Mathematische Grundlagen

für Wirtschaftsinformatiker

Prof. Dr. Peter Becker

Fachbereich Informatik
Hochschule Bonn-Rhein-Sieg

Wintersemester 2016/17

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Allgemeines zur Vorlesung

Homepage:

`http://www2.inf.h-brs.de/~pbecke2m/mathegrund/`

Die Vorlesung wird überwiegend folienbasiert gehalten.

Die Folien enthalten nur die wichtigsten Aspekte (Definitionen, Sätze, knappe Beispiele, wichtige Bemerkung).

Alles was sonst eine Vorlesung ausmacht (Erläuterungen, ausführliche Beispiele, Beweise von Sätzen, Anwendungen, Querverweise auf andere Gebiete der Mathematik und Informatik, etc.) gibt es nur in der Vorlesung selbst.

Die Folien zur Vorlesung (Skript) stehen auf der Homepage vor der Vorlesung zur Verfügung.

Termin der Vorlesung

- Donnerstags, 10:45 bis 12:15 Uhr, H 1/2

- Wir fangen pünktlich an!

  Nehmen Sie rechtzeitig ihre Plätze ein. Wer zu spät kommt, stört alle anderen Zuhörer.
- Sollten Sie dennoch zu spät sein, nutzen Sie bitte leise die oberen Eingänge.
- Bitte Ruhe während der Vorlesung.

  Sie stören nicht mich, sondern Ihre Kommilitonen.

Übungen

- Beginn der Übungen: ab KW 41 (5. Oktober 2016)
- 2 Stunden Übungen pro Woche
- 3 Gruppen insgesamt: Bitte beachten Sie die Gruppenzuordnung.
- Mit der Vorlesung wöchentlich Ausgabe eines Aufgabenblatts
- Ab dem 2. Aufgabenblatt müssen Sie handschriftliche Lösungen abgeben, die bewertet werden (Vorleistung!!!).
- Die Aufgaben werden in der Woche nach der Abgabe in den Übungen besprochen.
- keine Tests, keine Anwesenheitspflicht

Termine für die Übungen

BIS:

- Gruppe 1: Mi., 10:45–12:15 Uhr, C 120
- Gruppe 2: Mo., 9:00–10:30 Uhr, C 115
- Gruppe 3: Mo., 15:15–16:45 Uhr, C 115

Inhalt

Lernziele (allgemein)

- Grundlegende mathematische Begriffe kennen und deren exakte Definition wiedergeben können.
  - ☞ Es ist nicht ausreichend, nur eine ungefähre Vorstellung der mathematischen Begriffe zu haben.
- Die „Sprache“ der Mathematik in Grundzügen beherrschen und damit elementare mathematische Sachverhalte formulieren können.
  - ☞ Sprache muss man üben, üben, üben, ...
- Beweistechniken beherrschen und einfache mathematische Aussagen beweisen können.
  - ☞ Beweise sind das Herz der Mathematik.

Inhaltliche Voraussetzungen: Interesse an Mathematik und Informatik

Prüfungszulassung/Vorleistung

- Wöchentlich erscheint mit der Vorlesung ein Aufgabenblatt.
- Bearbeitungzeit: eine Woche, Abgabe vor der Vorlesung der nächsten Woche
- Die Hausaufgaben sind fristgerecht abzugeben und werden bewertet.
- Es werden nur handschriftliche Lösungen akzeptiert!
- Geben Sie bei der Abgabe Ihre Matrikelnummer und Übungsgruppe an. Keine Gruppenarbeit!
- Für die Zulassung zur Prüfung müssen 50% der möglichen Punkte erreicht werden.
- Dies gilt für alle, auch Wiederholer.
- Wer einmal die Zulassung geschafft hat, muss sie in späteren Jahren nicht wiederholen.

