Mathematik I:
Theoretische Grundlagen der Informatik

Prof. Dr.-Ing. Sebastian Schlesinger

17. November 2022

Aussagen

Unter einer **Aussage** versteht man einen sprachlichen Ausdruck, dem man eindeutig einen der beiden Wahrheitswerte w („wahr“) bzw. f („falsch“) zuordnen kann.
Aussagen werden mit Großbuchstaben bezeichnet,

$$A : Beschreibung$$

und können mit logischen Operationen verknüpft werden.
Grundlegende mathematische Aussagen, die nicht aus anderen Aussagen abgeleitet werden können, nennt man **Axiome**.

Beispiele von Aussagen

- Wahre Aussage A: Jede natürliche Zahl ist ein Produkt von Primzahlen.
- Falsche Aussage B: Jede Primzahl ist ungerade
- Unbewiesene Vermutung (wahr oder falsch, d.h. eine Aussage, bei der der Wahrheitswert noch nicht entschieden werden konnte) C: Es gibt unendlich viele Primzahlzwillinge.
- Keine Aussage (Feststellung ohne Wahrheitswert) D: Freitag der dreizehnte ist ein Unglückstag.

Logische Operationen

Logische Aussagen können durch die in der folgenden Tabelle angegebenen Operationen verknüpft werden.

Bezeichnung	Schreibweise	(Sprechweise)	wahr, gdw
Negation	$\neg A$	(nicht A)	A falsch ist
Konjunktion	$A \wedge B$	(A und B)	A und B wahr sind
Disjunktion	$A \vee B$	(A oder B)	A oder B wahr ist
Implikation	$A \Rightarrow B$	(wenn A dann B)	A falsch oder B wahr
Äquivalenz	$A \Leftrightarrow B$	(A äquivalent B)	A und B äquivalent

Bindungsstärke

Um in logischen Ausdrücken Klammern zu sparen, wird festgelegt, dass $\neg$ stärker bindet als $\wedge$ sowie $\vee$ und diese wiederum stärker als $\Rightarrow, \Leftrightarrow$.

Wahrheitstabelle

In der folgenden Tabelle sind die Wahrheitswerte der vorgestellten Verknüpfungen angegeben. Dabei steht w für wahr und f für falsch.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	f	w	w	w	w
w	f	f	f	w	f	f
f	w	w	f	w	w	f
f	f	w	f	f	w	w

Hinweis: Statt w für *wahr* und f für *falsch* werden auch die Symbole $\top$ und $\bot$ verwendet.

Gesetze für logische Operationen

Für logische Operationen gelten die folgenden Identitäten.

- Assoziativgesetze:

$$(A \wedge B) \wedge C = A \wedge (B \wedge C)$$

$$(A \vee B) \vee C = A \vee (B \vee C)$$

- Kommutativgesetze:

$$A \wedge B = B \wedge A$$

$$A \vee B = B \vee A$$

- Distributivgesetze:

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$$

Gesetze für logische Operationen

Für logische Operationen gelten die folgenden Identitäten.

- De Morgansche Regeln:

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

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

- Idempotenz:

$$\neg(\neg A) = A$$

$$A \vee A = A$$

$$A \wedge A = A$$

- Kürzungsregeln:

$$A \vee \bot = A$$

$$A \wedge \top = A$$

Prädikatenlogik

Wir führen nun Quantoren ein. Neben den atomaren Aussagen der Aussagenlogik möchte man in der Lage sein, Aussagen zu formulieren, die praktisch von Parametern abhängen.

Definition (Quantoren)

Wir definieren folgende Notation:

- Mit $\forall x : A(x)$ definieren wir, dass eine Aussage A, die eine Variable x beinhaltet, für alle Werte von x gelten soll (üblicherweise wird dann auch eine Grundmenge, aus denen die x stammen sollen, angegeben).
- Mit $\exists x : A(x)$ drücken wir aus, dass es ein x geben soll, so dass $A(x)$ gilt.

Die Aussagen $A(x)$ können komplexe Aussagen mit Verknüpfungen sein und es lassen sich auch Quantoren kombinieren und man kürzt oft ab.

Beweismethoden

Wie führt man nun einen Beweis? Es gibt verschiedene Beweismethoden. Die wichtigsten sind:

- Direkter Beweis: Man beweist direkt $A \Rightarrow B$, also dass B aus der Annahme von A folgt.
- Man verwendet die Umkehrung von $A \Rightarrow B$, also $\neg B \Rightarrow \neg A$
- Indirekter Beweis: Man nimmt an, A gelte und folgert dann B, was aber im Widerspruch zu A ist. Praktisch folgert man also $A \wedge \neq A$, was falsch sein muss. Also muss die Annahme falsch gewesen sein und da sie das Gegenteil von dem ist was man beweisen möchte, ist der Beweis komplett.

