Rechenregeln für momenterzeugende Funktionen

- **Momenterzeugende Funktion**
  Für eine beliebige Zufallsvariable X gilt $M_X(s) := \mathbb{E}\left[e^{Xs}\right]$. Je nachdem, ob X diskret oder stetig ist folgt:

$$M_X(s) = \sum_{k \in W_X} e^{ks} \cdot f_X(k) \qquad \text{oder} \qquad M_X(s) = \int_{-\infty}^{\infty} e^{ts} \cdot f_X(t)\, \mathrm{d}t$$

- **Beobachtung** (n-tes Moment)
  Für eine beliebige Zufallsvariable X mit momenterzeugender Funktion M_X gilt:

$$M_X^{(n)}(0) = \mathbb{E}[X^n].$$

- **Summen von Zufallsvariablen**
  Für unabhängige Zufallsvariablen $X_1, \ldots, X_n$ gilt:

$$M_{X_1+\ldots+X_n}(s) = M_{X_1}(s) \cdot \ldots \cdot M_{X_n}(s).$$

Tabelle: Formelsammlung für wichtige stetige Verteilungen

Verteilung	W_X	$f_X(x)$	$F_X(x)$	$\mathbb{E}[X]$	$\mathrm{Var}[X]$	$M_X(s)$
$X \sim \mathrm{Uni}(a,b)$	$[a,b]$	$\frac{1}{b-a}$	$\frac{x-a}{b-a}$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$	$\frac{e^{sb}-e^{sa}}{s(b-a)}$
$X \sim \mathrm{Exp}(\lambda)$	$[0,\infty)$	$\lambda e^{-\lambda x}$	$1-e^{-\lambda x}$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$	$\frac{\lambda}{\lambda-s}$
$X \sim \mathrm{Erl}(n,\lambda)$	$[0,\infty)$	$\frac{\lambda^n x^{n-1}}{(n-1)!}e^{-\lambda x}$	$1-\left(\sum_{k=0}^{n-1}\frac{(\lambda x)^k}{k!}\right)e^{-\lambda x}$	$\frac{n}{\lambda}$	$\frac{n}{\lambda^2}$	$\left(\frac{\lambda}{\lambda-s}\right)^n$
$X \sim \mathcal{N}(\mu,\sigma^2)$	$(-\infty,\infty)$	$\frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$	$\int_{-\infty}^{x} f_X(u)\,\mathrm{d}u$	μ	σ^2	$e^{\frac{s\mu+(s\sigma)^2}{2}}$

Wichtig!

- Die Formeln für f_X und F_X gelten nur für $x \in W_X$.
- Für die Verteilungsfunktion der Normalverteilung gibt es leider keine geschlossene Formel.

Erinnerung

Schaut euch bitte die Infos auf Folie 2045 an!

Themenübersicht

Themenübersicht

Das Ziel der ersten zwei Kapitel war es, sowohl für diskrete als auch für kontinuierliche Experimente, gewisse Wahrscheinlichkeiten entweder exakt oder approximativ zu bestimmen. Dabei haben wir immer versucht realistische Annahmen über die zugrunde liegenden Gesetzmäßigkeiten zu machen.

In diesem Kapitel wollen wir die zugrunde liegenden Gesetzmäßigkeiten nicht mehr annehmen, sondern auf sie schließen. Wir werden Zufallsexperimente mit Zufallsvariablen X modellieren, von denen wir, bis auf einen Parameter θ, alles wissen (bzw. mit gutem Gewissen annehmen können). Dann werden wir versuchen, mit Hilfsmitteln aus der Wahrscheinlichkeitstheorie, Aussagen über θ zu treffen. Für die Dichte von X werden wir $f_X(x;\theta)$ statt $f_X(x)$ schreiben, um zu verdeutlichen, dass sie von θ abhängig ist.

Schätzvariable

Gegeben sei eine Zufallsvariable X mit der Dichte $f_X(x, \theta)$. Eine Schätzvariable U für den Parameter θ ist eine Zufallsvariable, die aus mehreren Ausführungen $X_1, \ldots, X_n$ von X zusammengesetzt ist.

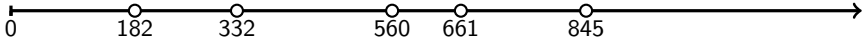
Man sagt auch kurz Schätzer statt Schätzvariable.

Wichtige Begriffe zu Schätzvariablen

Symbol	Bedeutung
X	Zufallsexperiment von dem wir einen Parameter nicht kennen, z.B. $X \sim \text{Bin}(10, p)$
$X_1, \ldots, X_n$	Ausführungen von X (Stichprobenvariablen).
θ	Unbekannter Parameter, z.B. p bei $X \sim \text{Bin}(10, p)$.
$f_X(x; \theta)$	Dichte von X in Abhängigkeit von θ, z.B. $f_X(x; p) = \binom{10}{x} p^x (1-p)^{10-x}$.
U	Schätzvariable oder Schätzer für θ, z.B. $U = \frac{X_1 + \ldots + X_{10}}{100n}$.

Beispiel

Wir stehen am Marienplatz und wollen die Gesamtanzahl der Taxis in München abschätzen. Dabei nehmen wir an, dass jedes Taxi, das wir sehen, gleich wahrscheinlich ist und eine eindeutige Identifikationsnummer $X \sim \text{Uni}(1, m)$ besitzt. Angenommen wir sehen 5 Taxis $X_1, \ldots, X_5$ mit Identifikationsnummern $X_1 = 560$, $X_2 = 332$, $X_3 = 661$, $X_4 = 845$ und $X_5 = 182$.



Einige Schätzer $U_1, \ldots, U_5$ für m könnten beispielsweise sein:

$$
\begin{aligned}
U_1 &= \max\{X_1, \ldots, X_5\} &&= 845,\\
U_2 &= \max\{X_1, \ldots, X_5\} + \tfrac{\max\{X_1,\ldots,X_5\}}{5} &&= 1014,\\
U_3 &= \max\{X_1, \ldots, X_5\} + \min\{X_1, \ldots, X_5\} &&= 1027,\\
U_4 &= 6\min\{X_1, \ldots, X_5\} &&= 1092,\\
U_5 &= 2\tfrac{X_1+\ldots+X_5}{5} &&= 1032.
\end{aligned}
$$

Woher weiß man welchen Schätzer man wählen sollte?

Sei X eine diskrete Zufallsvariable mit $X \sim \text{Bin}\left(m, \frac{1}{2}\right)$ und unbekanntem m. Ferner seien $X_1, \ldots, X_n$ unabhängige Ausführungen von X.

Ist

$$U = \max\{X_1, \ldots, X_n\}$$

ein Schätzer für m?

Antwort

Wieso nicht? U ist eine aus $X_1, \ldots, X_n$ zusammengesetzte Zufallsvariable.

Die Frage ist eher, wie sinnvoll U ist ;-)

Gütekriterien für Schätzer

Jeder Schätzer U kann jeden Parameter θ schätzen. Um die Qualität eines Schätzers U zu quantifizieren, können folgende Größen definiert werden:

- Das Bias:

$$\text{Bias}_\theta(U) \quad := \quad \mathbb{E}[U - \theta] \quad = \quad \mathbb{E}[U] - \theta$$

- Die mittlere quadratische Abweichung (engl. *mean squared error*):

$$\text{MSE}_\theta(U) \quad := \quad \mathbb{E}\big[(U - \theta)^2\big] \quad = \quad \mathbb{E}[U - \theta]^2 + \text{Var}[U] \quad = \quad \text{Bias}_\theta(U)^2 + \text{Var}[U]$$

Gütekriterien für Schätzer

Mithilfe von $\text{Bias}_\theta(U)$ und $\text{MSE}_\theta(U)$ können wir folgende Eigenschaften definieren:

- Die Erwartungstreue:

$$U \text{ erwartungstreu} \iff \text{Bias}_\theta(U) = 0 \iff \mathbb{E}[U] = \theta$$

- Die Konsistenz:

$$U \text{ konsistent im quadratischen Mittel} \iff \lim_{n\to\infty} \text{MSE}_\theta(U) = 0$$

- Die Effizienz:

$$U_1 \text{ effizienter als } U_2 \iff \text{MSE}_\theta(U_1) < \text{MSE}_\theta(U_2).$$

Für einen erwartungstreuen Schätzer U gilt dann: $\mathrm{MSE}_\theta(U) = \mathrm{Var}[U]$.

Beispiel

Wir schätzen den Parameter p einer Zufallsvariable $X \sim \text{Ber}(p)$ mit dem arithmetischen Mittel

$$\overline{X} = \frac{X_1 + \ldots + X_n}{n}.$$

- $\overline{X}$ ist erwartungstreu. Es gilt nämlich nach Folie 1964:

$$\mathbb{E}\left[\overline{X}\right] = \mathbb{E}[X] = p.$$

- Da $\overline{X}$ erwartungstreu ist, gilt $\text{MSE}_p(\overline{X}) = \text{Var}\left[\overline{X}\right]$. Es folgt wieder nach Folie 1964:

$$\text{MSE}_p(\overline{X}) = \text{Var}\left[\overline{X}\right] = \frac{\text{Var}[X]}{n} = \frac{p(1-p)}{n}.$$

- Wegen $\lim_{n\to\infty} \frac{p(1-p)}{n} = 0$ ist U sogar konsistent im quadratischen Mittel.

Sei X die diskrete Zufallsvariable $X \sim \text{Uni}(1, m)$ aus dem Beispiel auf Folie 2099 mit unbekanntem m. Ferner seien $X_1, \ldots, X_n$ unabhängige Ausführungen von X.

Sei U folgender Schätzer für m:

$$U = 2 \cdot \frac{X_1 + \ldots + X_n}{n} - 1.$$

1. Ist U erwartungstreu?
2. Was ist die mittlere quadratische Abweichung $\text{MSE}_m(U)$ von U?
3. Ist U konsistent im quadratischen Mittel?

Erinnerung: Für $X \sim \text{Uni}(a, b)$ gilt $\mathbb{E}[X] = \frac{a+b}{2}$ und $\text{Var}[X] = \frac{(b-a+1)^2-1}{12}$ (s. Folie 1931).

1. Ja! Es gilt:

$$\mathbb{E}[U] = \mathbb{E}\left[2 \cdot \frac{X_1 + \ldots + X_n}{n} - 1\right] = \frac{2}{n} \cdot \mathbb{E}[X_1 + \ldots + X_n] - 1$$
$$= \frac{2}{n} \cdot (\mathbb{E}[X_1] + \ldots + \mathbb{E}[X_n]) - 1 = \frac{2}{n} \cdot n \cdot \mathbb{E}[X] - 1 = 2 \cdot \mathbb{E}[X] - 1 = 2 \cdot \frac{1+m}{2} - 1 = m.$$

2. Da U erwartungstreu ist, gilt $\text{Bias}_m(U) = 0$ und somit $\text{MSE}_m(U) = \text{Var}[U]$. Es folgt:

$$\text{MSE}_m(U) = \text{Var}[U] = \text{Var}\left[\frac{2 \cdot (X_1 + \ldots + X_n)}{n} - 1\right] = \left(\frac{2}{n}\right)^2 \cdot \text{Var}[X_1 + \ldots + X_n]$$
$$= \left(\frac{2}{n}\right)^2 \cdot (\text{Var}[X_1] + \ldots + \text{Var}[X_n]) = \left(\frac{2}{n}\right)^2 \cdot n \cdot \text{Var}[X] = \frac{4}{n} \cdot \text{Var}[X]$$
$$= \frac{4}{n} \cdot \frac{m^2 - 1}{12} = \frac{m^2 - 1}{3n}.$$

3. Wegen $\lim_{n\to\infty} \frac{m^2-1}{3n} = 0$ ist U konsistent im quadratischen Mittel.

Bekannte erwartungstreue Schätzer

- Die Zufallsvariable $\overline{X}$ mit

$$\overline{X} = \frac{1}{n} \sum_{i=1}^{n} X_i$$

heißt Stichprobenmittel und ist immer ein erwartungstreuer Schätzer für den Erwartungswert $\mu_X = \mathbb{E}[X]$.

(Beispiele hierzu sind p in Ber(p), λ in Poi(λ) und μ in $\mathcal{N}(\mu, \sigma^2)$.)

- Die Zufallsvariable S^2 mit

$$S^2 = \frac{1}{n-1} \sum_{i=1}^{n} (X_i - \overline{X})^2$$

heißt Stichprobenvarianz und ist immer ein erwartungstreuer Schätzer für die Varianz $\sigma_X^2 = \mathrm{Var}[X]$.

(Beispiele hierzu sind λ in Poi(λ) und σ^2 in $\mathcal{N}(\mu, \sigma^2)$.)