Prüfung

- Klausur, 90 Minuten
- Inhalte: alles aus Vorlesung und Übung
- 3 Credits
- Termin: siehe Prüfungsplan (der ca. Anfang November erscheint)
- Vergessen Sie nicht sich zur Prüfung anzumelden.
- Abmeldung bis sieben Tage vor der Klausur möglich.
- Zulassung zur Prüfung nur mit erbrachter Vorleistung!

Vorsicht! Stolpergefahr

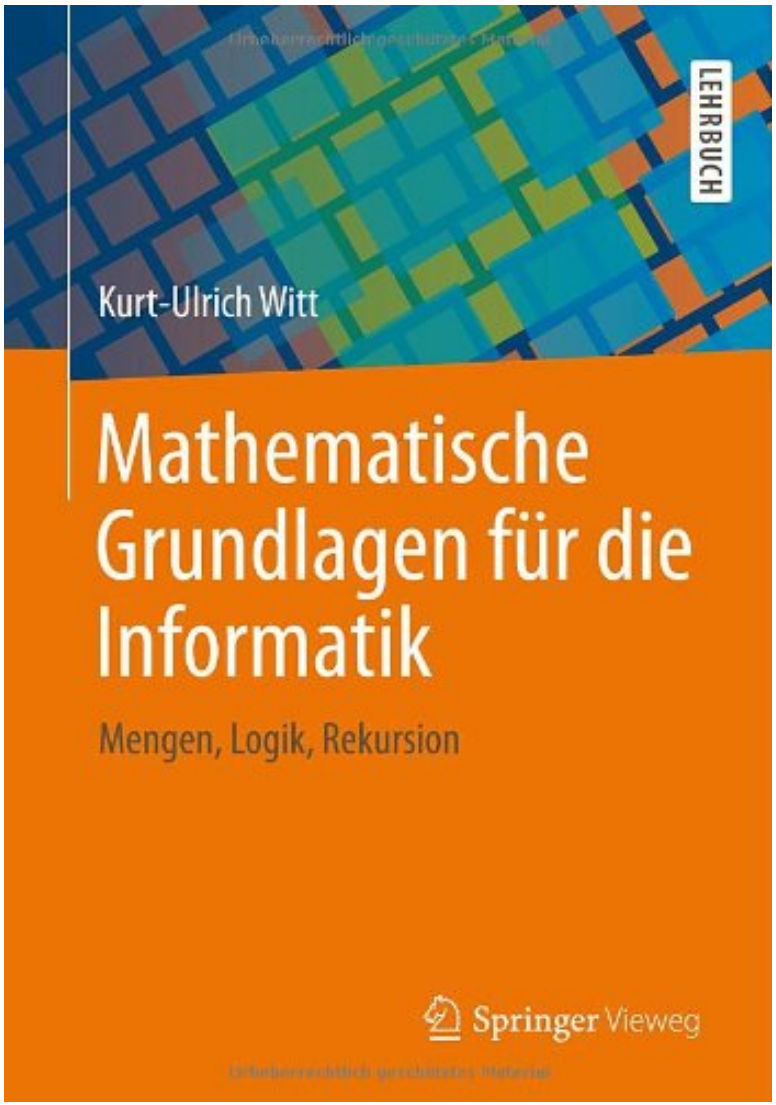
- in der Vergangenheit hohe Durchfallquoten
- Vorleistung erforderlich
- deutliche Steigerung im Niveau und Tempo gegenüber der Schulmathematik
- anderer Charakter der Hochschulmathematik:
  - klare Definition von Begriffen
  - im Vordergrund stehen mathematische Aussagen, weniger Rechentechniken
  - Schema: Definition, Satz, Beweis

Was tun bei Problemen?

Realistisch bleiben und ehrlich zu sich selbst sein!

- Besser verzichten als erzwingen: Gehen Sie niemals schlecht vorbereitet in eine Prüfung.
- Besser zwei Module voll als vier Module halb: Die Durchfallquoten sind hoch!
  Formal haben Sie beliebig lange Zeit fürs Studium, aber nicht beliebig viele Fehlversuche.
- Nehmen Sie mit, was Sie gelernt haben: Die Vorkenntnisse aus diesem Semester erleichtern Ihnen den Wiedereinstieg im nächsten Jahr.

