Diskrete Mathematik

Zahlenmengen

$\mathbb{N}$	natürliche Zahlen
$\mathbb{N}^+$	natürliche Zahlen ohne 0
$\mathbb{Z}$	ganze Zahlen
$\mathbb{Q}$	rationale Zahlen
$\mathbb{R}$	reelle Zahlen
$\mathbb{C}$	komplexe Zahlen

Aussagenlogik

Aussage	Ein Satz, der entweder wahr (w) oder falsch (f) ist.
Prädikat	Eine Aussage mit Variablen. n-stellige Prädikate.

Grundidee

Aus gegebenen Prädikaten/Aussagen lassen sich durch Junktoren neue Aussagen bilden. (z. B. Kombinationen mit $\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow$).

Definitionen

- **Negation:** $\neg A$ ist genau dann wahr, wenn A falsch ist. (Doppelte Negation: $A \Leftrightarrow \neg\neg A$.)
- **Konjunktion:** $A \wedge B$ ist wahr genau dann, wenn A und B wahr sind. (assoziativ, kommutativ, idempotent)
- **Disjunktion:** $A \vee B$ ist wahr, wenn mindestens eine der Aussagen wahr ist. (assoziativ, kommutativ, idempotent)
- **Implikation:** $A \Rightarrow B$ ist äquivalent zu $\neg A \vee B$. (Kontraposition: $A \Rightarrow B \Leftrightarrow \neg B \Rightarrow \neg A$.)
- **Äquivalenz:** $A \Leftrightarrow B$ genau dann, wenn $A \Rightarrow B \wedge B \Rightarrow A$.

Wichtige Regeln

- **De Morgan:** $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$
- **Distributivität:** $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
- **Syntaktische Bindung:** $\neg$ bindet stärker als $\wedge, \vee$; diese binden stärker als $\Rightarrow, \Leftrightarrow$.
- **Modus Ponens:** Aus $A \wedge (A \Rightarrow B)$ folgt B.
- **Transitivität:** Aus $(A \Rightarrow B) \wedge (B \Rightarrow C)$ folgt $A \Rightarrow C$.

Hinweis zur Redundanz

Jeder Ausdruck mit den Junktoren $\neg, \wedge, \vee, \Rightarrow$ lässt sich ausschliesslich mit $\neg$ und $\vee$ darstellen. z.B.

$$A \wedge B \Leftrightarrow \neg(\neg A \vee \neg B)$$
$$A \vee B \Leftrightarrow \neg(\neg A \wedge \neg B)$$

Quantoren

Quantoren dienen zur Formalisierung von Aussagen wie:

- $\forall x\, A(x)$: *Für alle x gilt $A(x)$*
- $\exists x\, A(x)$: *Es existiert ein x mit $A(x)$*

Mehrere gleichartige Quantoren:

$$\forall x, y\, A(x,y) \quad \text{statt} \quad \forall x \forall y\, A(x,y)$$

Eingeschränkte Quantoren

$$\forall x \in M\, A(x) : \text{Für alle } x \in M \text{ gilt } A(x)$$
$$\exists x \in M\, A(x) : \text{Es gibt } x \in M \text{ mit } A(x)$$

Auch möglich mit Relationen:

$$\forall x < y\, A(x) \quad \text{oder} \quad \exists x \leq y\, A(x)$$

Als Junktoren

Für endliche Mengen $M = \{x_1, \ldots, x_n\}$ gilt:

$$\forall x \in M\, A(x) \Leftrightarrow A(x_1) \wedge \cdots \wedge A(x_n)$$
$$\exists x \in M\, A(x) \Leftrightarrow A(x_1) \vee \cdots \vee A(x_n)$$

Als Makros

$$\exists x \in M\, A(x) \Leftrightarrow \exists x\, (x \in M \wedge A(x))$$
$$\forall x \in M\, A(x) \Leftrightarrow \forall x\, (x \in M \Rightarrow A(x))$$

Zusammenhang mit Junktoren

$$\neg\forall x\, A(x) \Leftrightarrow \exists x\, \neg A(x) \quad \text{und} \quad \neg\exists x\, A(x) \Leftrightarrow \forall x\, \neg A(x)$$
$$\forall x\, (A(x) \wedge B(x)) \Leftrightarrow (\forall x\, A(x)) \wedge (\forall x\, B(x))$$
$$\exists x\, (A(x) \vee B(x)) \Leftrightarrow (\exists x\, A(x)) \vee (\exists x\, B(x))$$

Leere Quantoren

Wenn x in B nicht vorkommt:

$$\forall x\, B \Leftrightarrow B, \quad \exists x\, B \Leftrightarrow B$$

Mengen

- **Menge / Element:** Eine Menge fasst mathematische Objekte (Elemente) zu einem Ganzen zusammen. Für Menge X und Element y gilt $y \in X$ bzw. $y \notin X$.
- **Aufzählende Schreibweise:** $\{x_1, \ldots, x_n\}$ bezeichnet die Menge, die genau die genannten Elemente enthält. Die leere Menge heisst $\varnothing$.
- **Extensionalitätsprinzip:** Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente haben.
  $$A = B \iff \forall x\, (x \in A \Leftrightarrow x \in B).$$
- **Teilmenge:** $A \subseteq B$ genau dann, wenn $\forall x\, (x \in A \Rightarrow x \in B)$. Ist $A \subseteq B$ und $A \neq B$, so ist A eine *echte* Teilmenge, geschrieben $A \subset B$.
- **Folgerungen:** Mengen sind ungeordnet; Mehrfachaufzählung desselben Elements ändert die Menge nicht. Für jede Menge A gilt $\varnothing \subseteq A$.

Eindeutigkeit der leeren Menge

Seien e_1, e_2 leere Mengen. Dann ist für alle x die Aussage $x \in e_1$ falsch, also ist die Implikation $x \in e_1 \Rightarrow x \in e_2$ wahr; somit $e_1 \subseteq e_2$. Analog $e_2 \subseteq e_1$. Nach Extensionalität folgt $e_1 = e_2$.

Aussonderungsprinzip

Ist A eine Menge und $E(x)$ eine Eigenschaft, dann gilt:

$$\{x \in A \mid E(x)\} = \text{Menge aller } x \in A \text{ mit } E(x).$$
$$a \in \{x \in A \mid E(x)\} \iff a \in A \wedge E(a)$$

Beispiele:

- Gerade Zahlen: $\{x \in \mathbb{N} \mid \exists y \in \mathbb{N}(x = 2y)\}$
- Primzahlen: $\{x \in \mathbb{N} \mid \exists y \in \mathbb{N}(y > 1) \wedge \forall a, b \in \mathbb{N}(ab = x \Rightarrow x = a \vee x = b)\}$

Ersetzungsprinzip

Ist A eine Menge und $t(x)$ ein Ausdruck, so gilt:

$$\{t(x) \mid x \in A\} = \text{Menge aller Werte von } t(x) \text{ mit } x \in A.$$
$$a \in \{t(x) \mid x \in A\} \iff \exists x \in A(a = t(x))$$

Beispiele:

- Quadratzahlen: $\{x^2 \mid x \in \mathbb{N}\}$
- Ungerade Zahlen: $\{2x + 1 \mid x \in \mathbb{N}\}$
- Rationale Zahlen: $\left\{\frac{a}{b} \mid a, b \in \mathbb{Z},\, b \neq 0\right\}$
- Anfangsabschnitte von $\mathbb{N}$: $\{\{x \in \mathbb{N} \mid x < y\} \mid y \in \mathbb{N}\}$

Vereinigung

Die Vereinigung von zwei Mengen beinhaltet genau die Elemente, die in mindestens einer der beiden Mengen enthalten sind:

$$A \cup B := \{x \mid x \in A \vee x \in B\}.$$

Schnitt

Die Schnittmenge von zwei Mengen beinhaltet genau die Elemente, die in beiden Mengen enthalten sind:

$$A \cap B := \{x \mid x \in A \wedge x \in B\}.$$

Allgemeine Vereinigung / Schnitt

Sei I eine beliebige Indexmenge (z. B. $I = \{1, 2, \ldots, n\}$ oder $I = \mathbb{N}$). Für jedes $i \in I$ sei A_i eine Menge.

