Diskrete Mathematik

David Jäggli

1. März 2023

Inhaltsverzeichnis

1 Allg

1.1 Grundlagen der Logik und Beweise

- Die Regeln der Logik geben mathematischen Aussagen eine präzise Bedeutung.
- Konstruktion korrekter mathematischer Argumente

1.2 Aussagen (Propositionen)

Propositionen:

- Bern ist die Bundesstadt
- $1 + 1 = 2$
- Goldbachsche Vermutung: sie ist entweder wahr oder falsch, man weis es noch nicht

Keine Propositionen:

- Wie spät ist es?
- $x + 1 = 2$
- Dieser Satz ist falsch.

Begründung: Es handelt sich hier nicht um Aussagen, die entweder wahr oder falsch sind. Eine Aussage ist wahrheitsdefiniert. In einer Aussage darf nicht offen sein ob die Aussage wahr oder falsch sein kann. Sie darf sich auch nicht selbst widersprechen.

2 Operatoren

- Negotiationsoperator: $\neg$
- Konjunktion $\wedge$
- Disjunktion $\vee$
- Implikation $\rightarrow$
- Bikonditional $\leftrightarrow$

2.1 Diskunktion

$p \lor q$
Wenn p oder q wahr ist, ist die Aussage wahr (logic OR).

p	q	$p \lor q$
w	w	w
w	f	w
f	w	w
f	f	f

2.2 Implikation

$p \to q$
Wenn p dann q

p	q	$p \to q$
w	w	w
w	f	f
f	w	w
f	f	w

2.3 Bikonditional

$p \leftrightarrow q$
Wenn beide den gleichen Wahrheitswert haben ist die Aussage wahr.
Wahrheitstabelle:

p	q	$p \leftrightarrow q$
w	w	w
w	f	f
f	w	f
f	f	w

2.4 Prioritäten

Operator	Priorität
$\neg$	1
$\wedge$	2
$\vee$	2
$\rightarrow$	3
$\leftrightarrow$	3

3 Aussagen

3.1 Tautologie und Wiederspruch

Tautologie ist eine Aussage, welche immer wahr ist.
Ein Wiederspruch ist eine Aussage, welche immer falsch ist.

3.2 Logische Äquivalenzen

Die Aussage p und q heissen logisch äquivalent, falls $p \leftrightarrow q$ eine Tautologie ist. Man schreibt dann $p \Leftrightarrow q$ oder $p \equiv q$ bzw. $p \sim q$

3.3 Logische Äquivalenzregeln

$\mathrm{p} \wedge \mathbf{T} \equiv \mathrm{p}$ *)	$\mathrm{p} \vee \mathbf{F} \equiv \mathrm{p}$	Identität
$\mathrm{p} \vee \mathbf{T} \equiv \mathbf{T}$	$\mathrm{p} \wedge \mathbf{F} \equiv \mathbf{F}$	Dominanz
$\mathrm{p} \vee \mathrm{p} \equiv \mathrm{p}$	$\mathrm{p} \wedge \mathrm{p} \equiv \mathrm{p}$	Idempotenz
$\neg(\neg \mathrm{p}) \equiv \mathrm{p}$		Doppelnegation
$\mathrm{p} \vee \neg \mathrm{p} \equiv \mathbf{T}$	$\mathrm{p} \wedge \neg \mathrm{p} \equiv \mathbf{F}$	Tautologie/Kontradiktion
$\mathrm{p} \vee \mathrm{q} \equiv \mathrm{q} \vee \mathrm{p}$	$\mathrm{p} \wedge \mathrm{q} \equiv \mathrm{q} \wedge \mathrm{p}$	Kommutativität
$\mathrm{p} \vee (\mathrm{p} \wedge \mathrm{q}) \equiv \mathrm{p}$	$\mathrm{p} \wedge (\mathrm{p} \vee \mathrm{q}) \equiv \mathrm{p}$	Absorption
$(\mathrm{p} \vee \mathrm{q}) \vee \mathrm{r} \equiv \mathrm{p} \vee (\mathrm{q} \vee \mathrm{r})$		Assoziativgesetz 1
$(\mathrm{p} \wedge \mathrm{q}) \wedge \mathrm{r} \equiv \mathrm{p} \wedge (\mathrm{q} \wedge \mathrm{r})$		Assoziativgesetz 2
$\mathrm{p} \vee (\mathrm{q} \wedge \mathrm{r}) \equiv (\mathrm{p} \vee \mathrm{q}) \wedge (\mathrm{p} \vee \mathrm{r})$		Distributivgesetz 1
$\mathrm{p} \wedge (\mathrm{q} \vee \mathrm{r}) \equiv (\mathrm{p} \wedge \mathrm{q}) \vee (\mathrm{p} \wedge \mathrm{r})$		Distributivgesetz 2
$\neg(\mathrm{p} \wedge \mathrm{q}) \equiv \neg \mathrm{p} \vee \neg \mathrm{q}$		De Morgan's Gesetz 1
$\neg(\mathrm{p} \vee \mathrm{q}) \equiv \neg \mathrm{p} \wedge \neg \mathrm{q}$		De Morgan's Gesetz 2

Duale Regeln: $\wedge$ mit $\vee$ vertauschen u. umgekehrt
und T mit F.