Themenübersicht

Maximum-Likelihood-Methode

Mit dieser Methode kann man für eine gegebene Zufallsvariable X mit Dichte $f_X(x;\theta)$ einen Schätzer U für θ finden:

1. Likelihood-Funktion aufstellen:

$$L(\vec{x};\theta) = \prod_{i=1}^{n} f_X(x_i;\theta)$$

2. θ so bestimmen, dass $L(\vec{x};\theta)$ maximal ist. Man erhält für θ einen Ausdruck in Abhängigkeit von $x_1, \ldots, x_n$.
3. U ist derselbe Ausdruck wie für θ, aber mit $X_1, \ldots, X_n$ statt $x_1, \ldots, x_n$.

Man nennt U den Maximum-Likelihood-Schätzer oder kurz: ML-Schätzer für θ.

Beispiel

Wir bestimmen, in Abhängigkeit der Stichprobenvariablen $X_1, \ldots, X_n$, einen ML-Schätzer U für p, falls $X \sim \text{Ber}(p)$.

1. Für alle $x_1, \ldots, x_n \in \{0, 1\}$ gilt:

$$L(\vec{x}, p) = \prod_{i=1}^{n} f(x_i; p) = \prod_{i=1}^{n} p^{x_i}(1-p)^{1-x_i} = p^{x_1+\ldots+x_n} \cdot (1-p)^{n-(x_1+\ldots+x_n)} = p^c \cdot (1-p)^{n-c},$$

wobei $c := x_1 + \ldots + x_n$ als konstant betrachtet werden kann, weil es nicht von p abhängt.

Beispiel

2. Für die Ableitung von $L(\vec{x}, p)$ gilt:

$$\begin{aligned} L'(\vec{x}, p) &= c \cdot p^{c-1} \cdot (1-p)^{n-c} + p^c \cdot (n-c) \cdot (1-p)^{n-c-1} \cdot (-1) \\ &= p^{c-1} \cdot (1-p)^{n-c-1} \cdot (c \cdot (1-p) - p(n-c)). \end{aligned}$$

   $L'(\vec{x}, p) \stackrel{!}{=} 0$ liefert die zwei Minima $p = 0$ und $p = 1$ und das Maximum $p = \frac{c}{n} = \frac{x_1 + \ldots + x_n}{n}$.

3. Somit ist $U = \frac{X_1 + \ldots + X_n}{n} = \overline{X}$ der ML-Schätzer für p und wir wissen aus Folie 2109, dass dieser erwartungstreu ist.

Noch ein Beispiel

Wir bestimmen, in Abhängigkeit der Stichprobenvariablen $X_1, \ldots, X_n$, einen ML-Schätzer U für p, falls $X \sim \text{Geo}(p)$.

1. Für alle $x_1, \ldots, x_n \in \mathbb{N}$ gilt:

$$L(\vec{x}, p) = \prod_{i=1}^{n} f(x_i; p) = \prod_{i=1}^{n} p(1-p)^{x_i - 1} = p^n \cdot (1-p)^{x_1 + \ldots + x_n - n} = p^n \cdot (1-p)^{c-n},$$

wobei $c := x_1 + \ldots + x_n$ als konstant betrachtet werden kann, weil es nicht von p abhängt.

Noch ein Beispiel

2. Für die Ableitung von $L(\vec{x}, p)$ gilt:

$$\begin{aligned} L'(\vec{x}, p) &= n \cdot p^{n-1} \cdot (1-p)^{c-n} + p^n \cdot (c-n) \cdot (1-p)^{c-n-1} \cdot (-1) \\ &= p^{n-1} \cdot (1-p)^{c-n-1} \cdot (n \cdot (1-p) - p(c-n)). \end{aligned}$$

   $L'(\vec{x}, p) \stackrel{!}{=} 0$ liefert die zwei Minima $p = 0$ und $p = 1$ und das Maximum $p = \frac{n}{c} = \frac{n}{x_1 + \ldots + x_n}$.

3. Somit ist $U = \frac{n}{X_1 + \ldots + X_n}$ der ML-Schätzer für p.

Infos

- Oft kann man den optimalen Wert für θ wie oben auf die übliche Art bestimmen: $L(\vec{x};\theta)$ nach θ ableiten und die Ableitung gleich Null setzen. Leider funktioniert das nicht immer, da z.B. θ auch diskret sein kann.
- Ist $L(\vec{x};\theta)$ zu schwer zum maximieren (z.B. weil zu viele Faktoren von θ abhängen), so kann man stattdessen auch

$$\ln L(\vec{x};\theta) = \ln\left(\prod_{i=1}^{n} f(x_i;\theta)\right) = \sum_{i=1}^{n} \ln f(x_i;\theta)$$

  maximieren, da *ln* monoton steigend ist.
- Mit der Maximum-Likelihood-Methode findet man zwar einen Schätzer für θ, aber nicht notwendigerweise den besten. Manchmal ist er nicht mal erwartungstreu!

Quizfrage (schwer!)

Ist der ML-Schätzer

$$U = \frac{1}{\overline{X}} = \frac{n}{\sum_{i=1}^{n} X_i}$$

einer geometrisch verteilten Zufallsvariable erwartungstreu für $n = 1$?

Hinweis: Für $-1 < x \leq 1$ gilt:

$$\sum_{k=1}^{\infty} \frac{(-x)^k}{k} = -\ln(1+x).$$

Wegen $n = 1$ ist $U = \frac{1}{X_1}$. Für den Erwartungswert von U folgt:

$$\mathbb{E}[U] = \mathbb{E}\left[\frac{1}{X_1}\right] = \sum_{k=1}^{\infty} \frac{1}{k} \cdot f_{X_1}(k) = \sum_{k=1}^{\infty} \frac{1}{k} \cdot p(1-p)^{k-1} = \frac{p}{1-p} \cdot \sum_{k=1}^{\infty} \frac{(1-p)^k}{k}$$

$$= \frac{p}{1-p} \cdot \sum_{k=1}^{\infty} \frac{(-(p-1))^k}{k} \overset{(*)}{=} \frac{p}{1-p} \cdot (-\ln(1+(p-1))) = -\frac{p \ln p}{1-p} \neq p.$$

$(*)$ Hinweis mit $x = p - 1$.

U ist also im Allgemeinen nicht erwartungstreu!

Themenübersicht

Konfidenzintervalle

Das Ziel ist es ein Intervall $I = [U_1, U_2]$ zu finden, so dass

$$\Pr[U_1 \leq \theta \leq U_2] \geq 1 - \alpha$$

gilt. Am häufigsten und einfachsten findet man symmetrische Konfidenzintervalle $[U_1, U_2]$ wie folgt:

1. Finde einen Schätzer U für θ, z.B. durch raten oder mit der Maximum-Likelihood-Methode.
2. Setze $U_1 := U - \delta$ und $U_2 := U + \delta$ für $\delta \geq 0$ und bestimme δ, so dass gilt:

   $$\Pr[\theta - \delta \leq U \leq \theta + \delta] \geq 1 - \alpha,$$

   z.B. mit dem zentralen Grenzwertsatz (falls anwendbar).

$$\Pr[\underbrace{U-\delta}_{U_1} \leq \theta \leq \underbrace{U+\delta}_{U_2}] = \Pr[|\theta - U| \leq \delta] = \Pr[|U - \theta| \leq \delta] = \Pr[\theta - \delta \leq U \leq \theta + \delta].$$

Wichtige Begriffe zu Konfidenzintervallen

Symbol	Bedeutung
$[U_1, U_2]$	Konfidenzintervall. U_1 und U_2 sind wieder Schätzvariablen.
θ	Wieder der unbekannte Parameter.
$1 - \alpha$	Konfidenzniveau. α ist die maximale Wahrscheinlichkeit, dass θ nicht in I liegt.

Beispiel

Wir Schätzen die Höhe h (in m) eines Hochhauses. Hierfür verwenden wir ein Messgerät X mit einem Erwartungswert von $\mathbb{E}[X] = h$ (in m) und einer (technisch bedingten) Varianz von $\mathrm{Var}[X] = 4$ (in m^2).

Wir benutzen das Stichprobenmittel $\overline{X}$ als Schätzer für h und erhalten nach 100 Messungen $X_1, \ldots, X_{100}$ den Mittelwert $\overline{X} = 87.25$ m. Wir interessieren uns für ein Intervall $I = [U_1, U_2]$, in dem sich die Höhe h des Hochhauses mit 90% Wahrscheinlichkeit befindet.

Aus Folie 1964 wissen wir:

$$\mathbb{E}\left[\overline{X}\right] = \mathbb{E}[X] = h \qquad \text{und} \qquad \mathrm{Var}\left[\overline{X}\right] = \frac{\mathrm{Var}[X]}{100} = \frac{1}{25}.$$

Beispiel

Mithilfe des Zentralen Grenzwertsatzes und des Tricks aus Folie 2079 kann das gesuchte Konfidenzintervall ermittelt werden:

$$\begin{aligned}\Pr[h-\delta \leq \overline{X} \leq h+\delta] &= \Pr\left[\frac{h-\delta-h}{\sqrt{1/25}} \leq \frac{\overline{X}-\mathbb{E}[X]}{\sqrt{\mathrm{Var}[X]}} \leq \frac{h+\delta-h}{\sqrt{1/25}}\right] \\ &\approx \Phi(5\delta) - \Phi(-5\delta) \\ &= 2\Phi(5\delta) - 1 \overset{!}{\geq} 0.9\end{aligned}$$

Daraus folgt:

$$\Phi(5\delta) \overset{!}{\geq} 0.95 \quad \Longleftrightarrow \quad 5\delta \overset{!}{\geq} z_{0.95} \quad \Longleftrightarrow \quad \delta \overset{!}{\geq} \frac{z_{0.95}}{5} \approx \frac{1.645}{5} = 0.329.$$

Wir wählen also $I = [U_1, U_2]$ mit $U_1 = \overline{X} - \delta \approx 86.921$ und $U_2 = \overline{X} + \delta \approx 87.579$.

Themenübersicht

Hypothesentests

Man benutzt statistische Tests, wenn man nicht an dem exakten Wert von θ interessiert ist, sondern falls man eine Vermutung (z.B. $\theta \leq 8$ oder $\theta = 3$) bestätigen, bzw. widerlegen will.

Wichtige Begriffe zu Hypothesentests

Symbol	Bedeutung
H_0	Nullhypothese. Was getestet werden soll.
H_1	Alternative. Was gilt, falls H_0 nicht stimmt.
α	Signifikanzniveau. Die maximale (worst case) Wahrscheinlichkeit, dass H_0 zwar gilt, aber vom Test abgelehnt wird.
β	Die maximale (worst case) Wahrscheinlichkeit, dass H_1 zwar gilt, aber H_0 vom Test angenommen wird.
T	Testgröße. Irgendeine Zufallsvariable in Abhängigkeit von $X_1, \ldots, X_n$ von der man F_T entweder kennt oder zumindest abschätzen kann.
K	Ablehnungsbereich. Falls $T \in K$, dann wird H_0 abgelehnt, ansonsten wird H_0 angenommen.

Fehlerwahrscheinlichkeiten 1. und 2. Art

- Die Fehlerwahrscheinlichkeit erster Art α ist die maximale Wahrscheinlichkeit dafür, dass H_0 gilt, aber abgelehnt wird:

$$\alpha := \sup_{\theta \in H_0} \Pr_\theta[T \in K].$$

- Die Fehlerwahrscheinlichkeit zweiter Art β ist die maximale Wahrscheinlichkeit dafür, dass H_0 nicht gilt, aber angenommen wird:

$$\beta := \sup_{\theta \in H_1} \Pr_\theta[T \notin K].$$

Erinnerung: sup ist das Supremum, d.h. die kleinste obere Schranke für $\Pr_\theta[\ldots]$.

Fehlerwahrscheinlichkeiten 1. und 2. Art

Als Tabelle:

	H_0 wird angenommen $T \notin K$	H_0 wird abgelehnt $T \in K$
H_0 gilt $\theta \in H_0$	Richtig $\Pr_\theta[T \notin K] \geq 1 - \alpha$	Fehler 1. Art $\Pr_\theta[T \in K] \leq \alpha$
H_1 gilt $\theta \in H_1$	Fehler 2. Art $\Pr_\theta[T \notin K] \leq \beta$	Richtig $\Pr_\theta[T \in K] \geq 1 - \beta$

Info

Bei jeder Zeile ist die Summe der Wahrscheinlichkeiten immer 1. $\alpha + \beta = 1$ muss allerdings nicht notwendigerweise gelten. Dies erkennt man beispielsweise an den Werten von α und β im Beispiel auf Folie 2132.