Allgemeine Vereinigung

x gehört zur Vereinigung genau dann, wenn es in *mindestens einer* der Mengen A_i enthalten ist.

$$\bigcup_{i \in I} A_i := \{\, x \mid \exists i \in I(x \in A_i)\}.$$

Allgemeiner Schnitt

x gehört zum Schnitt genau dann, wenn es in *allen* Mengen A_i enthalten ist.

$$\bigcap_{i \in I} A_i := \{\, x \mid \forall i \in I(x \in A_i)\}.$$

Differenz

Die Differenz von zwei Mengen beinhaltet genau die Elemente, die in der ersten Menge, aber nicht in der zweiten Menge enthalten sind:

$$A \setminus B := \{x \in A \mid x \notin B\}.$$

Disjunkte Mengen

Zwei Mengen A und B heissen disjunkt, wenn sie keine gemeinsamen Elemente besitzen.

$$A \cap B = \varnothing.$$

Paarweise disjunkt

Eine Familie von Mengen $(A_i)_{i \in I}$ heisst paarweise disjunkt, wenn keine zwei verschiedenen Mengen ein gemeinsames Element haben. Es gilt:

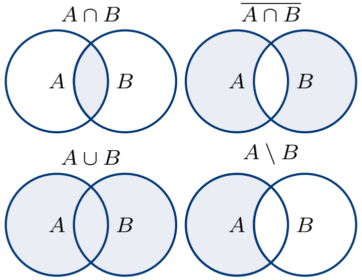
$$\forall i, j \in I\, (i \neq j \Rightarrow A_i \cap A_j = \varnothing).$$

Wichtige Eigenschaften

Für beliebige Mengen A, B, C gelten:

- Idempotenz: $A \cup A = A$, $A \cap A = A$.
- Kommutativität: $A \cup B = B \cup A$, $A \cap B = B \cap A$.
- Assoziativität: $A \cup (B \cup C) = (A \cup B) \cup C$ und analog für $\cap$.
- Teilmengen: $A \subseteq A \cup B$ und $A \cap B \subseteq A$.
- Distributivität:
  $$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
  $$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
- De Morgansche Regeln:
  $$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B),$$
  $$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B).$$

Venn-Diagramm



Potenzmenge

Für eine Menge A bezeichnet die Potenzmenge $\mathcal{P}(A)$ die Menge aller Teilmengen von A:

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

Beispiele:

$$\mathcal{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\},$$
$$\mathcal{P}(\varnothing) = \{\varnothing\},$$
$$\mathcal{P}(\{\{a\}\}) = \{\varnothing, \{\{a\}\}\}.$$

Eigenschaften:

- $A \in \mathcal{P}(A)$ und $\varnothing \in \mathcal{P}(A)$.
- Aus $A \subseteq B$ folgt $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- Für die leere Menge gilt $\mathcal{P}(\varnothing) = \{\varnothing\} \neq \varnothing$.
- $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$
- $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$
- $\mathcal{P}(A)$ einer endlichen Menge mit $|A| = n$ hat $|\mathcal{P}(A)| = 2^n$ Elemente.

Tupel

Ein n-Tupel ist ein *geordneter* Vektor

$$(a_1, \dots, a_n).$$

Der i-te Eintrag eines Tupels $a = (a_1, \dots, a_n)$ wird mit $a[i]$ bezeichnet. Zwei Tupel sind genau dann gleich, wenn sie dieselbe Länge haben und alle entsprechenden Einträge übereinstimmen:

$$(a_1, \dots, a_n) = (b_1, \dots, b_k) \iff n = k \;\wedge\; a_1 = b_1 \;\wedge \dots \wedge a_n = b_k$$

Kartesisches Produkt

Das kartesische Produkt $A_1 \times \dots \times A_n$ ist die Menge aller n-Tupel, deren Einträge aus den Mengen $A_1, \dots, A_n$ stammen.

$$A_1 \times \dots \times A_n := \{(a_1, \dots, a_n) \mid a_i \in A_i \text{ für } 1 \leq i \leq n\}.$$

Besonderheiten:

- Für das n-fache Produkt von A mit sich selbst gilt $A^n := A \times \dots \times A$ (n-mal).
- Für ein kartesisches Produkt von der Form $A_1 \times \dots \times A_n$ wird auch die Kurzschreibweise $\prod_{i=1}^{n} A_i$ verwendet.

Beispiele:

$$\{1\} \times \{a, b\} = \{(1, a), (1, b)\}$$
$$\mathbb{N}^2 = \{(x, y) \mid x \in \mathbb{N} \wedge y \in \mathbb{N}\}$$

Projektionen

Für eine Menge A von n-Tupeln und ist $k \leq n$ eine natürliche Zahl, definiert man die k-te Projektion:

$$\mathrm{pr}_k(A) := \{x[k] \mid x \in A\}.$$

Insbesondere gilt:

$$\mathrm{pr}_k(A_1 \times \dots \times A_n) = A_k.$$

Beispiele:

$$\mathrm{pr}_1(\{1, 2\} \times \{a, b\}) = \{1, 2\}$$
$$\mathrm{pr}_2(\{1, 2\} \times \{a, b\}) = \{a, b\}$$

Relationen

Eine *Relation* von A nach B ist ein Tripel

$$R = (G, A, B)$$

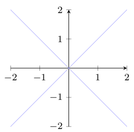
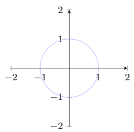
wobei A die Quellmenge, B die Zielmenge und $G \subseteq A \times B$ der *Graph* von R ist. Ist $A = B$, so heisst R *homogen* auf A.

Notation

Sei $R = (G, A, B)$ eine Relation von A nach B.

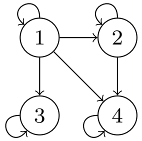
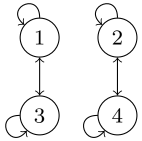
- Ist G der Graph von R, so schreibt man G_R
- Ist $(x, y) \in G$, dann schreibt man xRy (x steht in Relation zu y bezüglich R).
- Sind A und B Teilmengen von $\mathbb{R}$, so kann man R auch als Menge von Punkten in der Ebene darstellen: $\{(x, y) \mid xRy\}$.

$xRy :\Leftrightarrow x^2 = y^2$ $\quad$ $xRy :\Leftrightarrow x^2 + y^2 = 1$

- Als gerichteter Graph: Elemente von A und B als Knoten; für jedes $(x, y) \in G$ ein Pfeil $x \to y$.

$xRy :\Leftrightarrow x$ teilt y $\quad$ $xRy :\Leftrightarrow x + y$ ist gerade

Domäne und Bild

Die Domäne und das Bild einer Relation geben an, welche Elemente der Quell- bzw. Zielmenge tatsächlich in der Relation vorkommen.

$$\mathrm{dom}(R) := \mathrm{pr}_1(G_R) = \{a \in A \mid \exists b \in B (aRb)\}$$
$$\mathrm{im}(R) := \mathrm{pr}_2(G_R) = \{b \in B \mid \exists a \in A (aRb)\}$$

Im gerichteten Graphen entsprechen die Elemente der Domäne den Knoten mit ausgehenden Kanten, die des Bildes den Knoten mit eingehenden Kanten.