Weiterführend:
$p \rightarrow q \equiv \neg p \vee q$

Beispiel angewandte logische Äquivalenzregeln
Beispiel 1:
$(p \vee \neg(q \wedge p)) \wedge (r \vee (s \vee r))$
$\equiv (p \vee \neg q \vee \neg p) \wedge (r \vee r \vee s)$
$\equiv (T \vee \neg q) \wedge (r \vee s)$
$\equiv T \wedge (r \vee s)$
$\equiv r \vee s$

Beispiel 2:
$(a \to (b \to c)) \to ((a \to b) \to (a \to c))$
$\equiv (a \to (\neg b \vee c)) \to ((\neg a \vee b) \to (\neg a \vee c))$
$\equiv (\neg a \vee (\neg b \vee c)) \to (\neg(\neg a \vee b) \vee (\neg a \vee c))$
$\equiv (\neg a \vee \neg b \vee c) \to ((a \wedge \neg b) \vee \neg a \vee c)$
$\equiv (\neg a \vee \neg b \vee c) \to ((a \vee \neg a) \wedge (\neg b \vee \neg a) \vee c)$
$\equiv (\neg a \vee \neg b \vee c) \to (\neg b \vee \neg a \vee c)$
$\equiv \mathrm{X} \to \mathrm{X}$
$\equiv \neg\mathrm{X} \vee \mathrm{X}$
$\equiv \mathrm{T}$

4 Quantoren

Wird ein Quantor auf die Variable x angewandt, dann nennt man diese Variable *gebunden*, ansonsten *frei*.

4.1 Prädikate

Ein Prädikat ist ein Wortkonstrukt, welches mindestens eine Variable enthält.
$P(x) =$ "$x > 3$"
Die Aussage $P(4) = 4 > 3$ ist wahr, während $P(2) = 2 > 3$ falsch ist.

4.2 Allquantor

Ist $P(x)$ wahr für alle x aus einer bestimmten Universalmenge, dann schreibt man $\forall x P(x)$. Gelesen wird dies, "für alle x gilt $P(x)$".
Falls es nur auf eine Bestimmte Zahlenmenge zutrifft (z.B. $\mathbb{Z}$) dann schreibt man:
$\forall x \in \mathbb{Z}$ ist wahr.

4.3 Existenzquantor

Ist $P(x)$ wahr für mindestens ein x aus einer bestimmten Universalmenge, dann schreibt man $\exists x P(x)$ und liest: ës existiert ein x für welches $P(x)$ wahr ist".

4.4 Verschachtelte Quantoren

Die Reihenfolge der Quantoren ist wesentlich; ausser alle Quantoren sind vom gleichen Typ (also Allquantoren oder Existenzquantoren)!

5 Beweise

- Ein Satz (Theorem) ist eine Aussage, von der man zeigen kann, dass sie wahr ist.
- Um zu zeigen, dass ein Satz wahr ist, verwendet man eine Abfolge (Sequenz) von Aussagen, die zusammen ein Argument, genannt Beweis ergeben.
- Aussagen können Axiome oder Postulate enthalten (grundlegende Annahmen der mathematischen Strukturen).
- Durch logisches (also gewissen Regeln gehorchendes) schliessen werden Folgerungen gemacht, die zusammen den Beweis ergeben.
- Ein Lemma ist ein einfacher Satz, der in Beweisen von komplizierteren Sätzen verwendet wird.
- Ein Korollar ist eine einfache Folgerung eines Satzes.