Info

Die übliche Vorgehenweise bei Tests ist:

1. α festlegen (z.B. $\alpha = 0.05$),
2. Ablehnungsbereich K in Abhängigkeit von α bestimmen,
3. β in Abhängigkeit von K bestimmen,
4. Test durchführen und auswerten.

Beispiel

Basketballer Air Andrej vermutet, weil er eben bei vier von fünf Drei-Punkt-Würfen den Korb getroffen hat, dass seine Trefferwahrscheinlichkeit 80% ist. Trainer Ledian vermutet, dass er nur Glück hatte und dass seine Trefferwahrscheinlichkeit höchstens 50% ist. Sie einigen sich auf folgenden Test: Air Andrej soll 40 mal werfen. Trifft er mehr als 24 mal, so hatte er recht. Anderenfalls hatte sein Trainer recht. Sie legen also folgendes fest:

- Annahme: Jeder Wurf ist $\text{Ber}(p)$-verteilt und unabhängig von den Würfen davor.
- Hypothesen:

$$H_0 : p \leq 0.5 \qquad H_1 : p = 0.8$$

- Testgröße:

$$T = X_1 + \ldots + X_{40} \sim \text{Bin}(40, p)$$

- Ablehnungsbereich:

$$K = \{25, 26, 27, \ldots, 40\}$$

Was sind hier die Fehlerwahrscheinlichkeiten?

Beispiel

- Fehler 1. Art:

$$\alpha = \sup_{p \leq 0.5} \Pr_p[T > 24] \overset{(*)}{=} \Pr_{0.5}[T > 24] = \sum_{k=25}^{40} \binom{40}{k} \cdot 0.5^k \cdot 0.5^{40-k} \overset{\text{🪄}}{\approx} 0.077$$

  Es passiert also höchstens mit Wahrscheinlichkeit 7.7%, dass Basketballer Air Andrej fälschlicherweise recht hat.

- Fehler 2. Art:

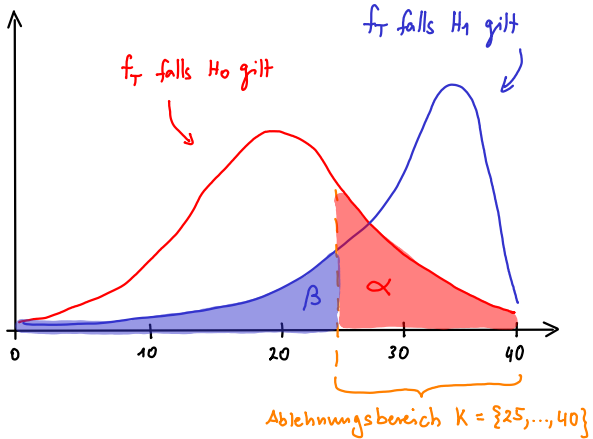
$$\beta = \sup_{p=0.8} \Pr_p[T \leq 24] = \Pr_{0.8}[T \leq 24] = \sum_{k=0}^{24} \binom{40}{k} \cdot 0.8^k \cdot 0.2^{40-k} \overset{\text{🪄}}{\approx} 0.003$$

  Es passiert also höchstens mit Wahrscheinlichkeit 0.3%, dass Trainer Ledian fälschlicherweise recht hat.

$(*)$ Je größer p, desto größer ist $\Pr_p[T > 24]$. Weil aber $p \leq 0.5$ gelten muss, wählt man einfach $p = 0.5$, damit $\Pr_p[T > 24]$ maximal ist.

Beispiel

Graphisch:



Air Andrej sind 40 Würfe zu viel. Er möchte nur 20 mal werfen und möchte die Wahrscheinlichkeit, dass sein Trainer fälschlicherweise recht bekommt, auf 1% beschränken.

1. Bleiben die Hypothesen wie zuvor ($H_0 : p \leq 0.5$ vs. $H_1 : p = 0.8$) oder werden sie vertauscht ($H_0 : p = 0.8$ vs. $H_1 : p \leq 0.5$)?
2. Wie oft muss er bei 20 Würfen mindestens daneben werfen, damit Ledian recht bekommt? (D.h. wie sieht der Ablehnungsbereich K aus?)
3. Was ist die kleinste obere Schranke dafür, dass Andrej fälschlicherweise recht bekommt? (D.h. Wie groß ist jetzt β?)

Hinweis: Bitte nicht exakt rechnen, sondern den zentralen Grenzwertsatz benutzen!

1. Es gilt $\alpha = 0.01$. Laut Aufgabe soll gelten:

$$\sup_{\text{Andrej hat recht}} \Pr_p[\text{Ledian bekommt recht}] = 0.01.$$

Somit is $p = 0.8$ (also „Andrej hat recht“) die Nullhypothese und $p \leq 0.5$ die Alternative:

$$H_0 : p = 0.8 \qquad\qquad H_1 : p \leq 0.5$$

Als Tabelle:

	Ledian bekommt recht	Andrej bekommt recht
$p \leq 0.5$ gilt	Richtig	Fehler 2. Art
$p = 0.8$ gilt	Fehler 1. Art	Richtig

2. Der Ablehnungsbereich ist von der Form $K = \{0, \dots, k\}$, denn $K = \{k+1, \dots, n\}$ würde keinen Sinn machen. Wir rechnen:

$$\begin{aligned}\sup_{p=0.8} \Pr_p[T \leq k] = \Pr_{0.8}[T \leq k] &= \Pr_{0.8}\left[\frac{T - \mathbb{E}[T]}{\sqrt{\mathrm{Var}[T]}} \leq \frac{k - 20p}{\sqrt{20p(1-p)}}\right] \\ &= \Pr\left[\frac{T - \mathbb{E}[T]}{\sqrt{\mathrm{Var}[T]}} \leq \frac{k - 20 \cdot 0.8}{\sqrt{20 \cdot 0.8 \cdot 0.2}}\right] \\ &\overset{\text{ZGWS}}{\approx} \Phi\left(\frac{k-16}{\sqrt{3.2}}\right) \overset{!}{=} 0.01\end{aligned}$$

$$\iff \frac{k-16}{\sqrt{3.2}} = z(0.01) = -z(0.99) \approx -2.33 \iff k = -2.33 \cdot \sqrt{3.2} + 16 \approx 11.83$$

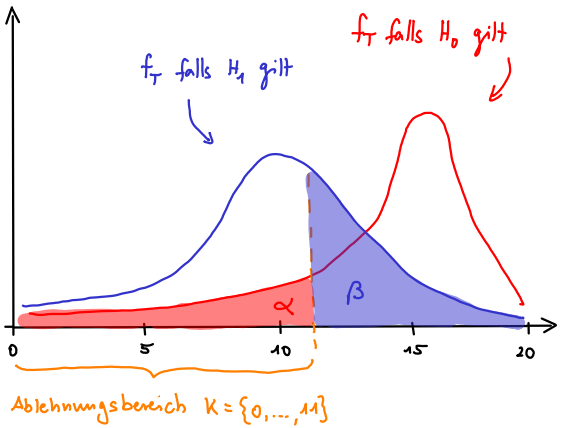
Somit ist $K = \{0, \dots, 11\}$, d.h. Andrej muss bei mindestens 12 von 20 Würfen treffen um recht zu bekommen.

3. Für β gilt:

$$\begin{aligned}
\beta &= \sup_{p \leq 0.5} \Pr_p[T > k] \\
&= \Pr_{0.5}[T > 11] \\
&= 1 - \Pr_{0.5}[T \leq 11] \\
&= 1 - \Pr_{0.5}\left[\frac{T - \mathbb{E}[T]}{\sqrt{\mathrm{Var}[T]}} \leq \frac{11 - 20p}{\sqrt{20p(1-p)}}\right] \\
&= 1 - \Pr\left[\frac{T - \mathbb{E}[T]}{\sqrt{\mathrm{Var}[T]}} \leq \frac{11 - 20 \cdot 0.5}{\sqrt{20 \cdot 0.5 \cdot 0.5}}\right] \\
&\overset{\text{ZGWS}}{\approx} 1 - \Phi\left(\frac{1}{\sqrt{5}}\right) \approx 1 - \Phi(0.45) \approx 0.3264
\end{aligned}$$

Die Wahrscheinlichkeit, dass Air Andrej eine Trefferwahrscheinlichkeit von höchstens 0.5 hat und trotzdem bei mehr als 11 von 20 Würfen trifft ist höchstens 32.64%.

Graphisch:


f_T falls H_0 gilt
f_T falls H_1 gilt
α
β
0
5
10
15
20
Ablehnungsbereich $K = \{0, \ldots, 11\}$

Das Signifikanzniveau α

Bei statistischen Tests ist es sehr schwer beide Fehlerarten klein zu halten. Je kleiner α gewählt wird, desto größer ist β und umgekehrt. Deswegen wird versucht nur α möglichst klein zu halten.

Dies hat zwei bedeutende Folgen:

- Wird H_0 abgelehnt, dann können wir mit hoher Sicherheit sagen, dass H_1 gilt. Wir wissen nämlich, dass H_0 mit höchstens α Wahrscheinlichkeit fälschlicherweise abgelehnt wird. Da α meistens sehr klein ist, ist die Fehlerwahrscheinlichkeit hier auch klein.
- Wird H_0 angenommen, dann können wir nichts mit Sicherheit sagen. Wir wissen nämlich, dass H_0 mit höchstens β Wahrscheinlichkeit fälschlicherweise angenommen wird. Da β meistens sehr groß ist, kann die Fehlerwahrscheinlichkeit sowohl klein als auch groß sein.

Quizfragen (Tills Grillparty)

Till schmeißt am Wochenende eine Grillparty und möchte mithilfe eines statistischen Tests entscheiden, für wie viele Gäste er Essen und Getränke einkaufen soll. Er hat 100 Freunde eingeladen und geht davon aus, dass jeder, unabhängig von den anderen, mit Wahrscheinlichkeit p zum grillen & chillen vorbeikommt.

Er vermutet, da seine Freunde ihn sehr gern haben, dass p mindestens 0.9 ist. Sein Bruder ist eher pessimistisch und vermutet, da Deutschland an dem Tag spielt, dass p höchstens 0.4 ist. Wie sollte er H_0, H_1 und α in folgenden Situationen jeweils wählen?

1. Er will die Wahrscheinlichkeit auf 0.1 beschränken, dass er mit $p \geq 0.9$ rechnet, aber tatsächlich $p \leq 0.4$ gilt. In dem Fall würde er ja zu viel Geld ausgeben.
2. Er will die Wahrscheinlichkeit auf 0.2 beschränken, dass er mit $p \leq 0.4$ rechnet, aber tatsächlich $p \geq 0.9$ gilt. In dem Fall könnte er seinen Gästen nicht genug zu essen und trinken anbieten und das wäre peinlich!

1. In diesem Fall sollte er

$$H_0 : p \leq 0.4, \quad H_1 : p \geq 0.9 \quad \text{und} \quad \alpha = 0.1$$

wählen. Auf diese Weise passiert es mit höchstens 0.1 Wahrscheinlichkeit, dass wenige Gäste kommen ($p \leq 0.4$ gilt), er aber zu viel einkauft (der Test sagt $p \geq 0.9$).

2. In diesem Fall sollte er

$$H_0 : p \geq 0.9, \quad H_1 : p \leq 0.4 \quad \text{und} \quad \alpha = 0.2$$

wählen. Auf diese Weise passiert es mit höchstens 0.2 Wahrscheinlichkeit, dass viele Gäste kommen ($p \geq 0.9$ gilt), er aber zu wenig einkauft (der Test sagt $p \leq 0.4$).

Approximativer Binomialtest

Annahmen:

$X_1, \ldots, X_n$ seien unabhängig und identisch verteilt mit $\Pr[X_i = 1] = p$ und $\Pr[X_i = 0] = 1-p$, wobei p unbekannt sei. n sei hinreichend groß, so dass die Approximation aus Korollar 109 brauchbare Ergebnisse liefert.

Hypothesen:

$$\begin{array}{lllll} a) & H_0 : p = p_0 & \text{gegen} & H_1 : p \neq p_0, \\ b) & H_0 : p \geq p_0 & \text{gegen} & H_1 : p < p_0, \\ c) & H_0 : p \leq p_0 & \text{gegen} & H_1 : p > p_0. \end{array}$$

Testgröße:

$$Z := \frac{h - np_0}{\sqrt{np_0(1-p_0)}},$$

wobei $h := X_1 + \ldots + X_n$ die Häufigkeit bezeichnet, mit der die Ereignisse $X_i = 1$ aufgetreten sind.