Klassifizierungen

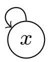
Sei $R \subseteq A \times A$ eine (homogene) Relation auf A.

Reflexivität

Eine Relation R heisst *reflexiv*, wenn jedes Element in Relation zu sich selbst steht:

$$\forall x \in A (xRx)$$

- $\{(a, a) \mid a \in A\} \subseteq R$.
- Im gerichteten Graphen hat jeder Knoten eine Kante zu sich selbst. Für jeden Wert $x \in A$ gilt:



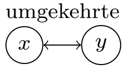
- In der Koordinatendarstellung enthält R die Winkelhalbierende $y = x$.

Symmetrie

Eine Relation R heisst *symmetrisch*, wenn für alle $x, y \in A$ gilt:

$$\forall x, y \; (xRy \Rightarrow yRx).$$

- Zu jedem Pfeil im gerichteten Graph existiert der umgekehrte Pfeil. Für alle $x, y \in A$ gilt:



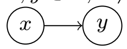
- Symmetrie spiegelt die Koordinatendarstellung an der Geraden $y = x$.

Antisymmetrie

Eine Relation R heisst *antisymmetrisch*, wenn für alle $x, y \in A$ gilt:

$$\forall x, y \; (xRy \wedge yRx \Rightarrow x = y).$$

- Es gibt keine zwei verschiedenen Knoten, die wechselseitig verbunden sind. Für alle $x, y \in A, x \neq y$ gilt:

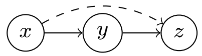


Transitivität

Eine Relation R heisst *transitiv*, wenn für jeden endlichen Pfad ein direkter Pfeil existiert. Für alle $x, y, z \in A$ gilt:

$$\forall x, y, z \; (xRy \wedge yRz \Rightarrow xRz).$$

- Im gerichteten Graphen: Aus $x \to y$ und $y \to z$ folgt $x \to z$. Für alle $x, y, z \in A$ gilt:



Totalität und Eindeutigkeit

Sei $R \subseteq A \times B$ eine Relation von A nach B mit

- **Linksvollständig / linkstotal:** $\mathrm{dom}(R) = A$ (jedes Element in A hat min. eine *ausgehende* Kante).
- **Rechtsvollständig / rechtstotal:** $\mathrm{im}(R) = B$ (jedes Element in B hat min. eine *eingehende* Kante).
- **Linkseindeutig:** $\forall x_1, x_2, y \; (x_1Ry \wedge x_2Ry \Rightarrow x_1 = x_2)$ (jedes Element in B hat max. eine *eingehende* Kante).
- **Rechtseindeutig:** $\forall x, y_1, y_2 \; (xRy_1 \wedge xRy_2 \Rightarrow y_1 = y_2)$ (jedes Element in A hat max. eine *ausgehende* Kante).

Inverse Relationen

Für eine Relation $R = (G, A, B)$ ist die *inverse Relation* definiert durch

$$R^{-1} = (G', B, A), \quad G' := \{(y, x) \mid (x, y) \in G\}.$$

Eigenschaften:

- $(R^{-1})^{-1} = R$
- R ist linksvollständig $\Leftrightarrow$ R^{-1} ist rechtsvollständig
- R ist linkseindeutig $\Leftrightarrow$ R^{-1} ist rechtseindeutig
- Für jede symmetrische Relation R gilt $R = R^{-1}$

Funktionen

Eine *Funktion* f von der Menge A nach B ist eine Relation, die *linksvollständig* und *rechtseindeutig* ist. Man schreibt:

$$f : A \to B,$$

und für jedes $x \in A$ existiert genau ein $y \in B$ mit $y = f(x)$.

Schreibweise

Oft werden Funktionen durch Angabe von Definitions- und Zielmenge sowie einer Zuordnungsvorschrift beschrieben. Beispielsweise gilt:

$$f = (\{(x, x^3) \mid x \in \mathbb{N}\}, \mathbb{N}, \mathbb{N})$$

bzw. äquivalent in der gebräuchlicheren Schreibweise:

$$f : \mathbb{N} \to \mathbb{N}, \quad f(x) = x^3.$$

Injektive Funktionen

Eine Funktion $f : A \to B$ ist *injektiv*, falls die Relation *linksvollständig*, *rechtseindeutig* und zusätzlich *linkseindeutig* ist:

$$\forall x_1, x_2 \in A (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$$
$$\forall x_1, x_2 \in A (x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))$$

Jedes Element in A wird auf ein eigenes unterschiedliches Element in B abgebildet.
Notation: $f : A \hookrightarrow B$.

Umkehrbarkeit

Eine Funktion $f : A \to B$ ist genau dann *umkehrbar*, wenn sie injektiv ist. Dann gilt:

$$f^{-1} : \mathrm{im}(f) \to A.$$
$$(G'_f, \mathrm{im}(f), A), \quad G'_f = \{(y, x) | (x, y) \in G_f\}$$

Surjektivität

Eine Funktion $f : A \to B$ ist *surjektiv*, falls die Relation *linksvollständig*, *rechtseindeutig* und zusätzlich *rechtsvollständig* ist:

$$\mathrm{im}(f) = B$$

Jedes Element in B wird von mindestens einem Element in A erreicht.
Notation: $f : A \twoheadrightarrow B$

Bijektivität

Eine Funktion $f : A \to B$ ist *bijektiv*, wenn sie sowohl injektiv als auch surjektiv ist. Die Umkehrfunktion ist dann definiert durch:

$$f^{-1} : B \to A.$$

J Notation: $f : A \rightleftharpoons B$

Umkehrfunktion

Für eine bijektive Funktion $f : A \rightleftharpoons B$ gilt:

$$f^{-1} \circ f = \mathrm{id}_A, \qquad f \circ f^{-1} = \mathrm{id}_B\,.$$

Komposition

Für $g : A \to B$ und $f : B \to C$ definiert man die *Komposition*:

$$(f \circ g)(x) = f(g(x)), \quad f \circ g : A \to C.$$

Komposition ist *assoziativ*:

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Eigenschaften der Komposition

Für Funktionen $f : A \to B$ und $g : B \to C$ gilt:

- Sind f und g injektiv, dann ist $g \circ f$ injektiv.
- Sind f und g surjektiv, dann ist $g \circ f$ surjektiv.
- Sind f und g bijektiv, dann ist $g \circ f$ bijektiv.

Äquivalenzrelationen

Eine Relation $\sim$ auf einer Menge A heisst *Äquivalenzrelation*, falls sie für alle $x, y, z \in A$ die folgenden Eigenschaften erfüllt:

- **reflexiv:** $x \sim x$,
- **symmetrisch:** $x \sim y \Rightarrow y \sim x$,
- **transitiv:** $x \sim y \wedge y \sim z \Rightarrow x \sim z$.

Beispiele

- Die Gleichheitsrelation $=$ auf jeder Menge.
- Auf $\mathbb{Z}$: $a \equiv_n b :\Leftrightarrow n \mid (a-b)$ (Restklasse modulo n).
- Relation „sitzen in derselben Sitzreihe" in einem Kinosaal.

Klein. und grösst. Äquivalenzrelation

Auf jeder Menge A existiert:

- die *kleinste* Äquivalenzrelation: die Gleichheitsrelation $\{(a, a) \mid a \in A\}$.
- die *grösste* Äquivalenzrelation: das ganze $A \times A$ (alles ist äquivalent).