Mengendefinition

Definition (Naive Mengendefinition)

Eine Menge ist die Zusammenfassung von bestimmten unterschiedlichen Objekten (die Elemente der Menge) zu einem neuen Ganzen. Wir schreiben $x \in M$, falls das Objekt x zur Menge M gehört. Wir schreiben $x \notin M$, falls das Objekt x nicht zur Menge M gehört. Falls $x \in M$ und $y \in M$ gilt, schreiben wir auch $x, y \in M$. Eine Menge, welche nur aus endlich vielen Objekten besteht (eine endliche Menge), kann durch explizite Auflistung dieser Elemente spezifiziert werden.

Beispiel: $M = \{2, 3, 5, 7\}$.
Hierbei spielt die Reihenfolge der Auflistung keine Rolle:

$$\{2, 3, 5, 7\} = \{7, 5, 3, 2\}$$

Auch Mehrfachauflistungen spielen keine Rolle:

$$\{2, 3, 5, 7\} = \{2, 2, 2, 3, 3, 5, 7\}$$

Mengennotation

Mengen können definiert werden durch

- Aufzählung der Elemente
- Formulierung von Bedingungen in der Form $M := \{x|p(x)\}$, wobei p ein *Prädikat*, also eine Aussage ist, die x enthält, so dass man jeweils bei Einsetzen von x entscheiden kann, ob sie wahr (und damit das Element zur Menge gehört) oder falsch ist (und damit das Element x nicht zu M gehört).

Wir schreiben zur Abkürzung auch $M := \{x \in N|p(x)\}$ statt $M := \{x|x \in N \wedge p(x)\}$.

Besondere Mengen

Eine besonders wichtige Menge ist die leere Menge $\emptyset = \{\}$, die keinerlei Elemente enthält.
In der Mathematik hat man es häufig auch mit unendlichen Mengen zu tun (Mengen, die aus unendlich vielen Objekten bestehen). Solche Mengen können durch Angabe einer Eigenschaft, welche die Elemente der Menge auszeichnet, spezifiziert werden.
Beispiele:

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- $\mathbb{Q} = \{\frac{p}{q} | p, q \in \mathbb{Z}, q \neq 0\}$

Warum naive Mengenlehre?

Die „Definition“der Menge ist anfällig für Widersprüche, z.B. die **Russelsche Antinomie**:
Man bilde die Menge aller Mengen, die sich nicht selbst als Element enthalten, in Formeln:

$$M := \{N | N \notin N\}$$

Frage: Gilt $M \in M$? Das führt auf einen Widerspruch.
Daher hat man die Mengenlehre mit dem **Zermelo-Fraenkelschen Axiomensystem** auf ein solides Fundament gehoben. Mehr dazu im optionalen Inhalt (ist zu kompliziert für eine erste Einführung).

Teilmengen

Definition (Teilmenge)

Seien A und B Mengen. $A \subseteq B$ bedeutet A ist *Teilmenge* von B, genau dann, wenn

$$\forall x : x \in A \Rightarrow x \in B$$

oder äquivalent dazu

$$\forall x \in A : x \in B$$

Lemma (Gleichheit von Mengen)

Seien A und B Mengen. Es ist $A = B$ genau dann, wenn $\forall x : x \in A \Leftrightarrow x \in B$, was wiederum äquivalent ist zu

$$A \subseteq B \land B \subseteq A$$

Um also die Gleichheit von zwei Mengen zu zeigen beweist man üblicherweise erst $A \subseteq B$ und dann $B \subseteq A$.