Literatur

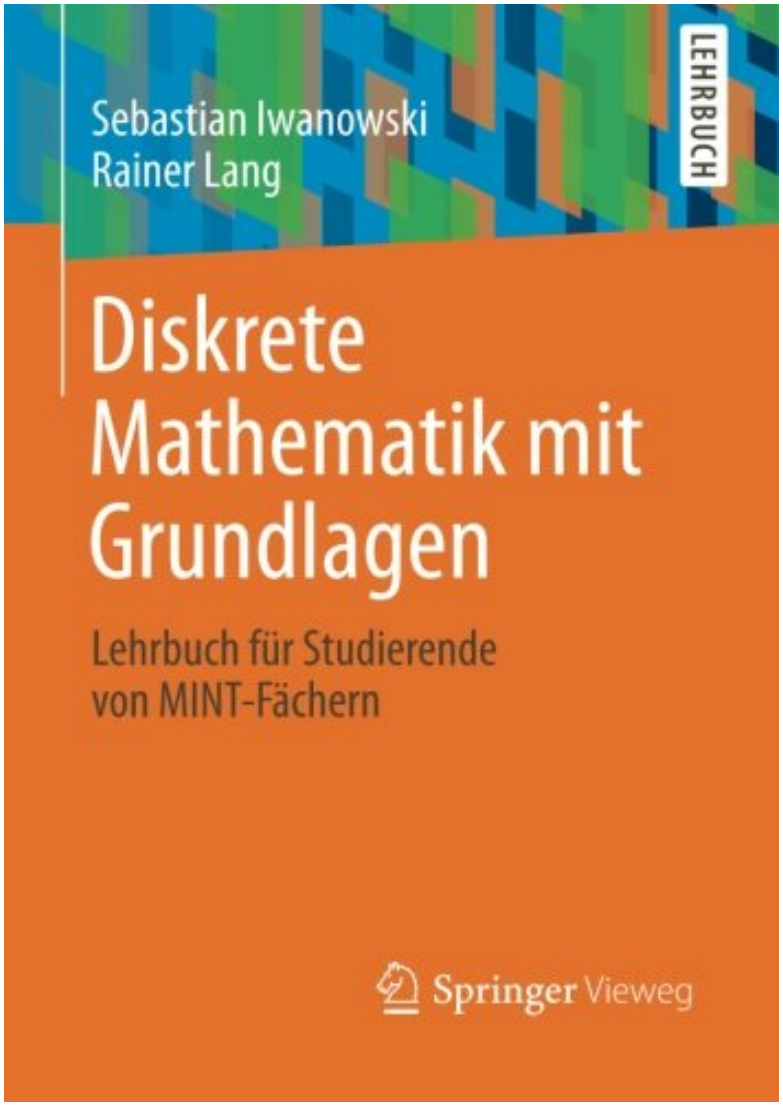


Kurt-Ulrich Witt
Mathematische Grundlagen für die Informatik
Springer Vieweg, 2013

- Standardwerk für diese Veranstaltung, auch für die Informatiker
- Ich halte mich inhaltlich eng an dieses Buch.
- PDF in Bibliothek online verfügbar