Äquivalenzklassen und Faktormenge

Für $a \in A$ ist die *Äquivalenzklasse*

$$[a]_\sim := \{x \in A \mid x \sim a\}.$$

Die Menge aller Äquivalenzklassen heisst *Faktormenge* $A/\sim := \{[a]_\sim \mid a \in A\}$. Jedes Element einer Äquivalenzklasse ist ein *Repräsentant* dieser Klasse.

Wichtige Eigenschaften

Für eine Äquivalenzrelation $\sim$ und $a, b \in A$ sind äquivalent:

1. $a \sim b$,
2. $[a]_\sim = [b]_\sim$,
3. $[a]_\sim \cap [b]_\sim \neq \varnothing$,
4. $a \in [b]_\sim$,
5. $b \in [a]_\sim$.

Daraus folgt: Zwei Äquivalenzklassen sind entweder gleich oder disjunkt.

Beispiele in $\mathbb{R}^2$

- $(a, b) \approx (c, d) := a = c$
  Äquivalenzklassen $=$ vertikale Geraden.
- $(a, b) \simeq (c, d) := \sqrt{a^2 + b^2} = \sqrt{c^2 + d^2}$
  Äquivalenzklassen $=$ Kreise um den Ursprung.
- Auf $\mathbb{R}^2 \setminus \{(0, 0)\}$:
  $(a, b) \sim (c, d) := \exists r \in \mathbb{R}(ra, rb) = (c, d)$
  Äquivalenzklassen $=$ Geraden durch den Ursprung.

Partitionen

Eine *Partition* einer Menge A ist eine Menge $\{A_i\}_{i \in I}$ paarweise disjunkter, nichtleerer Teilmengen mit

$$\bigcup_{i \in I} A_i = A.$$

Die A_i nennt man auch *Blöcke* der Partition.

Beispiele

- Gerade und ungerade natürliche Zahlen: $A_0 = \{2n\},\ A_1 = \{2n + 1\}$.
- Einzelmengen $\{n\}$ liefern eine feine Partition.
- Es gibt Partitionen von $\mathbb{N}$ in unendlich viele unendliche Blöcke.

Induzierte Partition

Ist $\sim$ eine Äquivalenzrelation auf A, so sind die Äquivalenzklassen $[a]_\sim$ die Blöcke der Partition $A/\sim$. Insbesondere sind die Klassen nichtleer und paarweise disjunkt.

Induzierte Äquivalenzrelation

Ist $P = \{A_i\}_{i \in I}$ eine Partition von A, definiert

$$a \sim b \quad :\Leftrightarrow \quad \exists i \in I\ (a \in A_i \wedge b \in A_i)$$

eine Äquivalenzrelation auf A mit Quotientenmenge $A/\sim = P$.

Äquivalenzrelationen und Funktionen

Eine Relation $\sim$ auf A ist genau dann eine Äquivalenzrelation, wenn es eine Menge B und eine Abbildung $f\colon A \to B$ gibt, mit der Eigenschaften:

$$x \sim y \quad \Leftrightarrow \quad f(x) = f(y).$$

(Äquivalenzklassen sind dann die Urbilder einzelner Werte von f.)

Halbordnungen

Eine Relation $\preceq$ auf einer Menge A heisst *Halbordnung*, falls sie für alle $x, y, z \in A$ die folgenden Eigenschaften erfüllt:

- **reflexiv:** $x \preceq x$,
- **transitiv:** $x \preceq y \wedge y \preceq z \Rightarrow x \preceq z$,
- **antisymmetrisch:** $x \preceq y \wedge y \preceq x \Rightarrow x = y$.

Typische Beispiele

- $(\mathcal{P}(A), \subseteq)$, die Mengeninklusion auf der Potenzmenge.
- Teilbarkeitsrelation auf $\mathbb{N}$.
- Die üblichen $\leq$-Relationen auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
- Versionen in der Informatik, z. B. Commit-Historien in Git (Ursprungsrelation).

Zyklenfreiheit

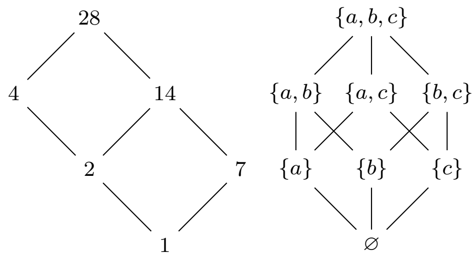
In einer Halbordnung sind echte Zyklen ausgeschlossen: Aus $a_1 \preceq a_2 \preceq \cdots \preceq a_n \preceq a_1$ folgt $a_1 = \cdots = a_n$. Dies folgt aus der Antisymmetrie und der Transitivität.

Hasse-Diagramme

Zur Visualisierung nutzt man Hasse-Diagramme:

- Relative Höhe zeigt die Ordnungsrichtung.
- Kanten werden nur zwischen *benachbarten* Elementen ohne Zwischenelement gezeichnet (Transitivitätskanten weglassen).
- Schleifen entfallen.

Beispiele: Hesse-Diagramm des Poset der Teilbarkeitsrelation auf 28 (*Rechts*) und $(\mathcal{P}(\{a, b, c\}), \subseteq)$ (*Links*):



Spezielle Elemente

Sei $X \subseteq A$ in einer Halbordnung $(A, \preceq)$. Ein Element $x \in X$ heisst:

- **minimales Element:** $\forall y\ (y \preceq x \Rightarrow y = x)$
  (Knoten zu *denen* kein Pfeil zeigt)
- **kleinstes Element:** $\forall y\ (x \preceq y)$
  (Knoten von *dem* ein Pfeil zu jedem anderen zeigt)
- **maximales Element:** $\forall y\ (x \preceq y \Rightarrow y = x)$
  (Knoten von *denen* kein Pfeil ausgeht)
- **grösstes Element:** $\forall y\ (y \preceq x)$
  (Knoten zu *dem* jeder Pfeil zeigt)

Existenz in endlichen Mengen

Ist $X \subseteq A$ nichtleer und endlich, so existiert mindestens ein minimales und mindestens ein maximales Element in X.

Erweiterungen

Eine Halbordnung $(A, \preceq_A)$ erweitert eine Halbordnung $(B, \preceq_B)$, wenn gilt:

$$B \subseteq A,$$

$$\forall a, b \in B (a \preceq_B b \Rightarrow a \preceq_A b).$$

Man sagt: $(A, \preceq_A)$ *erweitert* $(B, \preceq_B)$.

Lineare Ordnungen

Eine *lineare Ordnung* (auch *totale Ordnung*) ist eine Halbordnung $(A, \preceq)$, in der alle Elemente vergleichbar sind:

$$\forall a, b \in A (a \preceq b \vee b \preceq a).$$

Das heisst, es gibt keine *unvergleichbaren* Paare mehr.

Satz von Marczewski–Szpilrajn

Jede Halbordnung $(A, \preceq)$ lässt sich zu einer linearen Ordnung $(A, \trianglelefteq)$ erweitern, die die ursprüngliche Ordnung bewahrt und *alle* Elemente vergleichbar macht.

Graphentheoretische Sicht

- Eine endliche Halbordnung kann als gerichteter azyklischer Graph (DAG) dargestellt werden.
- Eine *Linearisierung* entspricht einer *topologischen Sortierung* des DAGs.

