Diskrete Mathematik

Zahlenmengen

$\mathbb{N}$	natürliche Zahlen
$\mathbb{N}_0$	natürliche Zahlen mit 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.

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

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: $\{x \in \mathbb{N} \mid \exists y \in \mathbb{N}(x = 2y)\}$
- Zahlen > 17: $\{x \in \mathbb{N} \mid x > 17\}$
- Alle ausser 22: $\{x \in \mathbb{N} \mid x \neq 22\}$

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:

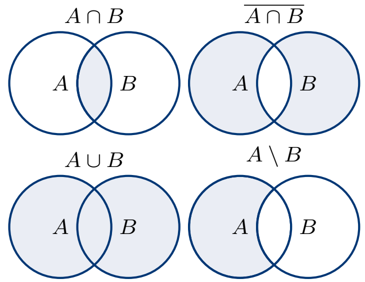
$$\forall i, j \in I\; (i \neq j \Rightarrow A_i \cap A_j = \varnothing).$$

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 $\mathcal{P}(\varnothing) = \{\varnothing\} \neq \varnothing$.
- $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$
- $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$

Relationen und Funktionen

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.

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

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 $k \le n$ 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

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

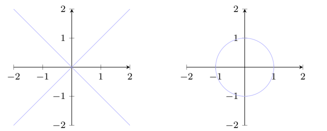
wobei A die Quellmenge, B die Zielmenge und $G \subseteq A \times B$ der *Graph* von R ist. Ist $A = B$, so heisst R *homogen* auf A.

Notation

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

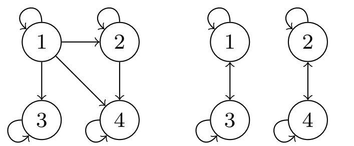
- Ist G der Graph von R, so schreibt man G_R
- Ist $(x, y) \in G$, dann schreibt man xRy (x steht in Relation zu y bezüglich R).
- Sind A und B Teilmengen von $\mathbb{R}$, so kann man R auch als Menge von Punkten in der Ebene darstellen: $\{(x, y) \mid xRy\}$.

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



- 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.

$$\mathrm{dom}(R) := pr_1(G_R) = \{a \in A \mid \exists b \in B(aRb)\}$$
$$\mathrm{im}(R) := pr_2(G_R) = \{b \in B \mid \exists a \in A(aRb)\}$$

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:

$$\begin{tikzcd} x \arrow[loop above] \end{tikzcd}$$

- 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:

$$x \longleftrightarrow y$$

- 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:

$$x \longrightarrow y$$

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:

$$\begin{tikzcd} x \arrow[r] \arrow[rr, bend left, dashed] & y \arrow[r] & z \end{tikzcd}$$

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:

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

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:

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

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:

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

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.

Copyright © 2025 Justin Iven Müller
github.com/JustinIven/zhaw-cheatsheets