Ablehnungskriterium für H_0 bei Signifikanzniveau α:

$$\begin{array}{ll} a) & |Z| > z_{1-\alpha/2}, \\ b) & Z < z_\alpha, \\ c) & Z > z_{1-\alpha}. \end{array}$$

Quelle: `www14.in.tum.de/lehre/2014SS/dwt/2014-[]dwt.pdf`, Seite 358.

Gaußtest

Annahmen:

$X_1, \ldots, X_n$ *seien unabhängig und identisch verteilt mit* $X_i \sim \mathcal{N}(\mu, \sigma^2)$, *wobei* σ^2 *bekannt ist. Alternativ gelte* $\mathbb{E}[X_i] = \mu$ *und* $\mathrm{Var}[X_i] = \sigma^2$, *und* n *sei groß genug.*

Hypothesen:

$$\begin{array}{lllll} a) & H_0 : \mu = \mu_0 & \textit{gegen} & H_1 : \mu \neq \mu_0, \\ b) & H_0 : \mu \geq \mu_0 & \textit{gegen} & H_1 : \mu < \mu_0, \\ c) & H_0 : \mu \leq \mu_0 & \textit{gegen} & H_1 : \mu > \mu_0. \end{array}$$

Testgröße:

$$Z := \frac{\overline{X} - \mu_0}{\sigma} \sqrt{n}\,.$$

Ablehnungskriterium für H_0 bei Signifikanzniveau α:

$$\begin{array}{ll} a) & |Z| > z_{1-\alpha/2}, \\ b) & Z < z_\alpha, \\ c) & Z > z_{1-\alpha}. \end{array}$$

Quelle: `www14.in.tum.de/lehre/2014SS/dwt/2014-[]dwt.pdf`, Seite 367.

t-Test

Annahmen:

$X_1, \ldots, X_n$ *seien unabhängig und identisch verteilt mit* $X_i \sim \mathcal{N}(\mu, \sigma^2)$.
Alternativ gelte $\mathbb{E}[X_i] = \mu$ *und* $\mathrm{Var}[X_i] = \sigma^2$, *und* n *sei groß genug.*

Hypothesen:

$$\begin{array}{lllll} a) & H_0 : \mu = \mu_0 & \textit{gegen} & H_1 : \mu \neq \mu_0, \\ b) & H_0 : \mu \geq \mu_0 & \textit{gegen} & H_1 : \mu < \mu_0, \\ c) & H_0 : \mu \leq \mu_0 & \textit{gegen} & H_1 : \mu > \mu_0. \end{array}$$

Testgröße:

$$T := \frac{\overline{X} - \mu_0}{S} \sqrt{n}.$$

Ablehnungskriterium für H_0 bei Signifikanzniveau α:

$$\begin{array}{ll} a) & |T| > t_{n-1,1-\alpha/2}, \\ b) & T < t_{n-1,\alpha}, \\ c) & T > t_{n-1,1-\alpha}. \end{array}$$

Quelle: `www14.in.tum.de/lehre/2014SS/dwt/2014-[]dwt.pdf`, Seite 369.

Zwei-Stichproben-t-Test

Annahmen:

$X_1, \ldots, X_m$ *und* $Y_1, \ldots, Y_n$ *seien unabhängig und jeweils identisch verteilt, wobei* $X_i \sim \mathcal{N}(\mu_X, \sigma_X^2)$ *und* $Y_i \sim \mathcal{N}(\mu_Y, \sigma_Y^2)$ *gelte. Die Varianzen seien identisch, also* $\sigma_X^2 = \sigma_Y^2$.

Hypothesen:

$$\begin{array}{lllll} a) & H_0 : \mu_X = \mu_Y & \text{gegen} & H_1 : \mu_X \neq \mu_Y, \\ b) & H_0 : \mu_X \geq \mu_Y & \text{gegen} & H_1 : \mu_X < \mu_Y, \\ c) & H_0 : \mu_X \leq \mu_Y & \text{gegen} & H_1 : \mu_X > \mu_Y. \end{array}$$

Testgröße:

$$T := \sqrt{\frac{n+m-2}{\frac{1}{m}+\frac{1}{n}}} \cdot \frac{\overline{X} - \overline{Y}}{\sqrt{(m-1) \cdot S_X^2 + (n-1) \cdot S_Y^2}}.$$

Ablehnungskriterium für H_0 bei Signifikanzniveau α:

$$\begin{array}{ll} a) & |T| > t_{m+n-2,1-\alpha/2}, \\ b) & T < t_{m+n-2,\alpha}, \\ c) & T > t_{m+n-2,1-\alpha}. \end{array}$$

Quelle: `www14.in.tum.de/lehre/2014SS/dwt/2014-[]dwt.pdf`, Seite 374.

χ^2-Anpassungstest

Annahmen:

$X_1, \ldots, X_n$ *seien unabhängig und identisch verteilt mit* $W_{X_i} = \{1, \ldots, k\}$.

Hypothesen:

$$H_0 \ : \ \Pr[X = i] = p_i \quad \text{für } i = 1, \ldots, k,$$
$$H_1 \ : \ \Pr[X = i] \neq p_i \quad \text{für mindestens ein } i \in \{1, \ldots, k\},$$

Testgröße:

$$T = \sum_{i=1}^{k} \frac{(h_i - np_i)^2}{np_i},$$

wobei h_i *die Häufigkeit angibt, mit der* $X_1, \ldots, X_n$ *den Wert* i *angenommen haben.*

Ablehnungskriterium für H_0 bei Signifikanzniveau α:

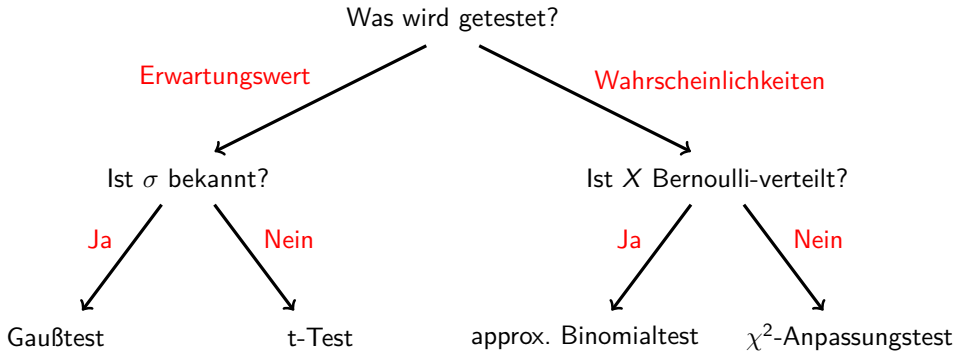
$$T > \chi^2_{k-1,1-\alpha};$$

dabei sollte gelten, dass $np_i \geq 1$ *für alle* i *und* $np_i \geq 5$ *für mindestens* 80% *der Werte* $i = 1, \ldots, k$.

Quelle: `www14.in.tum.de/lehre/2014SS/dwt/2014-[]dwt.pdf`, Seite 377.

Vorgefertigte Tests

Gegeben seien unabhängige Ausführungen $X_1, \ldots, X_n$ (Stichproben) einer Zufallsvariable X mit Erwartungswert μ und Standardabweichung σ (bzw. Varianz σ^2). Welchen vorgefertigten Test sollte man wählen?



Tests zum Improvisieren

Diese Tests sind etwas schwieriger. Deswegen gibts hier einige Erklärungen zu ihnen und ein paar Altklausuraufgaben zum Üben.

Gegeben sind:

- unabhängige Stichproben $X_1, \ldots, X_n \sim \text{Ber}(p)$ mit bekanntem n, aber unbekanntem p,
- die Testgröße $T = X_1 + \ldots + X_n$ mit $T \sim \text{Bin}(n, p)$,
- der Ablehnungsbereich K,
- die Hypothesen H_0 und H_1.

Gesucht sind dann die Fehlerwahrscheinlichkeiten

$$\alpha = \sup_{p \in H_0} \text{Pr}_p[T \in K] \qquad \text{und} \qquad \beta = \sup_{p \in H_1} \text{Pr}_p[T \notin K].$$

Tests zum Improvisieren

Erinnerung:

- H_0 und H_1 sind bei diesen Tests irgendwelche Aussagen über p, wie z.B. $p \leq 0.3$ oder $0.5 \leq p \leq 0.7$. Alles, was weder zu H_0 noch zu H_1 gehört, ist das, „was ausgeschlossen werden darf“.
- Der Ablehnungsbereich K enthält diejenigen Werte aus dem Wertebereich $W_T = \{0, \ldots, n\}$ von T, die „gegen H_0 sprechen“.
- α und β sind jeweils die größtmöglichen Fehlerwahrscheinlichkeiten für eine Fehlentscheidung:

	H_0 wird angenommen $T \notin K$	H_0 wird abgelehnt $T \in K$
H_0 gilt $p \in H_0$	Richtig $\Pr_p[T \notin K] \geq 1 - \alpha$	Fehler 1. Art $\Pr_p[T \in K] \leq \alpha$
H_1 gilt $p \in H_1$	Fehler 2. Art $\Pr_p[T \notin K] \leq \beta$	Richtig $\Pr_p[T \in K] \geq 1 - \beta$

Tests zum Improvisieren

Situation 1: Die Werte in H_0 sind kleiner als die in H_1:

H_0 muss also abgelehnt werden, wenn T zu groß ist:

$$W_T = \{\underbrace{0, \ldots, k}_{\text{annehmen}}, \underbrace{k+1, \ldots, n}_{\text{ablehnen}}\} \qquad \rightsquigarrow \qquad K = \{k+1, \ldots, n\}.$$

Es folgt:

$$\alpha = \sup_{p \in H_0} \Pr_p[T \in K] = \sup_{p \in H_0} \Pr_p[T > k] = \ldots$$
$$\beta = \sup_{p \in H_1} \Pr_p[T \notin K] = \sup_{p \in H_1} \Pr_p[T \leq k] = \ldots$$

Für p wählt man bei α den größten Wert aus H_0 und bei β den kleinsten Wert aus H_1.

Tests zum Improvisieren

Situation 2: Die Werte in H_0 sind größer als die in H_1:

H_0 muss also abgelehnt werden, wenn T zu klein ist:

$$W_T = \{\underbrace{0, \ldots, k}_{\text{ablehnen}}, \underbrace{k+1, \ldots, n}_{\text{annehmen}}\} \qquad \rightsquigarrow \qquad K = \{0, \ldots, k\}\,.$$

Es folgt:

$$\alpha = \sup_{p \in H_0} \Pr_p[T \in K] = \sup_{p \in H_0} \Pr_p[T \leq k] = \ldots$$
$$\beta = \sup_{p \in H_1} \Pr_p[T \notin K] = \sup_{p \in H_1} \Pr_p[T > k] = \ldots$$

Für p wählt man bei α den kleinsten Wert aus H_0 und bei β den größten Wert aus H_1.

Tests zum Improvisieren

Wie bestimmt man aber $\Pr_p[T \leq k]$ bzw. $\Pr_p[T > k]$?

Auch hier gibt es zwei Situationen:

- Steht in der Aufgabe, dass man approximieren soll, dann muss man den Zentralen Grenzwertsatz anwenden.
- Steht in der Aufgabe nicht, dass man approximieren soll, dann muss man mit der Dichtefunktion der Binomialverteilung exakt rechnen.

Wie das gemacht wird steht auf Folien 2154 und 2155.

Mit Approximation:

Der zentrale Grenzwertsatz kann auf T angewendet werden, weil T die Summe unabhängiger, identisch verteilter Zufallsvariablen ist. Für $\Pr_p[T \leq k]$ erhalten wir:

$$\Pr_p[T \leq k] = \Pr_p\left[\frac{T - \mathbb{E}[T]}{\sqrt{\mathrm{Var}[T]}} \leq \frac{k - np}{\sqrt{np(1-p)}}\right] \approx \Phi\left(\frac{k - np}{\sqrt{np(1-p)}}\right).$$

Daraus folgt sofort:

$$\Pr_p[T > k] = 1 - \Pr_p[T \leq k] \approx 1 - \Phi\left(\frac{k - np}{\sqrt{np(1-p)}}\right).$$

Erinnerung: n und k sind immer gegeben und das p wird wie auf Folie 2151 bzw. Folie 2152 gewählt.

Ohne Approximation:

Die Dichtefunktion der Binomialverteilung für $k \in W_T$ lautet:

$$f_T(k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

Mit ihr rechnet man:

$$\Pr_p[T \leq k] = \sum_{i=0}^{k} f_T(i) \qquad \text{und} \qquad \Pr_p[T > k] = \sum_{i=k+1}^{n} f_T(i).$$

Natürlich kann man auch nur einen der beiden Ausdrücke berechnen und den Trick $\Pr_p[T \leq k] + \Pr_p[T > k] = 1$ für den anderen benutzen.