Unendliche Mengen

Zwei Mengen A und B haben dieselbe Mächtigkeit (Kardinalität) $|A| = |B|$, genau dann, wenn eine bijektive Abbildung $f : A \longleftrightarrow B$ existiert. Eine Menge heisst endlich, falls sie bijektiv zu $\{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ ist; andernfalls heisst sie unendlich.

Wichtige Definitionen

- $|A| = |B|$: Existenz einer Bijektion $f : A \to B$.
- $|A| \leq |B|$: Es existiert eine injektive Abbildung $g : A \hookrightarrow B$ (äquivalent: surjektive Abbildung $B \twoheadrightarrow A$).
- $|A| = \infty$: Abkürzung dafür, dass A nicht endlich ist.
- $|\varnothing| \leq |A|$ für alle Mengen A.

Elementare Eigenschaften

- Die Relation $\sim$ mit $A \sim B \Leftrightarrow |A| = |B|$ ist eine Äquivalenzrelation.
- Für endliche Mengen A und B mit $|A| = n$ und $|B| = m$ gilt $|A| \leq |B| \iff n \leq m$.
- Eine Menge A ist genau dann unendlich, wenn $|\mathbb{N}| \leq |A|$.
- $A \subseteq B \Rightarrow |A| \leq |B|$. Umgekehrt: $|A| \leq |B|$ genau dann, wenn es $A' \subseteq B$ mit $|A'| = |A|$ gibt.

Satz von Cantor–Bernstein

Sind A und B nichtleer, dann gilt

$$(|A| \leq |B| \ \wedge\ |B| \leq |A|) \iff |A| = |B|.$$

(Dieser Satz liefert aus beidseitigen Injektionen eine Bijektion.)

Wichtige Folgerungen

- **Schubfachprinzip (Pigeonhole):** Aus $|A| \leq |B|$ und $|A| \neq |B|$ folgt $|B| \not\leq |A|$.
- **Dedekind:** A ist unendlich $\Leftrightarrow$ es existiert eine injektive, nicht surjektive Abbildung $f : A \hookrightarrow A$. z.B. die Abbildung $f : \mathbb{N}, n \mapsto n + 1$.
- **Hilbert's Hotel (Anschaulichkeit):** Eine Menge A ist unendlich genau dann, wenn es eine echte Teilmenge $B \subset A$ mit $|B| = |A|$ gibt.

Abzählbare Mengen

Eine Menge A heisst *abzählbar*, wenn $A = \varnothing$ oder eine der folgenden (äquivalenten) Bedingungen erfüllt ist:

- $|A| \le |\mathbb{N}|$
- Es existiert eine surjektive Funktion $f : \mathbb{N} \twoheadrightarrow A$.
- Es existiert eine injektive Funktion $f : A \hookrightarrow \mathbb{N}$.

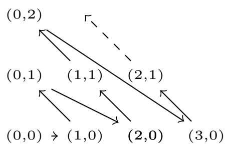
Bemerkung: Ist A abzählbar und unendlich, so gilt $|A| = |\mathbb{N}|$.

Beispiele

- Die leere Menge $\varnothing$ ist abzählbar.
- Jede Teilmenge $A \subseteq \mathbb{N}$ ist abzählbar (insbesondere $\mathbb{N}$ selbst).
- $\mathbb{Z}$ ist abzählbar.
- $\mathbb{Q}$ ist abzählbar (als Schlussfolgerung aus Abzählbarkeit von $\mathbb{Z} \times \mathbb{Z}$ und Quotientenbildung).

Wichtige Aussagen

- Jede endliche Menge ist abzählbar. (Beweis: Aufzählung der Elemente liefert eine surjektive Abbildung $\mathbb{N} \twoheadrightarrow A$.)
- Jede Teilmenge einer abzählbaren Menge ist abzählbar. (Bild- bzw. Einschränkungsargument.)
- Bild einer abzählbaren Menge unter einer surjektiven Abbildung ist abzählbar. (Komposition surjektiver Abbildungen.)
- $\mathbb{N} \times \mathbb{N}$ ist abzählbar. Daraus folgt die Abzählbarkeit von $\mathbb{Z} \times \mathbb{Z}$ und damit $\mathbb{Q}$.



- Jede abzählbare Vereinigung abzählbarer Mengen $\bigcup_{i \in \mathbb{N}} A_i$ ist abzählbar. (Beweisidee: doppelte Indizierung und Aufzählung aller Paare (i, n).)

Überabzählbare Mengen

- Es gibt verschiedene "Grössen" unendlicher Mengen; aus $|A| = \infty$ und $|B| = \infty$ folgt nicht notwendigerweise $|A| = |B|$.
- Es existiert eine unendliche *Hierarchie* von Kardinalitäten: Mengen $A_0, A_1, A_2, \ldots$ mit
$$|A_0| < |A_1| < |A_2| < \ldots$$
- Die Menge aller unendlichen Binärsequenzen $B = \{0,1\}^{\mathbb{N}}$ ist *nicht abzählbar.*

Sequenzen

Eine *Sequenz* in einer Menge A ist eine Abbildung $s : \mathbb{N} \to A$. Die Menge aller Sequenzen in A sei $A^{\mathbb{N}}$. Entspricht $s(0) = a_0$, $s(1) = a_1$, $s(2) = a_2$, …, so schreiben wir
$$s = (a_0, a_1, a_2, \ldots).$$

Unendliche Binärsequenzen

Eine *Binärsequenz* ist eine Funktion $s : \mathbb{N} \to \{0,1\}$. Die Menge aller Binärsequenzen sei $B = \{0,1\}^{\mathbb{N}}$.

Cantors Diagonalisierungsargument

Für jede Abbildung $f : \mathbb{N} \to B$ konstruiere man $s \in B$ durch
$$s_n := 1 - f(n)_n$$
$$\begin{aligned}
f(0) &= (a_0^0, a_1^0, a_2^0, \ldots a_n^0, \ldots) \\
f(1) &= (a_0^1, a_1^1, a_2^1, \ldots a_n^1, \ldots) \\
f(2) &= (a_0^2, a_1^2, a_2^2, \ldots a_n^2, \ldots) \\
&\vdots \\
f(n) &= (a_0^n, a_1^n, a_2^n, \ldots a_n^n, \ldots) \\
&\vdots
\end{aligned}$$

s unterscheidet sich von jedem Bild $f(n)$ in der n-ten Stelle. Somit ist $s \notin \operatorname{im}(f)$ und es gibt keine surjektive Abbildung $\mathbb{N} \to B$. Daher ist B nicht abzählbar.

Folgerungen

- Das Intervall $[0,1)$ und damit $\mathbb{R}$ sind überabzählbar.
- Die Menge aller Funktionen $\mathbb{N} \to \mathbb{N}$ ist überabzählbar.
- Es existieren Funktionen $\mathbb{N} \to \mathbb{N}$, die nicht berechenbar sind.

Potenzmenge und Cantors Theorem

Für jede Menge A gilt streng:
$$|A| < |\mathcal{P}(A)|.$$

Begründung:

1. Es existiert eine Injektion $A \hookrightarrow \mathcal{P}(A)$, $x \mapsto \{x\}$, also $|A| \le |\mathcal{P}(A)|$.
2. Für jede Abbildung $f : A \to \mathcal{P}(A)$ betrachte die Menge
$$\Delta_f := \{a \in A \mid a \notin f(a)\}.$$
$\Delta_f \in \mathcal{P}(A)$, aber $\Delta_f \notin \operatorname{im}(f)$ (diagonalisiertes Argument), also ist f nicht surjektiv. Damit $|\mathcal{P}(A)| \not\le |A|$.