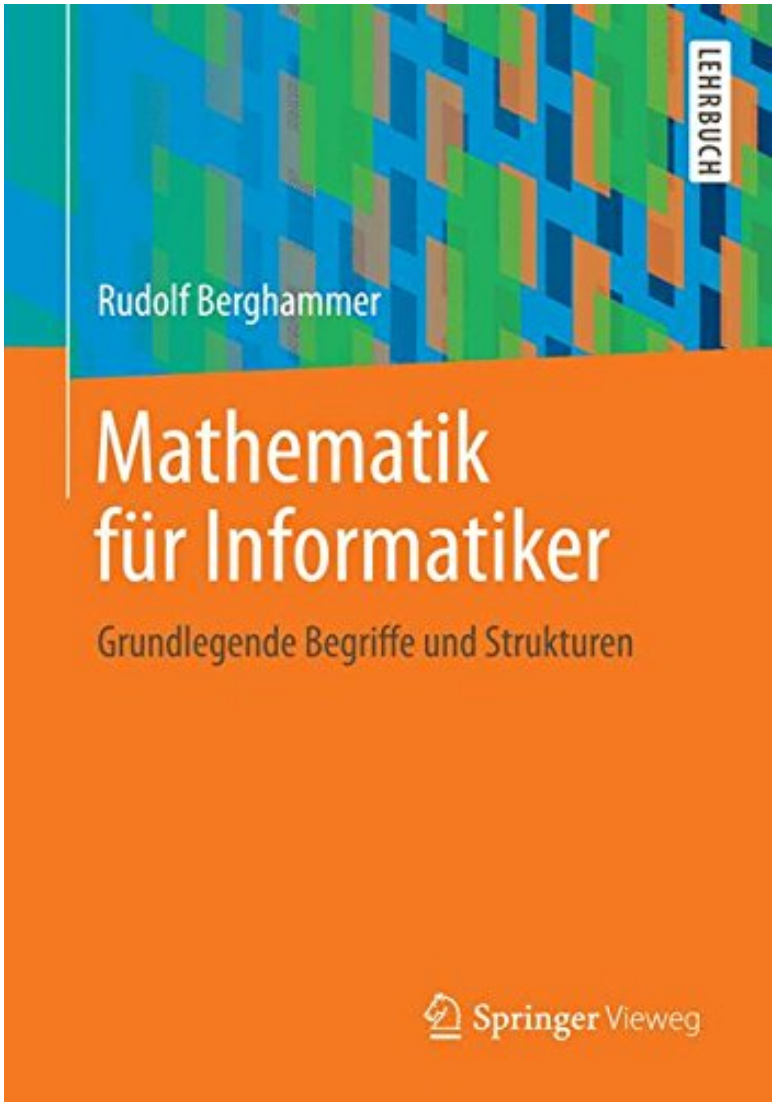
Christoph Meinel, Martin Mundhenk
Mathematische Grundlagen der Informatik
Vieweg und Teubner, 2011

- Inhaltlich ähnlich zum Buch von Witt.
- weniger kompakt und die Reihenfolge ist etwas anders
- Als Ergänzung sehr zu empfehlen.
- PDF in Bibliothek online verfügbar



Sebastian Iwanowski, Rainer Lang
Diskrete Mathematik mit Grundlagen
Springer Vieweg, 2014

- Logik wird eher nur kurz abgehandelt.
- enthält viele Aufgaben
- Als Ergänzung sehr zu empfehlen.
- PDF in Bibliothek online verfügbar