Mengenoperationen

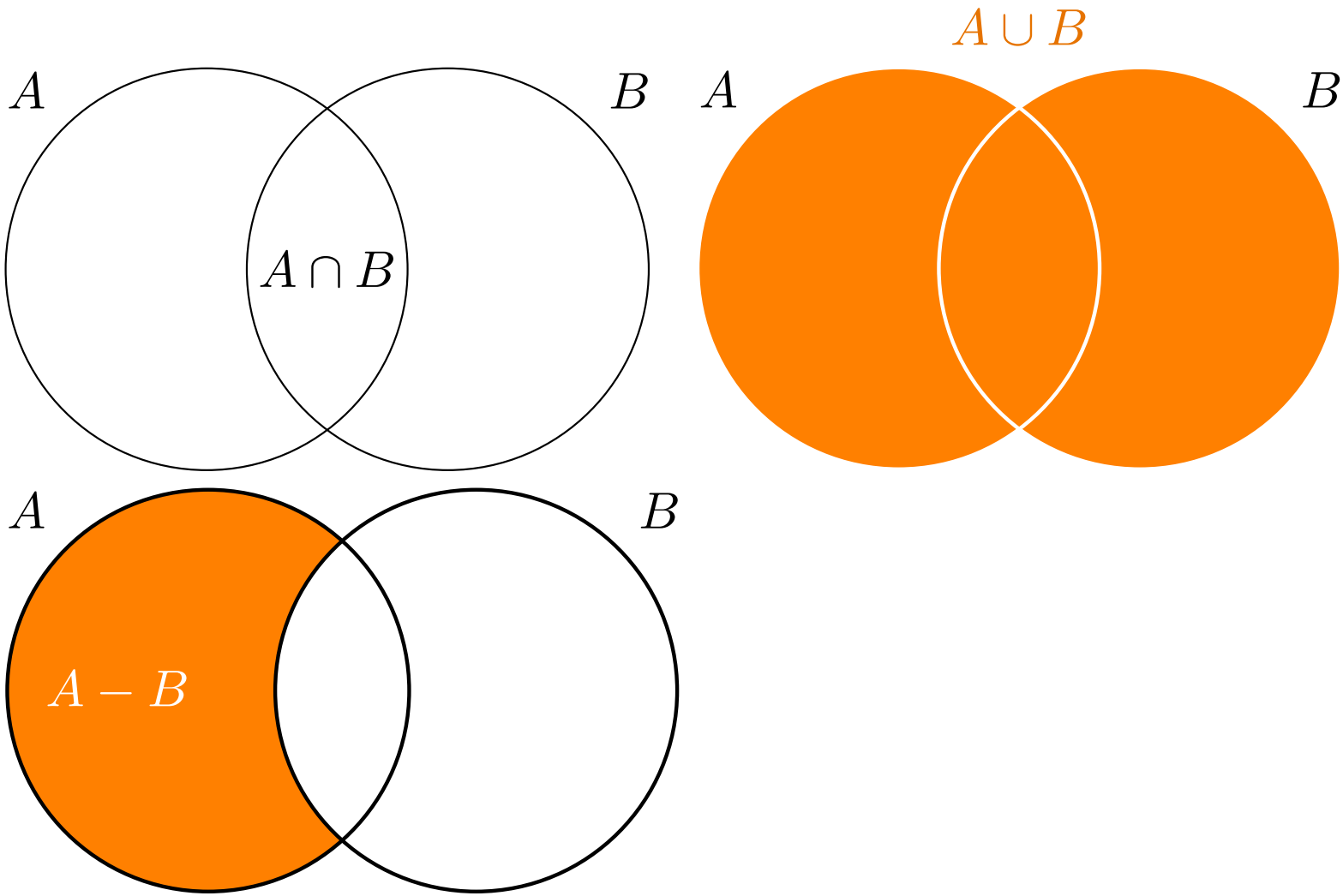
Definition (Mengenoperationen)

Seien A und B Mengen. Wir definieren:

- $A \cap B := \{x | x \in A \land x \in B\}$, den *Schnitt* von A und B
- $A \cup B := \{x | x \in A \lor x \in B\}$, die *Vereinigung* von A und B
- $A \backslash B := \{x \in A | x \notin B\}$, die *Differenz* von A und B

Venn-Diagramme

Die Operationen lassen sich in **Venn-Diagrammen** visualisieren.



Weitere Mengen und Eigenschaften

Definition (Potenzmenge)

Mit

$$\mathscr{P}(A) := 2^A := \{B | B \subseteq A\}$$

bezeichnen wir die **Potenzmenge**, die Menge aller Teilmengen von A.

Definition (Disjunktheit)

Zwei Mengen A und B sind *disjunkt*, falls $A \cap B = \emptyset$ gilt.

Beispiele für Mengenaussagen

Es gilt:

- $\forall A : \emptyset \subseteq A$
- $\forall A : A \subseteq A$
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- $\{1, 2, 3\} \cap \{4, 5, 6\} = \emptyset$
- $\mathscr{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1.2\}\}$
- $\mathscr{P}(\emptyset) = \{\emptyset\}$
- $\forall A : A \cap \emptyset = \emptyset$
- $\forall A : A \cup \emptyset = A$
- $\forall A, B, C : A \cap (B \cup C) = (A \cap B) \cup (B \cap C)$
- $\forall A, B, C : A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\forall A, B, C : A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$
- $\forall A, B, C : A \backslash (B \cap C) = (A \backslash B) \cap (A \backslash C)$