Erinnerung (nochmal): n und k sind immer gegeben und das p wird wie auf Folie 2151 bzw. Folie 2152 gewählt.

Info

Hier sind ein paar gute Aufgaben zum Üben.

1. Endtermklausur 2005, Aufgabe 5 (Teilaufgaben (b) und (c))
2. Wiederholungsklausur 2005, Aufgabe 9 (Teilaufgaben (b) und (c), in der Musterlösung ist zwar das Ergebnis richtig, aber die Rechnung falsch.)
3. Endtermklausur 2010, Aufgabe 3 (Teilaufgaben 1. und 3.)
4. Wiederholungsklausur 2010, Aufgabe 7 (identisch zu 2.)
5. Endtermklausur 2014, Aufgabe 6 (Teilaufgabe 2.)
6. Wiederholungsklausur 2014, Aufgabe 6

Auf den folgenden Folien gibt es die Lösungen zu einigen dieser Aufgaben. Ich habe sie alle gleich formatiert, damit ihr die Ähnlichkeit unter ihnen erkennt.

3. Endtermklausur 2005, Aufgabe 5 (Teilaufgaben (b) und (c))

Gegeben sind:

- unabhängige Stichproben $X_1, X_2 \sim \text{Ber}(p)$ mit unbekanntem p,
- die Testgröße $T = X_1 + X_2$ mit $T \sim \text{Bin}(2, p)$,
- die Hypothesen $H_0 : p \geq \frac{2}{3}$ und $H_1 : p \leq \frac{1}{3}$ und
- der Ablehnungsbereich $K = \{0\}$.

Es liegt Situation 2 mit $k = 0$ vor und gesucht sind α und β (bzw. α_1 und α_2) ohne Approximation. Wir erhalten

$$\text{Pr}_p[T \leq 0] = \text{Pr}_p[T = 0] = (1 - p)^2$$

und:

$$\alpha = \sup_{p \geq \frac{2}{3}} \Pr_p[T \leq 0] = \Pr_{\frac{2}{3}}[T \leq 0] = \left(1 - \frac{2}{3}\right)^2 = \frac{1}{9}$$

$$\beta = \sup_{p \leq \frac{1}{3}} \Pr_p[T > 0] = 1 - \Pr_{\frac{1}{3}}[T \leq 0] = 1 - \left(1 - \frac{1}{3}\right)^2 = 1 - \frac{4}{9} = \frac{5}{9}$$

Gegeben sind:

- unabhängige Stichproben $X_1, X_2 \sim \text{Ber}(p)$ mit unbekanntem p,
- die Testgröße $T = X_1 + X_2$ mit $T \sim \text{Bin}(2, p)$,
- die Hypothesen $H_0 : p \leq \frac{1}{3}$ und $H_1 : p \geq \frac{2}{3}$ und
- der Ablehnungsbereich $K = \{2\}$.

Es liegt Situation 1 mit $k = 1$ vor und gesucht sind α und β (bzw. α_1 und α_2) ohne Approximation. Wir erhalten

$$\text{Pr}_p[T > 1] = \text{Pr}_p[T = 2] = p^2$$

und:

$$\alpha = \sup_{p \leq \frac{1}{3}} \mathsf{Pr}_p[T > 1] = \mathsf{Pr}_{\frac{1}{3}}[T > 1] = \left(\frac{1}{3}\right)^2 = \frac{1}{9}$$

$$\beta = \sup_{p \geq \frac{2}{3}} \mathsf{Pr}_p[T \leq 1] = 1 - \mathsf{Pr}_{\frac{2}{3}}[T > 1] = 1 - \left(\frac{2}{3}\right)^2 = \frac{5}{9}$$

5. Endtermklausur 2010, Aufgabe 3 (Teilaufgaben 1. und 3.)

Gegeben sind:

- unabhängige Stichproben $X_1, X_2, X_3, X_4 \sim \text{Ber}(p)$ mit unbekanntem p,
- die Testgröße $T = X_1 + X_2 + X_3 + X_4$ mit $T \sim \text{Bin}(4, p)$,
- die Hypothesen $H_0 : p \leq \frac{1}{4}$ und $H_1 : \frac{1}{4} < p \leq \frac{3}{4}$ und
- der Ablehnungsbereich $K = \{3, 4\}$.

Es liegt Situation 1 mit $k = 2$ vor und gesucht sind α und β ohne Approximation. Wir erhalten

$$\text{Pr}_p[T > 2] = \binom{4}{3} p^3(1-p) + \binom{4}{4} p^4 = 4p^3(1-p) + p^4 = 4p^3 - 3p^4$$

und:

$$\alpha = \sup_{p \leq \frac{1}{4}} \mathrm{Pr}_p[T > 2] = \mathrm{Pr}_{\frac{1}{4}}[T > 2] = \left(\frac{1}{16} - \frac{3}{256}\right) = \frac{13}{256}$$

$$\beta = \sup_{\frac{1}{4} < p \leq \frac{3}{4}} \mathrm{Pr}_p[T \leq 2] = \mathrm{Pr}_{\frac{1}{4}}[T \leq 2] = 1 - \left(\frac{1}{16} - \frac{3}{256}\right) = 1 - \frac{13}{256} = \frac{243}{256}$$

Gegeben sind:

- unabhängige Stichproben $X_1, \ldots, X_{12} \sim \text{Ber}(p)$ mit unbekanntem p,
- die Testgröße $T = X_1 + \ldots + X_{12}$ mit $T \sim \text{Bin}(12, p)$,
- die Hypothesen $H_0 : p \geq \frac{3}{4}$ und $H_1 : p \leq \frac{1}{4}$ und
- der Ablehnungsbereich $K = \{0, \ldots, 6\}$.

Es liegt Situation 2 mit $k = 6$ vor und gesucht sind α und β mit Approximation. Wir erhalten

$$\text{Pr}_p[T \leq 6] = \text{Pr}_p\left[\frac{T - \mathbb{E}[T]}{\sqrt{\text{Var}[T]}} \leq \frac{6 - 12p}{\sqrt{12p(1-p)}}\right] \approx \Phi\left(\frac{6 - 12p}{\sqrt{12p(1-p)}}\right)$$

und:

$$\alpha = \sup_{p \geq \frac{3}{4}} \mathrm{Pr}_p[T \leq 6] = \mathrm{Pr}_{\frac{3}{4}}[T \leq 6] = \Phi(-2) = 1 - \Phi(2) \approx 1 - 0.9772 = 0.0228$$

$$\beta = \sup_{p \leq \frac{1}{4}} \mathrm{Pr}_p[T > 6] = 1 - \mathrm{Pr}_{\frac{1}{4}}[T \leq 6] = 1 - \Phi(2) \approx 1 - 0.9772 = 0.0228$$

7. Endterm 2014, Aufgabe 6 (Teilaufgabe 2.)

Gegeben sind:

- unabhängige Stichproben $X_1, X_2, X_3 \sim \text{Ber}(p)$ mit unbekanntem p,
- die Testgröße $S = X_1 + X_2 + X_3$ mit $S \sim \text{Bin}(3, p)$,
- die Hypothese $H_0 : p \leq \frac{1}{5}$ und
- der Ablehnungsbereich $K = \{2, 3\}$.

Es liegt Situation 1 mit $k = 1$ vor und gesucht ist α (bzw. α_1) ohne Approximation. Wir erhalten

$$\text{Pr}_p[S \leq 1] = \binom{3}{0}(1-p)^3 + \binom{3}{1}p(1-p)^2 = (1-p)^3 + 3p(1-p)^2 = (1+2p)(1-p)^2$$

und:

$$\alpha = \sup_{p \leq \frac{1}{5}} \text{Pr}_p[S > 1] = 1 - \text{Pr}_{\frac{1}{5}}[S \leq 1] = 1 - \frac{112}{125} = \frac{13}{125}$$

Info

Es gibt aber auch ein paar Aufgaben bei denen man zusätzlich ein bisschen überlegen muss:

1. Endtermklausur 2006, Aufgabe 5 (Teilaufgabe 2.)
2. Endtermklausur 2014, Aufgabe 6 (Teilaufgabe 3.)

Zu diesen Aufgaben gibt es hier auch Lösungen, damit ihr merkt, dass sie alles andere als schwierig sind :-)

1. Endtermklausur 2006, Aufgabe 5 (Teilaufgabe 2.)

Hier ist die Testgröße zwar nicht Binomialverteilt, aber trotzdem funktioniert die Aufgabe analog zu den anderen!

Gegeben sind:

- die Testgröße T mit $W_T = \{1, 2, 3, 4\}$, $f_T(1) = q$, $f_T(2) = \frac{q}{2}$ und $f_T(3) = \frac{q}{3}$,
- die Hypothese $H_0 : q \geq \frac{1}{4}$ und
- der Ablehnungsbereich $K = \{4\}$.

Gesucht ist nur α. Wir erhalten $f_T(4) = 1 - \left(q + \frac{q}{2} + \frac{q}{3}\right) = 1 - \frac{11}{6}q$ und:

$$\alpha = \sup_{q \geq \frac{1}{4}} \Pr_q[T \in K] = \sup_{q \geq \frac{1}{4}} \Pr_q[T = 4] = \sup_{q \geq \frac{1}{4}} \left(1 - \frac{11}{6}q\right) \overset{(*)}{=} \frac{13}{24}$$

Die Überlegung an der Stelle $(*)$ ist, dass $1 - \frac{11}{6}q$ maximiert werden soll, d.h. p muss so klein wie möglich gewählt werden. Weil aber $p \geq \frac{1}{4}$ gelten muss, wählt man einfach $p = \frac{1}{4}$.

2. Endterm 2014, Aufgabe 6 (Teilaufgabe 3.)

Gegeben sind:

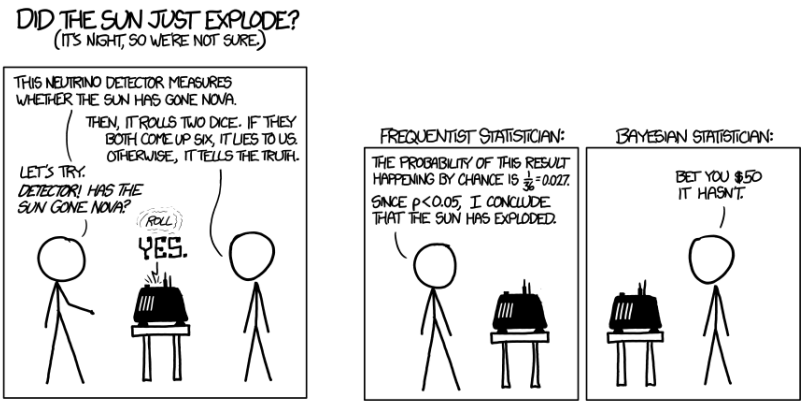
- unabhängige Stichproben $X_1, X_2, X_3 \sim \text{Ber}(p)$ mit unbekanntem p,
- die Testgröße $S = X_1 + X_2 + X_3$ mit $S \sim \text{Bin}(3, p)$,
- die Hypothesen $H_0 : p \leq \frac{1}{5}$ und $H_1 : p > \frac{1}{5}$ und
- der Ablehnungsbereich $K = \emptyset$.

Es liegt hier eine Art Situation 1 mit $k = 3$ vor, aber das ist für diese Aufgabe nicht mehr wichtig. Gesucht ist β (bzw. α_2). Wir erhalten:

$$\beta = \sup_{p > \frac{1}{5}} \text{Pr}_p[S \notin K] = \sup_{p > \frac{1}{5}} \overbrace{\text{Pr}_p[S \notin \emptyset]}^{=1} = 1$$

Hier hat man die Überlegung gebraucht, dass das Ereignis „$S \in \emptyset$“ unmöglich ist.

Frequentists vs. Bayesians



Quelle: `xkcd.com/1132`.

Themenübersicht

Themenübersicht

Markov-Ketten

Eine endliche Markov-Kette M besteht aus:

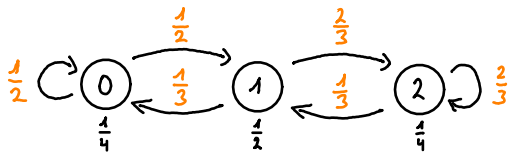
- einer Zustandsmenge $S = \{0, \ldots, n-1\}$ bzw. $S = \mathbb{N}_0$,
- einer Übergangsmatrix

$$P = \begin{pmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,n-1} \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-1} \\ \vdots & \vdots & & \vdots \\ p_{n-1,0} & p_{n-1,1} & \cdots & p_{n-1,n-1} \end{pmatrix}$$

  mit Zeilensummen 1

- und einer Startverteilung $q_0 = (s_0, \ldots, s_{n-1})$ mit $s_0, \ldots, s_{n-1} \geq 0$ und $s_0 + \ldots + s_{n-1} = 1$

- Man kann Markov-Ketten graphisch als gerichtete Graphen mit Kantengewichten $p_{i,j}$ und Knotengewichten s_i darstellen. Beispielsweise entspricht der Graph



einer Markov-Kette mit Zustandsmenge $S = \{0, 1, 2\}$, Übergangsmatrix

$$P = \begin{pmatrix} 1/2 & 1/2 & 0 \\ 1/3 & 0 & 2/3 \\ 0 & 1/3 & 2/3 \end{pmatrix}$$

und Startverteilung $q_0 = \left(\frac{1}{4}, \frac{1}{2}, \frac{1}{4}\right)$.