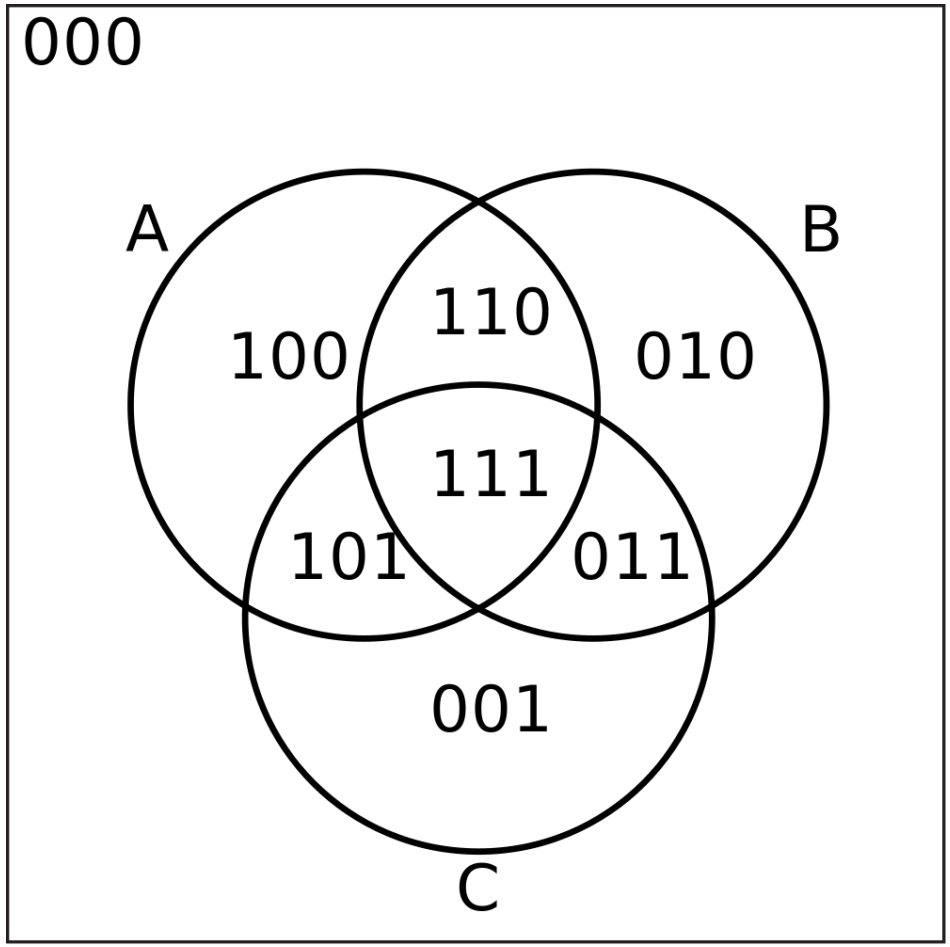


Rudolf Berghammer
Mathematik für Informatiker
Springer Vieweg, 2014

- Inhaltlich ähnlich zum Buch von Witt.
- Als Ergänzung sehr zu empfehlen.
- PDF in Bibliothek online verfügbar

Kapitel 1

Mengen



Inhalt

Ein Mengenbegriff

- In der Mathematik dient der Begriff der Menge dazu, Objekte zu einer neuen Einheit zusammenzufassen,
- so dass diese Einheit als (neues) Ganzes betrachtet und weiterverwendet werden kann.

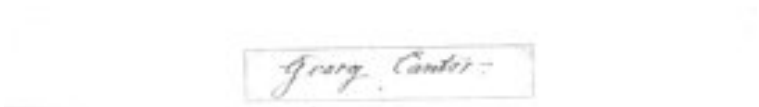
Festlegung: Cantorscher Mengenbegriff

Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Dinge unserer Anschauung oder unseres Denkens, welche Elemente der Menge genannt werden, zu einem Ganzen.

Georg Cantor

Georg Cantor (1845-1918) war ein deutscher Mathematiker.

Cantor lieferte wichtige Beiträge zur modernen Mathematik. Insbesondere ist er der Begründer der Mengenlehre und veränderte den Begriff der Unendlichkeit.



Darstellung von Mengen

Die Notation einer Menge erfolgt in der Art

$$\{\ldots\}$$

Die Elemente der Menge werden durch die Mengenklammern $\{$ und $\}$ zu einem Ganzen zusammengefasst.

„...“ ist ein Platzhalter und steht für die eindeutige Festlegung, welche Dinge Elemente der Menge sind (dazu später mehr).