6 Mengen

Eine Menge ist eine ungeordnete Zusammenfassung wohldefinierter, unterscheidbarer Objekte, genannt *Elemente*, zu einem Ganzen. Für irgendein Objekt x gilt dann bezüglich der Menge A entweder $x \in A$ oder dann $x \notin A$.
Beispiel:
Endliche Mengen lassen sich durch Aufschreiben der in ihnen enthaltenen Elemente beschreiben. z.B. die Menge aller natürlichen Zahlen kleiner als 101:
$A = 0, 1, 2, ..., 99, 100$ (aufzählend notiert)
$99 \in A$ aber $101 \notin A$ (beschreibend notiert)

andere Schreibweisen sind:

$A = n \in \mathbb{N} | n < 101 = n \in \mathbb{N} : n <= 100 = n | n \in \mathbb{N} \wedge n <= 100$

6.1 Gleichheit, elementare Mengen

Zwei Mengen A und B sind **gleich** ($A = B$), falls sie dieselben Elemente enthalten. $(A \subset B) \wedge (B \subset A)$

Einige bekannte Mengen:
$\mathbb{N}$ - Menge der natürlichen Zahlen ($\mathbb{N}^* = \mathbb{N} \setminus \{0\}$)
$\mathbb{Z}$ - Menge der ganzen Zahlen
$\mathbb{Z}^+$ - Menge der positiven ganzen Zahlen
$\mathbb{Q}$ - Menge der Brüche
$\mathbb{R}$ - Menge der reellen Zahlen
$\mathbb{C}$ - Menge der komplexen Zahlen

6.2 Spezielle Mengen

Teilmenge: A ist Teilmenge von B, geschrieben $A \subset B$, genau dann, wenn $\forall x(x \in A \rightarrow x \in B)$: es gilt $A \subset A$!

Leere Menge: Für jede Menge A gilt: $\emptyset \subset A$.

Kardinalität: Ist S eine endliche Menge, dann bezeichnet $|S|$ die Kardinalität. Die Kardinalität ist die Anzahl Elemente von S.

Potenzmenge: Die Potenzmenge $P(S)$ oder 2^S der Menge S besteht aus der Menge aller Teilmengen $A \subset S$.

Beispiel:
Bestimmen Sie die Potenzmenge von $S = \{1, 2\}$
$S = \{1, 2\}$
$P(S) = 2^S = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
Es gilt allgemein $|2^S| = 2^{|S|}$

6.3 Das Kreuzprodukt zweier Mengen / kartesisches Produkt

$A \times B = \{(a, b) | a \in A \wedge b \in B\}$
Reihenfolge ist entscheidend, $A \times B \neq B \times A$
$|A \times B| = |A| \cdot |B|$

Beispiel: $A \times B = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$

6.4 Mengenoperationen

6.4.1 Komplement

Ist A eine Teilmenge der Menge M, so bezeichnet

$A^c = \overline{A} = \{m \in M | m \notin A\}$

das Komplement von A bezüglich M.

6.4.2 Durchschnitt

Sind A und B Teilmengen einer Menge M, so bezeichnet

$A \cap B = \{m \in M | m \in A \wedge m \in B\}$

den Durchschnitt von A und B.

6.4.3 Vereinigung

Sind A und B Teilmengen einer Menge M, so bezeichnet

$A \cup B = \{m \in M | m \in A \vee m \in B\}$

die Vereinigung von A und B.

6.4.4 Differenz

Sind A und B Teilmengen einer Menge M, so bezeichnet

$$B \setminus A = \{m \in M | m \in B \land m \notin A\}$$

die Differenz

6.5 Set Operatoren

Allg. Operator	Set Operator
$p \lor q$	$A \cup B$
$p \land q$	$A \cap B$
$\neg p$	$\overline{A}$

6.5.1 Rechenregeln

Theorem

Für das Rechnen mit Mengen $A, B, C \subseteq M$ *gelten die folgenden Regeln:*

$$\begin{aligned}
A \cup B &= B \cup A && \textit{Kommutativgesetz}\\
A \cap B &= B \cap A && \textit{Kommutativgesetz}\\
A \cup (B \cup C) &= (A \cup B) \cup C && \textit{Assoziativgesetz}\\
A \cap (B \cap C) &= (A \cap B) \cap C && \textit{Assoziativgesetz}\\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) && \textit{Distributivgesetz}\\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) && \textit{Distributivgesetz}\\
\overline{A \cup B} &= \overline{A} \cap \overline{B} && \textit{De Morgan's Gesetz}\\
\overline{A \cap B} &= \overline{A} \cup \overline{B} && \textit{De Morgan's Gesetz.}
\end{aligned}$$

Die duale Rechenregel (jeweils auf den Zeilen 2, 4, 6 *und* 8*, erhält man, indem man* $\cap$ *und* $\cup$ *vertauscht und* $\emptyset$ *mit der Universalmenge* M *(falls diese vorkommen).*

6.5.2 Mengen Identitäten

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

7 Funktionen

Wird jedem Element x einer Menge X genau ein Element y einer Menge Y zugeordnet, so heisst die Zuordnung **Funktion**.