Infos

- Mit Markov-Ketten definiert man eine Folge von Zufallsvariablen $X_0, X_1, X_2, \ldots$ mit $W_{X_t} = S$ und $p_{i,j} = \Pr[X_{t+1} = j \mid X_t = i]$ für alle $t \in \mathbb{N}_0$.
- Intuitiv gibt X_t den Zustand an, in dem sich der Prozess nach t Zeitschritten befindet.
- Die Markov-Bedingung

$$\Pr[X_{t+1} = i_{t+1} \mid X_t = i_t, \ldots, X_0 = i_0] = \Pr[X_{t+1} = i_{t+1} \mid X_t = i_t]$$

  besagt, dass der Wert von X_{t+1} nur von X_t und nicht von $X_{t-1}, \ldots, X_0$ abhängig ist.
- Ein Zustand i heißt absorbierend, falls $p_{i,i} = 1$ gilt, d.h. wenn er niemals verlassen wird.
- Eine visuelle Erklärung zu Markov-Ketten findet man z.B. hier:
  `http://setosa.io/blog/2014/07/26/markov-[]chains/index.html`

Wahrscheinlichkeiten bei Markov-Ketten

Der zugrunde liegende Wahrscheinlichkeitsraum $W = (\Omega, \Pr)$ einer Markov-Kette M besteht für ein beliebiges $t_0 \in \mathbb{N}$, aus

$$\Omega = \{(x_0, \ldots, x_{t_0}) \mid x_0, \ldots, x_{t_0} \in S\}$$

und Pr mit

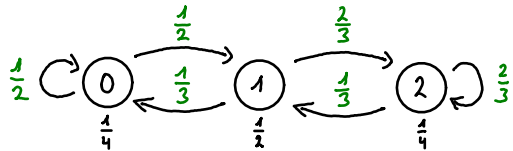
$$\Pr[(x_0, \ldots, x_{t_0})] = s_{x_0} \cdot \prod_{i=1}^{t_0} p_{x_{i-1}, x_i}$$

für alle $(x_0, \ldots, x_{t_0}) \in \Omega$.

Dabei ist s_{x_0} die x_0-te Komponente der Startverteilung q_0 und p_{x_{i-1}, x_i} die Übergangswahrscheinlichkeit vom Zustand x_{i-1} zum Zustand x_i.

Beispiel

Bei der folgenden Markov-Kette



gilt beispielsweise für $t_0 = 3$:

$$\begin{array}{lcccl} \Pr[(1,0,1,2)] & = & \frac{1}{2} \cdot \frac{1}{3} \cdot \frac{1}{2} \cdot \frac{2}{3} & = & \frac{1}{18}, \\ \Pr[(0,0,0,0)] & = & \frac{1}{4} \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} & = & \frac{1}{32}, \\ \Pr[(0,2,1,0)] & = & \frac{1}{4} \cdot 0 \cdot \frac{1}{3} \cdot \frac{1}{3} & = & 0. \end{array}$$

Verteilung von X_t

Die Verteilung von X_t wird für jedes $t \in \mathbb{N}_0$ als Zeilenvektor kodiert. Es gilt:

$$q_t = (\Pr[X_t = 0], \Pr[X_t = 1], \ldots, \Pr[X_t = n-1]),$$

falls die Markov-Kette endlich ist bzw.

$$q_t = (\Pr[X_t = 0], \Pr[X_t = 1], \Pr[X_t = 2], \ldots),$$

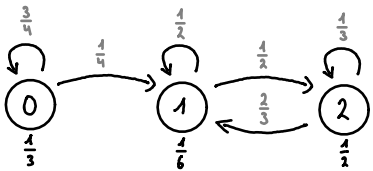
falls sie unendlich ist.

Sei M eine Markov-Kette mit Übergangsmatrix

$$P = \begin{pmatrix} 3/4 & 1/4 & 0 \\ 0 & 1/2 & 1/2 \\ 0 & 2/3 & 1/3 \end{pmatrix}$$

und Startverteilung $q_0 = \left(\frac{1}{3}, \frac{1}{6}, \frac{1}{2}\right)$.

Graphisch:



Was ist q_1?

Für alle $k \in \{0,1,2\}$ gilt nach dem Satz der totalen Wahrscheinlichkeit:

$$\begin{aligned} \Pr[X_1 = k] &= \Pr[X_1 = k | X_0 = 0 \cdot \Pr[X_0 = 0] \quad + \\ &\quad \Pr[X_1 = k | X_0 = 1 \cdot \Pr[X_0 = 1] \quad + \\ &\quad \Pr[X_1 = k | X_0 = 2 \cdot \Pr[X_0 = 2]. \end{aligned}$$

D.h.:

$$\begin{aligned} \Pr[X_1 = k] &= p_{0,k} \cdot s_0 + p_{1,k} \cdot s_1 + p_{2,k} \cdot s_2 \\ &= p_{0,k} \cdot \tfrac{1}{3} + p_{1,k} \cdot \tfrac{1}{6} + p_{2,k} \cdot \tfrac{1}{2}. \end{aligned}$$

Daraus folgt:

$$q_1 = \left(\tfrac{3}{4} \cdot \tfrac{1}{3} + 0 \cdot \tfrac{1}{6} + 0 \cdot \tfrac{1}{2}, \tfrac{1}{4} \cdot \tfrac{1}{3} + \tfrac{1}{2} \cdot \tfrac{1}{6} + \tfrac{2}{3} \cdot \tfrac{1}{2}, 0 \cdot \tfrac{1}{3} + \tfrac{1}{2} \cdot \tfrac{1}{6} + \tfrac{1}{3} \cdot \tfrac{1}{2}\right) = \left(\tfrac{1}{4}, \tfrac{1}{2}, \tfrac{1}{4}\right).$$

Allgemein gilt:

$$q_{t+1} = q_t \cdot P.$$

Stationäre Verteilungen

Wir interessieren uns für die zeitliche Entwicklung

$$q_0 \rightsquigarrow q_1 \rightsquigarrow q_2 \rightsquigarrow q_3 \rightsquigarrow q_4 \rightsquigarrow \dots$$

von q_t.

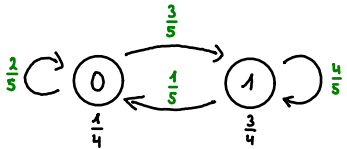
- Für jede Verteilung q_t gilt:
$$q_{t+1} = q_t \cdot P.$$
- Eine Verteilung π heißt stationär, falls gilt:
$$\pi = \pi \cdot P.$$

Wird also zum Zeitpunkt t eine stationäre Verteilung $\pi = q_t$ erreicht, dann bleibt die Verteilung unverändert. Es gilt dann:

$$\pi = q_t = q_{t+1} = q_{t+2} = q_{t+3} = \dots$$

Beispiel

Sei M folgende Markov-Kette:



Für eine stationäre Verteilung $\pi = (\pi_0, \pi_1)$ von M soll gelten:

$$(\pi_0, \pi_1) = (\pi_0, \pi_1) \cdot \begin{pmatrix} 2/5 & 3/5 \\ 1/5 & 4/5 \end{pmatrix}.$$

Es entsteht folgendes Gleichungssystem

$$\pi_0 = \tfrac{2}{5}\pi_0 + \tfrac{1}{5}\pi_1, \quad \pi_1 = \tfrac{3}{5}\pi_0 + \tfrac{4}{5}\pi_1, \quad \pi_0 + \pi_1 = 1$$

mit eindeutiger Lösung $\pi_0 = \frac{1}{4}$ und $\pi_1 = \frac{3}{4}$.

Infos

- Jede endliche Markov-Kette besitzt mindestens eine stationäre Verteilung.
- Die stationäre Verteilungen einer Markov-Kette sind nicht von der Startverteilung q_0 abhängig!
- Ob die Verteilung der Markov-Kette gegen eine stationäre Verteilung konvergiert oder nicht kann wiederum schon von q_0 abhängig sein.

Übergangs- und Rückkehrzeit

Folgende Zufallsvariablen werden wir öfters benutzen:

$$\begin{aligned} T_{i,j} &:= \min\{n \geq 0 \,|\, X_0 = i \text{ und } X_n = j\}, \\ T_i &:= \min\{n \geq 1 \,|\, X_0 = i \text{ und } X_n = i\}. \end{aligned}$$

$T_{i,j}$ ist die Übergangszeit von i nach j und T_i die Rückkehrzeit von i wieder zurück zu sich selbst.

Ankunfts- und Rückkehrwahrscheinlichkeiten

Die Ankunfts- bzw. Rückkehrwahrscheinlichkeiten $f_{i,j}$ bzw. f_i sind definiert als:

$$\begin{aligned} f_{i,j} &:= \Pr[T_{i,j} < \infty], \\ f_i &:= \Pr[T_i < \infty]. \end{aligned}$$

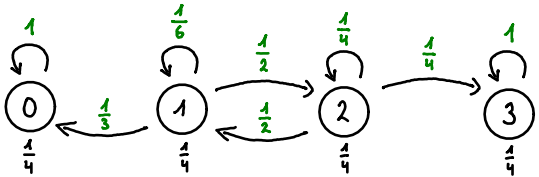
Für sie gilt:

$$f_{i,j} = \sum_{k \in S} p_{i,k} \cdot f_{k,j} \qquad \text{und} \qquad f_i = \sum_{k \in S} p_{i,k} \cdot f_{k,i} \qquad \text{mit} \qquad f_{i,i} = 1.$$

Ist i absorbierend, dann gilt $f_{i,j} = 0$ für alle $j \neq i$.

Beispiel

Was ist $f_{1,3}$ in folgender Markov-Kette?



Es gilt das Gleichungssystem

$$\begin{aligned} f_{0,3} &= 0, \\ f_{1,3} &= \tfrac{1}{3} f_{0,3} + \tfrac{1}{6} f_{1,3} + \tfrac{1}{2} f_{2,3}, \\ f_{2,3} &= \tfrac{1}{2} f_{1,3} + \tfrac{1}{4} f_{2,3} + \tfrac{1}{4} f_{3,3}, \\ f_{3,3} &= 1. \end{aligned}$$

Dieses besitzt die eindeutige Lösung $f_{0,3} = 0$, $f_{1,3} = \frac{1}{3}$, $f_{2,3} = \frac{5}{9}$ und $f_{3,3} = 1$.

Erwartete Übergangs- bzw. Rückkehrzeiten

Die erwartete Übergangs- bzw. Rückkehrzeiten $h_{i,j}$ bzw. h_i sind definiert als:

$$\begin{aligned} h_{i,j} &:= \mathbb{E}[T_{i,j}], \\ h_i &:= \mathbb{E}[T_i]. \end{aligned}$$

Für sie gilt:

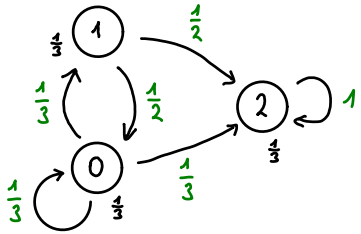
$$h_{i,j} = 1 + \sum_{k \in S} p_{i,k} \cdot h_{k,j} \qquad \text{und} \qquad h_i = 1 + \sum_{k \in S} p_{i,k} \cdot h_{k,i} \qquad \text{mit} \qquad h_{i,i} = 0.$$

Ist i absorbierend, dann gilt $h_{i,j} = \infty$ für alle $j \neq i$.

Übrigens: $h_{i,j}$ bzw. h_i existieren genau dann, wenn gilt: $f_{i,j} = 1$ bzw. $f_i = 1$.

Beispiel

Was ist $h_{0,2}$ in folgender Markov-Kette?



Es gilt das Gleichungssystem

$$\begin{aligned} h_{0,2} &= 1 + \tfrac{1}{3}h_{0,2} + \tfrac{1}{3}h_{1,2} + \tfrac{1}{3}h_{2,2}, \\ h_{1,2} &= 1 + \tfrac{1}{2}h_{0,2} + \tfrac{1}{2}h_{2,2}, \\ h_{2,2} &= 0. \end{aligned}$$

Dieses besitzt die eindeutige Lösung $h_{0,2} = \frac{8}{3}$, $h_{1,2} = \frac{7}{3}$ und $h_{2,2} = 0$.