Peano-Axiome

Die Peano-Axiome beschreiben die Grundstruktur der natürlichen Zahlen $\mathbb{N}$:

Axiom 1: $0 \in \mathbb{N}$.

Axiom 2: Zu jeder $k \in \mathbb{N}$ existiert genau ein Nachfolger $k+1 \in \mathbb{N}$ (Nachfolgerfunktion $\eta : \mathbb{N} \to \mathbb{N}, \quad \eta(n) = n+1$).

Axiom 3: 0 ist die einzige Zahl, die kein Nachfolger ist. $\forall n \in \mathbb{N}\ (\forall k \in \mathbb{N}\ (n \ne k+1) \Leftrightarrow n = 0)$

Axiom 4: Die Nachfolgerfunktion $\eta : \mathbb{N} \hookrightarrow \mathbb{N} \setminus \{0\}$ ist injektiv: $n+1 = m+1 \Rightarrow n = m$.

Induktion

Axiom der vollständigen Induktion

Sei $A(n)$ eine Aussage für $n \in \mathbb{N}$. Gilt

- *Induktionsverankerung (I.V.)*: $A(0)$
- *Induktionsschritt (I.S.)*: $\forall n \in \mathbb{N}\ (A(n) \Rightarrow A(n+1))$,

so folgt $\forall n \in (\mathbb{N}\ A(n))$.

Varianten der vollständigen Induktion

Mengeninduktion Für $A \subseteq \mathbb{N}$ gilt: Ist $0 \in A$ und $\forall n \in \mathbb{N} (n \in A \Rightarrow n+1 \in A)$, so ist $A = \mathbb{N}$.

Induktion mit Startwert Für festen $z \in \mathbb{Z}$: Aus $A(z)$ und $\forall n \ge z\ (A(n) \Rightarrow A(n+1))$ folgt $\forall n \ge z\ A(n)$. Dies folgt durch Anwendung der normalen Induktion auf $B(n) := A(n+z)$.

Minimumsprinzip Jede nichtleere Teilmenge $A \subseteq \mathbb{N}$ besitzt ein kleinstes Element. Dieses Prinzip ist äquivalent zum Induktionsprinzip.

Kleinster Verbrecher Beweis per Widerspruch: Existiert eine kleinste n ohne Eigenschaft A, führt dies oft zu einem Widerspruch und damit zum Beweis von $\forall n\ A(n)$.

Starke Induktion Gilt $\forall n \in \mathbb{N}\ \big(\forall m < n\ A(m) \Rightarrow A(n)\big)$, so folgt $\forall n \in \mathbb{N}\ A(n)$. Die starke Induktion ist logisch äquivalent zur gewöhnlichen Induktion.

Absteigende Ketten Es existiert keine unendliche streng absteigende Folge $a_0 > a_1 > a_2 > \ldots$ in $\mathbb{N}$. Andernfalls würde die Menge $\{a_i\}$ kein Minimum besitzen, im Widerspruch zum Minimumsprinzip.

Rekursion

Rekursive Algorithmen folgen dem Prinzip: *Problem* $\to$ in kleinere ähnliche Teilprobleme zerlegen; Basisfälle direkt lösen; Teillösungen rekursiv berechnen und kombinieren.

Rekursive Definitionen

1. Man spezifiziert Basisfälle (einfachste Bestandteile).
2. Man gibt Rekursionsschritte an, die aus bereits definierten (einfacheren) Fällen neue Fälle aufbauen.
3. Die Gesamtheit dieser Regeln definiert das Objekt.

Primitive Rekursion (ohne Parameter)

Seien M eine Menge, $g : M \times \mathbb{N} \to M$ und $c \in M$. Dann existiert eindeutig eine Funktion $f : \mathbb{N} \to M$ mit
$$\begin{aligned} f(0) &= c, \\ f(n+1) &= g(f(n), n). \end{aligned}$$

Primitive Rekursion (mit Parameter)

Sind M, X Mengen, $g : M \times \mathbb{N} \times X \to M$ und $c : X \to M$, so gibt es eindeutig $f : \mathbb{N} \times X \to M$ mit
$$\begin{aligned} f(0, x) &= c(x), \\ f(n+1, x) &= g(f(n,x), n, x) \quad (\forall x \in X). \end{aligned}$$

Wichtige Beispiele (primitive Rekursion)

- **Addition:**
$$\begin{aligned} x + 0 &= x, \\ x + (n+1) &= (x+n) + 1. \end{aligned}$$
- **Multiplikation:**
$$\begin{aligned} x \cdot 0 &= 0, \\ x \cdot (n+1) &= (x \cdot n) + x. \end{aligned}$$
- **Exponentiation:**
$$\begin{aligned} x^0 &= 1, \\ x^{n+1} &= x \cdot x^n. \end{aligned}$$
- **Endliche Summen und Produkte** lassen sich ebenfalls rekursiv definieren (rekursiver Startwert und Schritt).

Zusammenspiel von Rekursion und Induktion

Rekursive Definitionen von Objekten (z.B. Summen, Produkte) erlauben Beweise über deren Eigenschaften (Kommutativität, Assoziativität, etc.) mittels Induktion.

Strukturelle Induktion/Rekursion

Induktive Mengen verallgemeinern die Struktur der natürlichen Zahlen. Statt eines speziellen Grundelements 0 und der Nachfolgerabbildung $\eta(n) = n+1$ betrachtet man:

- eine Menge von *Grundelementen* $A_0 \subseteq M$,
- eine Menge von (n-stelligen) *Regeln* R, wobei jede Regel r eine Funktion $r : M^n \to M$ ist.

Die induktive Menge $N(A_0, R)$ ist die kleinste Teilmenge von M, die A_0 enthält und unter allen Regeln in R abgeschlossen ist.

Abschlussregeln und Abgeschlossenheit

Eine Menge $A \subseteq M$ ist *unter einer Regel* $r : M^n \to M$ abgeschlossen, falls
$$(x_1, \ldots, x_n) \in A^n \ \Rightarrow\ r(x_1, \ldots, x_n) \in A.$$

Ist R eine Menge von Regeln, so ist A unter R abgeschlossen, wenn sie unter jeder Regel in R abgeschlossen ist. Beispiele:

- $\mathbb{N}$ ist abgeschlossen unter $\{+, \cdot\}$.
- $\mathbb{Z}$ ist abgeschlossen unter $\{+, -, \cdot\}$.
- Die Menge der geraden Zahlen ist abgeschlossen unter $\{+, -, \cdot\}$.

Existenz und Eindeutigkeit

Für gegebene M, $A_0 \subseteq M$ und Regelmenge R existiert eine eindeutige kleinste Menge
$$N(A_0, R) := \bigcap \{A \subseteq M \mid A_0 \subseteq A \wedge A \text{ ist abg. unter } R\},$$
die alle Grundelemente enthält und unter R abgeschlossen ist.

Strukturelle Induktion

Um eine Eigenschaft $P(x)$ für alle $x \in N(A_0, R)$ zu beweisen, reicht es zu zeigen:

(a) Für alle Grundelemente $a \in A_0$ gilt $P(a)$.

(b) Für jede Regel $f \in R$ mit k Argumenten aus $P(x_1), \dots, P(x_k)$ folgt $P(f(x_1, \dots, x_k))$.

Dann gilt $P(x)$ für alle $x \in N(A_0, R)$.

Strukturelle Rekursion

Strukturelle Rekursion definiert Funktionen auf $N(A_0, R)$ durch Angabe:

- Werte für alle Grundelemente $a \in A_0$ (Basisfälle),
- Rekursionsgleichungen, die jedem Konstruktor $f \in R$ eine Funktion g_f zuordnen, welche die Werte auf den Komponenten zu einem Wert für $f(\dots)$ kombiniert.

Dies generalisiert primitive Rekursion auf $\mathbb{N}$.

Beispiele

Listen / Tupel A^*

Induktive Definition: $A^* := N(\{()\}, \{\mathrm{cons}_a \mid a \in A\})$ mit $\mathrm{cons}_a(\ell) = (a, \ell)$.

- Länge:

$$\mathrm{len}(()) := 0,$$
$$\mathrm{len}(\mathrm{cons}_a(\ell)) := 1 + \mathrm{len}(\ell)$$

- Summe:

$$\mathrm{sum}(()) := 0,$$
$$\mathrm{sum}(\mathrm{cons}_a(\ell)) := a + \mathrm{sum}(\ell)$$

- Minimum:

$$\min(()) := \infty,$$
$$\min(\mathrm{cons}_a(\ell)) := \min(a, \min(\ell)).$$

Binärbäume tree(A)

Induktive Definition: $\mathrm{tree}(A) := N(A, \{\mathrm{node}\})$ mit $\mathrm{node}(x, y) = (x, y)$ und Blättern aus A.

- Tiefe:

$$\mathrm{depth}(a) := 0,$$
$$\mathrm{depth}(\mathrm{node}(x, y)) := 1 + \max(\mathrm{depth}(x), \mathrm{depth}(y)).$$

- Blatt-Summe:

$$\mathrm{sumLeaf}(a) := a,$$
$$\mathrm{sumLeaf}(\mathrm{node}(x, y)) := \mathrm{sumLeaf}(x) + \mathrm{sumLeaf}(y).$$

Formale Aussagenlogik

Die Menge der aussagenlogischen Formeln wird induktiv definiert:

- Grundelemente: Variablen $x_1, x_2, \dots$
- Wenn A, B Formeln sind, dann sind $(A \wedge B)$ und $(A \vee B)$ Formeln.
- Wenn A eine Formel ist, dann ist $\neg A$ eine Formel.

Syntax

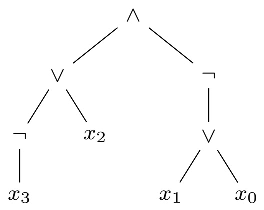
Die Syntax der Aussagenlogik (Menge aller aussagenlogischen Formeln) wird durch die obige Induktion definiert. Sie ist gegeben durch $N(\{x_1, x_2, \dots\}, \{\mathrm{and}, \mathrm{or}, \mathrm{not}\})$ mit

$$\mathrm{and}(A, B) := (A \wedge B)$$
$$\mathrm{or}(A, B) := (A \vee B)$$
$$\mathrm{not}(A) := (\neg A).$$

Syntaxbaum

Jede Formel besitzt einen zugehörigen Syntaxbaum, der ihre rekursive Struktur darstellt.

$$(\neg x_3 \vee x_2) \wedge \neg(x_1 \vee x_0)$$



Strukturelle Rekursion

Strukturelle Rekursion ist wie primitive Rekursion, nur dass sie nicht über $\mathbb{N}$, sondern über die jeweils echte Unterstruktur eines rekursiven Datentyps (z. B. Listen oder Bäume) definiert wird.
Funktionen auf Formeln werden begründet durch:

- *Basisfall*: für jede Variable x_i wird $f(x_i)$ definiert.
- *Rekursionsschritte*: für jede Verknüpfung (z.B. $\wedge, \vee, \neg$) wird eine Funktion $g_\wedge, g_\vee, g_\neg$ definiert, die die Werte der Funktion auf den Teilformeln kombiniert.

Beispiele: Die Menge aller Subfunktionen einer Formel ist durch strukturelle Rekursion definiert als:

$$\mathrm{sufo}(x_i) := \{x_i\}$$
$$\mathrm{sufo}(A \wedge B) := \{A \wedge B\} \cup \mathrm{sufo}(A) \cup \mathrm{sufo}(B)$$
$$\mathrm{sufo}(A \vee B) := \{A \vee B\} \cup \mathrm{sufo}(A) \cup \mathrm{sufo}(B)$$
$$\mathrm{sufo}(\neg A) := \{\neg A\} \cup \mathrm{sufo}(A)$$

Analog: Menge aller Variablen in einer Formel vars$(\cdot)$.

Semantik

Jede Formel A mit Variablen in $\{x_1, \dots, x_n\}$ wird als boolesche Funktion $[\![A]\!]_n : \{0,1\}^n \to \{0,1\}$ interpretiert:

$$[\![x_i]\!]_n(b_1, \dots, b_n) = \begin{cases} b_i & 1 \le i \le n \\ 0 & \text{sonst} \end{cases}$$

$$[\![A \wedge B]\!]_n(b_1, \dots, b_n) = \min([\![A]\!]_n, [\![B]\!]_n),$$
$$[\![A \vee B]\!]_n(b_1, \dots, b_n) = \max([\![A]\!]_n, [\![B]\!]_n),$$
$$[\![\neg A]\!]_n(b_1, \dots, b_n) = 1 - [\![A]\!]_n.$$

Semantische Eigenschaften

Viele Eigenschaften von Formeln lassen sich über ihre semantische Interpretation definieren. Beispiele:

- *allgemeingültig*: $[\![A]\!]_n = (\vec{b} \mapsto 1)$ für alle $n \in \mathbb{N}$,
- *unerfüllbar*: $[\![A]\!]_n = (\vec{b} \mapsto 0)$ für alle $n \in \mathbb{N}$,
- *erfüllbar*: es existiert ein $n \in \mathbb{N}$ und ein Vektor $\vec{b} \in \{0,1\}^n$ mit $[\![A]\!]_n(\vec{b}) = 1$,
- *äquivalent*: $[\![A]\!]_n = [\![B]\!]_n$ für alle $n \in \mathbb{N}$.

Wahrheitstabellen

Die Semantik einer Formel kann durch Wahrheitstabellen dargestellt werden; die letzte Spalte gibt Werte von $[\![A]\!]_n$ an. Erfüllbarkeit, Allgemeingültigkeit und Äquivalenz lassen sich daraus ablesen.

$\{0,1\}^2$	$[\![x_1]\!]_2$	$[\![x_2]\!]_2$	$[\![\neg x_2]\!]_2$	$[\![(x_1 \wedge \neg x_2)]\!]_2$
$(0,0)$	0	0	1	0
$(1,0)$	1	0	1	1
$(0,1)$	0	1	0	0
$(1,1)$	1	1	0	0

Funktionale Vollständigkeit

Für jede boolesche Funktion $f : \{0,1\}^n \to \{0,1\}$ existiert eine aussagenlogische Formel A mit $[\![A]\!]_n = f$. Diese kann z.B. durch die disjunktive Normalform (DNF) konstruiert werden.

Normalformen

Rekursive Definitionen für Mengen K_n und D_n:

$$K_0 = D_0 = \{x_i, \neg x_i \mid i \in \mathbb{N}\},$$
$$K_{n+1} = \{\bigwedge_j A_j \mid A_j \in D_n\},$$
$$D_{n+1} = \{\bigvee_j A_j \mid A_j \in K_n\}.$$

Es gilt für alle $n \in \mathbb{N}$:

$$D_n \subseteq K_{n+1}, \quad D_n \subseteq D_{n+1},$$
$$K_n \subseteq K_{n+1}, \quad K_n \subseteq D_{n+1}.$$

Formeln in K_2 sind in konjunktiver Normalform (KNF), solche in D_2 in disjunktiver Normalform (DNF). Jede Formel $[\![A]\!]_n$ besitzt äquivalente Darstellungen in KNF und DNF (Konstruktion über die Wertetabelle und De-Morgan-Transformationen).