Eigenschaften von Zuständen

Ein Zustand i einer Markov-Kette heißt:

- transient, falls $f_i < 1$ gilt, d.h. wenn die Möglichkeit besteht, dass der Zustand nie wieder besucht wird.
- rekurrent, falls $f_i = 1$ gilt, d.h. wenn der Zustand immer wieder besucht wird.

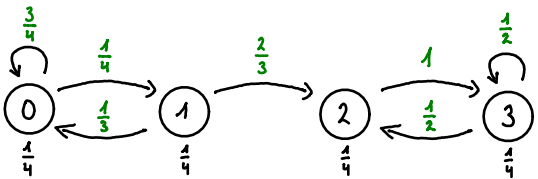
Jeder Zustand ist entweder transient oder rekurrent.

Info

Jeder absorbierende Zustand ist automatisch rekurrent.

Beispiel

Sei M folgende Markov-Kette:



Die Zustände 0 und 1 sind transient. 2 und 3 sind dagegen rekurrent.

Mit den Formeln aus Folie 2184 kann man sogar die konkreten Werte berechnen. Wir erhalten: $f_0 = \frac{5}{6}$, $f_1 = \frac{1}{3}$, $f_2 = 1$ und $f_3 = 1$.

Periodizität

Die Periode ξ („Xi“, manchmal auch $d(i)$) eines Zustands i ist definiert als

$$\xi := \mathrm{ggT}\left\{ n \in \mathbb{N} \,\middle|\, p_{i,i}^{(n)} > 0 \right\},$$

wobei $p_{i,i}^{(n)} = \Pr[X_n = i | X_0 = i]$ die Wahrscheinlichkeit ist, dass man in n Schritten von Zustand i wieder zu sich selbst kommt.

Intuitiv ist die Periode von i der größte gemeinsame Teiler der Längen aller möglichen Pfaden von i zu sich selbst. Gibt es gar keinen Pfad von i zu sich selbst, dann setzt man für die Periode ∞.

Ein Zustand mit Periode $\xi = 1$ heißt aperiodisch.

Infos

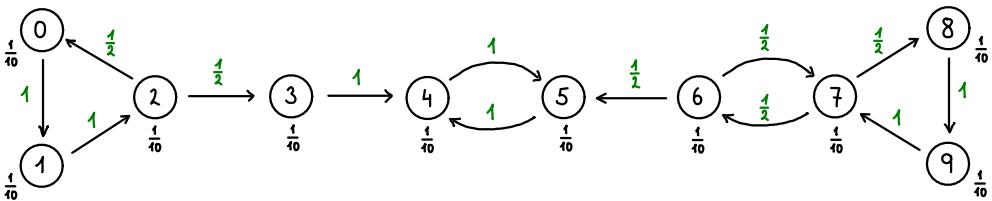
Ein Zustand i ist auf jeden Fall aperiodisch, falls:

- der Graph zwei Pfade von i zu sich selbst enthält, deren Längen l_1 und l_2 teilerfremd zueinander sind (z.B. falls $l_2 = l_1 + 1$), oder
- der Knoten i im Graph eine Schleife besitzt.

Diese Spezialfälle sind meistens völlig ausreichend.

Beispiel

Sei M folgende Markov-Kette.



Dann besitzen die Zustände von M folgende Perioden.

Zustand	0	1	2	3	4	5	6	7	8	9
Periode	3	3	3	∞	2	2	1	1	1	1

Eigenschaften von Markov-Ketten

Eine Markov-Kette M heißt:

- irreduzibel, falls jeder Zustand in M von jedem anderen in endlich vielen Schritten erreichbar ist.
- aperiodisch, falls jeder Zustand aperiodisch ist.
- ergodisch, falls M irreduzibel und aperiodisch ist.

Wichtige Aussagen

Für eine irreduzible, endliche Markov-Kette M gilt:

- M besitzt eine eindeutige stationäre Verteilung π und es gilt:

$$\pi = \left(\frac{1}{h_1}, \ldots, \frac{1}{h_n}\right) .$$

- Falls die Übergangsmatrix von M doppelstochastisch ist, dann gilt $\pi = \left(\frac{1}{n}, \ldots, \frac{1}{n}\right)$, wobei n die Anzahl der Zustände ist.
- Besitzt M mindestens eine Schleife (d.h. $p_{i,i} > 0$ für mindestens ein $i \in S$), dann ist M automatisch aperiodisch und somit ergodisch.

Für eine ergodische, endliche Markov-Kette M gilt:

- Die Verteilung q_t von M konvergiert, unabhängig von der Startverteilung, gegen die eindeutige stationäre Verteilung π, d.h.:

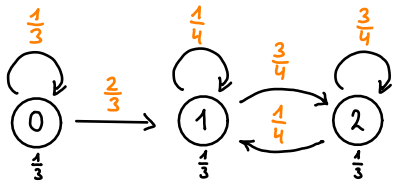
$$\lim_{t \to \infty} q_t = \pi.$$

Infos

- Die Aussagen

$$M \text{ irreduzibel} \implies M \text{ besitzt eine eindeutige stationäre Verteilung}$$
$$M \text{ ergodisch} \implies M \text{ konvergiert gegen die eindeutige stationäre Verteilung}$$

sind Implikationen und keine Äquivalenzen! Eine Markov-Kette kann beispielsweise eine eindeutige stationäre Verteilung besitzen ohne irreduzibel zu sein, z.B.:



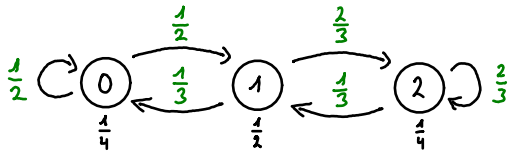
Diese Markov-Kette ist nicht irreduzibel und trotzdem besitzt sie die eindeutige stationäre Verteilung $\pi = \left(0, \frac{1}{4}, \frac{3}{4}\right)$.

- Eine Matrix P ist doppelstochastisch, wenn sowohl die Zeilensummen als auch die Spaltensummen 1 ergeben, z.B.:

$$P = \begin{pmatrix} 0.2 & 0.3 & 0.5 \\ 0.3 & 0.6 & 0.1 \\ 0.5 & 0.1 & 0.4 \end{pmatrix}, \quad P = \begin{pmatrix} 0.7 & 0.2 & 0.1 \\ 0.1 & 0.7 & 0.2 \\ 0.2 & 0.1 & 0.7 \end{pmatrix} \quad \text{oder} \quad P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Beispiel

Folgende Markov-Kette ist irreduzibel:



Für ihre eindeutige stationäre Verteilung $\pi = (\pi_0, \pi_1, \pi_2)$ soll gelten:

$$(\pi_0, \pi_1, \pi_2) = (\pi_0, \pi_1, \pi_2) \cdot \begin{pmatrix} 1/2 & 1/2 & 0 \\ 1/3 & 0 & 2/3 \\ 0 & 1/3 & 2/3 \end{pmatrix}.$$

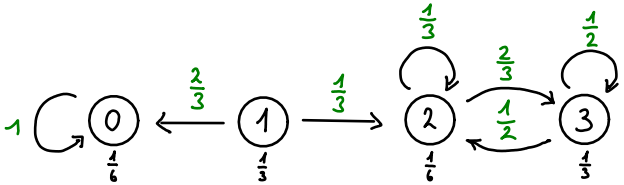
Es entsteht ein lineares Gleichungssystem mit folgenden Gleichungen:

$$\pi_0 = \tfrac{1}{2}\pi_0 + \tfrac{1}{3}\pi_1, \quad \pi_1 = \tfrac{1}{2}\pi_0 + \tfrac{1}{3}\pi_2, \quad \pi_2 = \tfrac{2}{3}\pi_1 + \tfrac{2}{3}\pi_2, \quad \pi_0 + \pi_1 + \pi_2 = 1,$$

welches die eindeutige Lösung $\pi_0 = \frac{2}{11},\ \pi_1 = \frac{3}{11},\ \pi_2 = \frac{6}{11}$ besitzt.

Noch ein Beispiel

Folgende Markov-Kette ist nicht irreduzibel:



Für jede stationäre Verteilung $\pi = (\pi_0, \pi_1, \pi_2, \pi_3)$ soll gelten:

$$(\pi_0, \pi_1, \pi_2, \pi_3) = (\pi_0, \pi_1, \pi_2, \pi_3) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2/3 & 0 & 1/3 & 0 \\ 0 & 0 & 1/3 & 2/3 \\ 0 & 0 & 1/2 & 1/2 \end{pmatrix}.$$

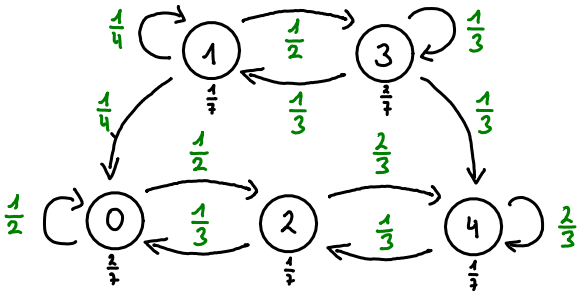
Es entsteht ein Gleichungssystem mit folgenden Gleichungen:

$$\pi_0 = \pi_0 + \tfrac{2}{3}\pi_1, \quad \pi_1 = 0, \quad \pi_2 = \tfrac{1}{3}\pi_1 + \tfrac{1}{3}\pi_2 + \tfrac{1}{2}\pi_3, \quad \pi_3 = \tfrac{2}{3}\pi_2 + \tfrac{1}{2}\pi_3, \quad \pi_0 + \pi_1 + \pi_2 + \pi_3 = 1.$$

Dann ist $\pi = \big(p, 0, \tfrac{3}{7}(1-p), \tfrac{4}{7}(1-p)\big)$ für jedes $p \in [0, 1]$ eine stationäre Verteilung.

Ein letztes Beispiel

Folgende Markov-Kette ist nicht irreduzibel:



Man kann aber trotzdem wie folgt argumentieren, dass diese Markov-Kette eine eindeutige stationäre Verteilung besitzt:

Ein letztes Beispiel

1. Sowohl von Zustand 1 als auch von Zustand 3 werden die Zustände 0, 2 oder 4 mit Wahrscheinlichkeit 1 erreicht.
2. Die Teilkette mit Zuständen 0, 2 und 4 ist irreduzibel und wird nicht verlassen.
3. Demnach muss die Markov-Kette eine eindeutige stationäre Verteilung der Form $\pi = (\pi_0, 0, \pi_2, 0, \pi_4)$ besitzen.

Ein letztes Beispiel

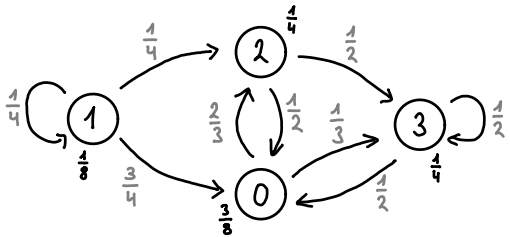
Die stationäre Verteilung π lässt sich dann mithilfe der Übergangsmatrix der Teilkette finden. Es soll gelten:

$$(\pi_0, \pi_2, \pi_4) = (\pi_0, \pi_2, \pi_4) \cdot \begin{pmatrix} 1/2 & 1/2 & 0 \\ 1/3 & 0 & 2/3 \\ 0 & 1/3 & 2/3 \end{pmatrix}$$

wie auf dem vorletzten Beispiel ist die Lösung $\pi_0 = \frac{2}{11}$, $\pi_2 = \frac{3}{11}$ und $\pi_4 = \frac{6}{11}$. Diesmal ist die gesamte stationäre Verteilung

$$\pi = \left(\tfrac{2}{11}, 0, \tfrac{3}{11}, 0, \tfrac{6}{11}\right) \ .$$

Gegeben sei folgende Markov-Kette M:



1. Ist M irreduzibel?
2. Besitzt M eine stationäre Verteilung $\pi = (\pi_0, \pi_1, \pi_2, \pi_3)$?
3. Falls ja, ist sie eindeutig?

Hinweis: Berechne alle stationäre Verteilungen von M!

1. Nein. Der Zustand 1 ist nicht von den Zuständen 0, 2 und 3 erreichbar.
2. Ja. Von Zustand 1 aus werden nämlich die Zustände 0, 2 und 3 mit Wahrscheinlichkeit 1 erreicht und die Teilkette mit Zuständen 0, 2 und 3 ist wohl irreduzibel. Da sie auch nicht verlassen wird, muss die Markov-Kette eine stationäre Verteilung der Form $\pi = (\pi_0, 0, \pi_2, \pi_3)$ besitzen.
3. Ja. Für π soll
$$(\pi_0, \pi_2, \pi_3) = (\pi_0, \pi_2, \pi_3) \cdot \begin{pmatrix} 0 & 2/3 & 1/3 \\ 1/2 & 0 & 1/2 \\ 1/2 & 0 & 1/2 \end{pmatrix}$$
gelten. Es entsteht ein lineares Gleichungssystem mit folgenden Gleichungen:
$$\pi_0 = \tfrac{1}{2}\pi_2 + \tfrac{1}{2}\pi_3, \quad \pi_2 = \tfrac{2}{3}\pi_0, \quad \pi_3 = \tfrac{1}{3}\pi_0 + \tfrac{1}{2}\pi_2 + \tfrac{1}{2}\pi_3, \quad \pi_0 + \pi_2 + \pi_3 = 1,$$
welches die eindeutige Lösung $\pi_0 = \frac{1}{3}$, $\pi_2 = \frac{2}{9}$ und $\pi_3 = \frac{4}{9}$ besitzt.

Themenübersicht

Themenübersicht

Rezept

Frage: Gegeben sind ein Graph $G = (V, E)$ mit Kantengewichten $w : E \to \mathbb{R}_0^+$ und einen Startknoten $s \in V$. Wie findet man den kürzesten Weg von s zu allen anderen Knoten?
Methode Algorithmus von Dijkstra:

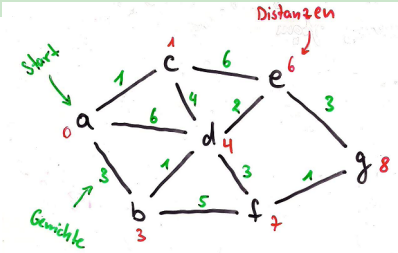
1. Setze $\text{dist}[s] := 0$ und $\text{dist}[v] = \infty$ für alle restlichen Knoten v;
2. Bis alle Knoten markiert sind wiederhole:
3. Bestimme unmarkierten Knoten u mit kleinstem Wert $d(u)$ und markiere es;
4. Für jeden unmarkierten Nachbarn v von u mach:
5. falls $\text{dist}[u] + w(\{u, v\}) < \text{dist}[v]$
6. Setze $\text{dist}[v] := \text{dist}[u] + w(\{u, v\})$ und $\text{pred}[v] = u$;

Am Ende geben $\text{dist}[v]$ die kürzeste Distanz zu einem Knoten v und $\text{pred}[v]$ den Vorgänger von v im kürzesten Weg an.

Info

Der Algorithmus von Dijkstra hat eine Laufzeit von $\mathcal{O}(|V|^2)$.

Beispiel



Protokoll:

	b	c	d	e	f	g
a:	$(3, a)$	$\underline{(1, a)}$	$(6, a)$	–	–	–
c:	$\underline{(3, a)}$		$(5, c)$	$(7, c)$	–	–
b:			$\underline{(4, b)}$	$(7, c)$	$(8, b)$	–
d:				$\underline{(6, d)}$	$(7, d)$	–
e:					$\underline{(7, d)}$	$(9, e)$
f:						$\underline{(8, f)}$

Die kürzeste Distanz von a nach z.B. g ist 8 und der Weg ist $a \to b \to d \to f \to g$.

Themenübersicht

Rezept

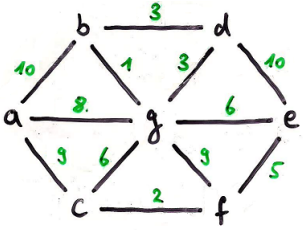
Frage: Gegeben sind ein Graph $G = (V, E)$ mit Kantengewichten $w : E \to \mathbb{R}$. Wie findet man einen Spannbaum mit minimaler Kantengewichtssumme?
Methode Algorithmus von Kruskal:

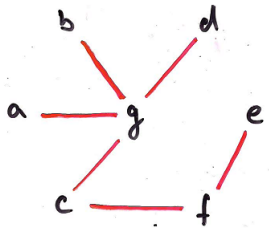
1. Sortiere alle Kanten nach Gewicht;
2. Gehe die Kanten in aufsteigender Reihenfolge durch und für jede Kante mach:
3. falls sie keinen Kreis bildet:
4. füge sie in den Spannbaum hinzu;

Infos

- Der Algorithmus von Kruskal hat eine Laufzeit von $\mathcal{O}(|E| \cdot log|V|)$
- Geht man die Kanten in absteigender Reihenfolge durch, so bekommt man einen Spannbaum mit maximaler Kantengewichtssumme.

Beispiel





Beispiel

Protokoll:

Gewicht	hinzugefügte Kante
1	$\{b, g\}$
2	$\{c, f\}$
3	$\{d, g\}$
5	$\{e, f\}$
6	$\{c, g\}$
8	$\{a, g\}$

Alle minimale Spannbäume haben die Kantensumme $1 + 2 + 3 + 5 + 6 + 8 = 25$.

Themenübersicht

Themenübersicht

Aufgabe

Gib für jede der folgenden regulären Sprachen $L \subseteq \Sigma^*$ einen DFA A mit $L = L(A)$ an.

1. $L = \emptyset$
2. $L = \{\epsilon\}$
3. $L = \{a, b\}^3$
4. $L = \{a, b\}^*$

Aufgabe

Sei $\Sigma = \{a, b\}$ ein zweielementiges Alphabet. Gib für jede der folgenden regulären Sprachen $L \subseteq \Sigma^*$ einen DFA A mit $L = L(A)$ an.

1. $L = \{w \in \Sigma^* \mid |w| \text{ ist gerade}\}$
2. $L = \{w \in \Sigma^* \mid |w|_a \text{ ist gerade}\}$
3. $L = \{w \in \Sigma^* \mid |w|_b \text{ ist durch 3 teilbar}\}$
4. $L = \{w \in \Sigma^* \mid |w|_a \bmod 4 \in \{1, 3\}\}$

Aufgabe

Sei $\Sigma = \{a, b\}$ ein zweielementiges Alphabet. Gib für jede der folgenden regulären Sprachen $L \subseteq \Sigma^*$ einen DFA A mit $L = L(A)$ an.

1. $L = \{w \in \Sigma^* \mid bbb \text{ ist ein Präfix von } w\}$
2. $L = \{w \in \Sigma^* \mid abaa \text{ ist ein Präfix von } w\}$
3. $L = \{w \in \Sigma^* \mid aba \text{ ist ein Teilwort von } w\}$
4. $L = \{w \in \Sigma^* \mid baba \text{ ist ein Teilwort von } w\}$
5. $L = \{w \in \Sigma^* \mid aa \text{ ist ein Suffix von } w\}$
6. $L = \{w \in \Sigma^* \mid abb \text{ ist ein Suffix von } w\}$
7. $L = \{w \in \Sigma^* \mid ab \text{ ist ein Präfix und } ba \text{ ein Suffix von } w\}$
8. $L = \{w \in \Sigma^* \mid abb \text{ ist kein Präfix von } w\}$
9. $L = \{w \in \Sigma^* \mid aba \text{ ist kein Teilwort von } w\}$
10. $L = \{w \in \Sigma^* \mid ab \text{ ist kein Suffix von } w\}$

Aufgabe

Sei $\Sigma = \{a, b\}$ ein zweielementiges Alphabet. Gib für jede der folgenden regulären Sprachen $L \subseteq \Sigma^*$ einen DFA A mit $L = L(A)$ an.

1. $L = \{\epsilon\}$
2. $L = \{w \in \Sigma^* \mid |w| \text{ ist gerade}\}$
3. $L = \{w \in \Sigma^* \mid |w|_a \text{ ist gerade}\}$
4. $L = \{w \in \Sigma^* \mid |w|_b \text{ ist durch 3 teilbar}\}$
5. $L = \{w \in \Sigma^* \mid |w|_a \bmod 4 \in \{1, 3\}\}$
6. $L = \{w \in \Sigma^* \mid bbb \text{ ist ein Präfix von } w\}$
7. $L = \{w \in \Sigma^* \mid abaa \text{ ist ein Präfix von } w\}$
8. $L = \{w \in \Sigma^* \mid aba \text{ ist ein Teilwort von } w\}$
9. $L = \{w \in \Sigma^* \mid baba \text{ ist ein Teilwort von } w\}$

Aufgabe

10. $L = \{w \in \Sigma^* \mid aa \text{ ist ein Suffix von } w\}$
11. $L = \{w \in \Sigma^* \mid abb \text{ ist ein Suffix von } w\}$
12. $L = \{w \in \Sigma^* \mid ab \text{ ist ein Präfix und } ba \text{ ein Suffix von } w\}$
13. $L = \{w \in \Sigma^* \mid abb \text{ ist kein Präfix von } w\}$
14. $L = \{w \in \Sigma^* \mid aba \text{ ist kein Teilwort von } w\}$
15. $L = \{w \in \Sigma^* \mid ab \text{ ist kein Suffix von } w\}$

Aufgabe

Sei $\Sigma = \{a, b\}$ ein zweielementiges Alphabet. Gib für jede der folgenden regulären Sprachen $L \subseteq \Sigma^*$ einen DFA A mit $L = L(A)$ an.

1. $L = \{\epsilon\}$
2. $L = \{w \in \Sigma^* \mid |w| \text{ ist gerade}\}$
3. $L = \{w \in \Sigma^* \mid |w|_a \text{ ist gerade}\}$
4. $L = \{w \in \Sigma^* \mid |w|_b \text{ ist durch 3 teilbar}\}$
5. $L = \{w \in \Sigma^* \mid |w|_a \bmod 4 \in \{1, 3\}\}$
6. $L = \{w \in \Sigma^* \mid bbb \text{ ist ein Präfix von } w\}$
7. $L = \{w \in \Sigma^* \mid abaa \text{ ist ein Präfix von } w\}$
8. $L = \{w \in \Sigma^* \mid aba \text{ ist ein Teilwort von } w\}$
9. $L = \{w \in \Sigma^* \mid baba \text{ ist ein Teilwort von } w\}$

Aufgabe

10. $L = \{w \in \Sigma^* \mid aa \text{ ist ein Suffix von } w\}$
11. $L = \{w \in \Sigma^* \mid abb \text{ ist ein Suffix von } w\}$
12. $L = \{w \in \Sigma^* \mid ab \text{ ist ein Präfix und } ba \text{ ein Suffix von } w\}$
13. $L = \{w \in \Sigma^* \mid abb \text{ ist kein Präfix von } w\}$
14. $L = \{w \in \Sigma^* \mid aba \text{ ist kein Teilwort von } w\}$
15. $L = \{w \in \Sigma^* \mid ab \text{ ist kein Suffix von } w\}$

Gib einen DFA an, das die folgende Sprache L akzeptiert:

$$L = \left\{ x \in \{0,1\}^* \mid [x]_2 \text{ ist durch 3 teilbar} \right\}.$$

Hinweise:

- Für $x \in \{0,1\}^n$ mit $x = x_1 \dots x_n$ ist $[x]_2$ die durch x kodierte Zahl im Dualsystem, d.h.: $[x]_2 = \sum_{i=1}^{n} x_i \cdot 2^i$.
- Beispielsweise gilt: $[011]_2 = 3$, $[1001]_2 = 9$ und $[01011]_2 = 11$ und somit $011, 1001 \in L$ und $01011 \notin L$.

Themenübersicht

Übungsaufgabe

Zeige mithilfe des Pumping-Lemmas, dass folgende Sprachen nicht regulär sind.

1. $L = \{a^m b^m \mid m \geq 5\}$
2. $L = \left\{w \in \{a, b\}^* \mid |w|_a = |w|_b\right\}$
3. $L = \left\{a^l b^m \mid l < m\right\}$
4. $L = \left\{a^l b^m \mid l > m\right\}$
5. $L = \left\{w \in \{a, b\}^* \mid w = w^R\right\}$
6. $L = \left\{a^{2^m} \mid m \in \mathbb{N}\right\}$
7. $L = \left\{a^{m^2} \mid m \in \mathbb{N}\right\}$

Themenübersicht

Themenübersicht

Satz von Rice

Seien $\mathcal{P}$ die Menge aller berechenbaren partiellen Funktionen von Σ^* nach Σ^* und $\mathcal{S}$ eine Teilmenge von $\mathcal{P}$. Dann gilt:

$$L = \{w \in \Sigma^* \mid \varphi_w \in \mathcal{S}\} \text{ entscheidbar } \iff \mathcal{S} = \mathcal{P} \text{ oder } \mathcal{S} = \emptyset.$$