Konstruktion der DNF

Die disjunktive Normalform (DNF) einer Formel A mit Variablen in $\{x_1, \dots, x_n\}$ wird konstruiert durch:

- Bestimmen aller Belegungen $\vec{b} \in \{0,1\}^n$, für $[\![A]\!]_n(\vec{b}) = 1$.
- Für jede solche Belegung $\vec{b} = (b_1, \dots, b_n)$ wird ein Konjunktionsglied $K_{\vec{b}}$ gebildet:

$$K_{\vec{b}} = \bigwedge_{i=1}^{n} \begin{cases} x_i & \text{wenn } b_i = 1 \\ \neg x_i & \text{wenn } b_i = 0 \end{cases}$$

- Die DNF von A ist dann die Disjunktion aller Konjunktionsglieder:

$$\mathrm{DNF}(A) = \bigvee_{\vec{b} \text{ mit } [\![A]\!]_n(\vec{b}) = 1} K_{\vec{b}}$$

Konstruktion der KNF

Die konjunktive Normalform (KNF) einer Formel A mit Variablen in $\{x_1, \dots, x_n\}$ wird konstruiert durch:

- Bestimmen aller Belegungen $\vec{b} \in \{0,1\}^n$, für $[\![A]\!]_n(\vec{b}) = 0$.
- Für jede solche Belegung $\vec{b} = (b_1, \dots, b_n)$ wird ein Disjunktionsglied $D_{\vec{b}}$ gebildet:

$$D_{\vec{b}} = \bigvee_{i=1}^{n} \begin{cases} \neg x_i & \text{wenn } b_i = 1 \\ x_i & \text{wenn } b_i = 0 \end{cases}$$

- Die KNF von A ist dann die Konjunktion aller Disjunktionsglieder:

$$\mathrm{KNF}(A) = \bigwedge_{\vec{b} \text{ mit } [\![A]\!]_n(\vec{b}) = 0} D_{\vec{b}}$$

Elementare Zahlentheorie

Teilbarkeitsrelation

Für ganze Zahlen $x, y \in \mathbb{Z}$ heisst y ein Vielfaches von x, wenn es ein $t \in \mathbb{Z}$ mit $y = tx$ gibt. In diesem Fall heisst x ein Teiler von y und man schreibt $x|y$. Die Menge der natürlichen Teiler einer Zahl x ist

$$T(x) := \{n \in \mathbb{N} \mid n|x\}.$$

Teilen mit Rest

Für $a, b \in \mathbb{Z}$ mit $b \neq 0$ existieren eindeutig bestimmte ganze Zahlen $m, r \in \mathbb{Z}$ mit

$$a = mb + r, \qquad 0 \le r < |b|.$$

Für natürliche Zahlen $a, b \in \mathbb{N}$ mit $b \neq 0$ gilt entsprechend mit $m, r \in \mathbb{N}$

$$a = mb + r, \qquad r < b.$$

Ganzzahlige Division und Modulo

Für $a, b \in \mathbb{Z}$ mit $b \neq 0$ werden die Funktionen

$$\mathrm{div} : \mathbb{N} \times \mathbb{N} \setminus \{0\} \to \mathbb{Z},$$
$$\mathrm{mod} : \mathbb{N} \times \mathbb{N} \setminus \{0\} \to \mathbb{N}.$$

durch

$$a = \mathrm{div}(a, b) \cdot b + \mathrm{mod}(a, b), \qquad 0 \le \mathrm{mod}(a, b) < |b|$$

definiert. Dabei entspricht div der ganzzahligen Division und mod dem Rest.

Grösster gemeinsamer Teiler

Für ganze Zahlen $a_1, \dots, a_n$ ist die Menge der gemeinsamen Teiler

$$T(a_1, \dots, a_n) := T(a_1) \cap \dots \cap T(a_n).$$

Der grösste gemeinsame Teiler ist definiert als

$$\mathrm{ggT}(a_1, \dots, a_n) := \max T(a_1, \dots, a_n),$$

sofern nicht alle Zahlen Null sind. Zwei Zahlen heissen *teilerfremd*, wenn ihr grösster gemeinsamer Teiler gleich 1 ist.

Euklidischer Algorithmus

Für beliebige ganze Zahlen a, b gilt

$$\mathrm{T}(a,b) = \mathrm{T}(a, b-a).$$

Für ganze Zahlen a, b die nicht beide Null sind, gilt

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(a, b-a).$$

Daraus folgt allgemein die rekursive Definition des ggT. Für $(a,b) \in \mathbb{N}^2 \setminus \{(0,0)\}$ gilt:

$$\mathrm{ggT}(a,b) = \begin{cases} \max(a,b) & \text{falls } a = 0 \vee b = 0 \\ \mathrm{ggT}(\mathrm{mod}(a,b), b) & \text{falls } a \geq b \\ \mathrm{ggT}(a, \mathrm{mod}(b,a)) & \text{sonst} \end{cases}$$

Durch Festlegung von $\mathrm{ggT}(a,b) := \mathrm{ggT}(|a|, |b|)$ für $a, b \in \mathbb{Z}$ wird der euklidische Algorithmus auf alle ganzen Zahlen erweitert.

Lemma von Bézout

Für $x, y \in \mathbb{Z}$, die nicht beide Null sind, existieren ganze Zahlen a, b mit

$$\mathrm{ggT}(x,y) = ax + by.$$

Die Zahlen a und b heissen Bézout-Koeffizienten. Sie lassen sich mit dem erweiterten euklidischen Algorithmus bestimmen.

Primzahlen

Eine Zahl $p \in \mathbb{N}$ heisst Primzahl, wenn $|T(p)| = 2$; äquivalent dazu ist $p > 1$ und $T(p) = \{1, p\}$. Die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet.

- **Existenz von Primfaktoren.** Zu jeder natürlichen Zahl $n > 1$ existiert eine Primzahl p mit $p \mid n$. Daher lässt sich jede $n > 1$ als Produkt endlich vieler Primzahlen darstellen.
- **Unendlichkeit der Primzahlen.** Es existieren unendlich viele Primzahlen (klassisches Argument nach Euklid).
- **Euklidsches Lemma.** Für $p \in \mathbb{N}$ sind äquivalent:
  1. p ist eine Primzahl.
  2. $\forall a, b \in \mathbb{N}(p|ab \Rightarrow p|a \vee p|b)$.
- **Eindeutigkeit der Primfaktorzerlegung (Fundamentalsatz der Arithmetik).** Jede $n > 1$ besitzt eine Darstellung

  $$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

  mit Primzahlen $p_1 < \cdots < p_k$ und Exponenten $\alpha_i \in \mathbb{N}$. Diese Darstellung ist bis auf die Reihenfolge eindeutig.
- **Primfaktorzerlegung und ggT.** Für zwei Zahlen

  $$a = \prod_{i=1}^{n} p_i^{\alpha_i}, \qquad b = \prod_{i=1}^{m} p_i^{\beta_i},$$

  gilt insbesondere

  $$\mathrm{ggT}(a,b) = \prod_{i=1}^{\min(n,m)} p_i^{\min(\alpha_i, \beta_i)}.$$

  Beispiel: $\mathrm{ggT}(20, 25) = \mathrm{ggT}(2^2 \cdot 3^0 \cdot 5^1, 2^0 \cdot 3^0 \cdot 5^2) \Rightarrow 2^0 \cdot 3^0 \cdot 5^1 = 5.$