Wir können Mengen einen Namen geben. Dies erfolgt mithilfe eines Gleichheitszeichens:

$$M = \{\ldots\}$$

Element

Ist ein Ding a Element einer Menge M, dann schreiben wir

$$a \in M$$

Ist ein Ding a kein Element einer Menge M, dann schreiben wir

$$a \notin M$$

Für mehrere Elemente vereinbaren wir abkürzende Schreibweisen.

$$a, b, c \in M$$

bedeutet $a \in M$ und $b \in M$ und $c \in M$. Analog bedeutet

$$a, b, c \notin M$$

dass $a \notin M$ und $b \notin M$ und $c \notin M$ gilt.

Schachtelung und leere Menge

Anschaulich kann man sich Mengen als Behälter, z. B. als Schachteln, vorstellen. Die Schachtel wird durch die Mengenklammern dargestellt.

Genau wie Schachteln weitere Schachteln enthalten können, kann auch eine Menge weitere Mengen enthalten.

Und genau wie eine Schachtel leer sein kann, kann auch eine Menge leer sein.

Die leere Menge wird durch $\{\}$ oder durch $\emptyset$ dargestellt.

Ist die Menge M leer, so notieren wir $M = \emptyset$ (oder $M = \{\}$).

Offensichtlich gilt $a \notin \emptyset$ für jedes Ding a.

Beispiele zur Notation

Beispiel 1.1

(i) Die Menge

$$A = \{1, 2, 3, 4, 5\}$$

enthält als Elemente die Zahlen $1, 2, 3, 4$ und 5. Es gilt also z. B. $2, 5 \in A$ sowie $0, 6, 13 \notin A$.

(ii) Die Menge

$$B = \{1, 2, \{3, 4, 5, 6\}\}$$

enthält drei Elemente: die Zahlen 1 und 2 sowie die Menge $C = \{3, 4, 5, 6\}$, die selbst vier Elemente enthält. Wir könnten auch

$$B = \{1, 2, C\}$$

schreiben.

Fortsetzung Beispiel.

(iii) Die Menge

$$D = \{\{\,\}\}$$

enthält genau ein Element, nämlich die leere Menge. Somit ist die Menge D selbst nicht leer.

Schachtelmetapher: Die Schachtel D ist nicht leer, denn sie enthält ein Element, die leere Schachtel.

Es gilt $\{\,\} \in D$.

Wenn wir $E = \{\,\}$ setzen, dann ist

$$D = \{E\}$$

wodurch auch in der mathematischen Notation deutlich wird, dass D nicht die leere Menge ist.

Darstellung von Mengen

Unsere Festlegung des Mengenbegriffs besagt, dass die Elemente einer Menge bestimmt sein müssen.

Dazu verwenden wir zwei Arten der Darstellung von Mengen:

- aufzählende Darstellung

  Bei der aufzählenden Darstellung werden die Elemente einer Menge wie in Beispiel 1.1 explizit angegeben.
- beschreibende Darstellung

  Bei der beschreibenden Darstellung werden die Elemente nicht explizit aufgezählt, sondern es wird eine definierende Eigenschaft angegeben.

Aufzählende Darstellung

Beispiel 1.2

$$
\begin{aligned}
A &= \{2, 3, 5, 7, 11\} \\
B &= \{1, 2, \ldots, 50\} \\
C &= \{1, 2, \ldots\} \\
D &= \{43, 44, \ldots\}
\end{aligned}
$$

Die Menge A enthält fünf Element, nämlich die Primzahlen kleiner gleich 11.

Bei den drei anderen Mengen wird ein Problem der aufzählenden Darstellung von Mengen eutlich: Für welche Elemente steht „. . .“?

Bei B sind vermutlich die natürlichen Zahlen von 1 bis 50 gemeint, bei C die natürlichen Zahlen und bei D die natürlichen Zahlen größer gleich 43.

Die allgemeine Form der aufzählenden Darstellung von Mengen ist also

$$M = \{a_1, a_2, \ldots, a_n\}$$

für endliche Mengen sowie

$$M = \{a_1, a_2, \ldots\}$$

für unendliche Mengen.

Beschreibende Darstellung

Bei der beschreibenden Darstellung werden die Elemente nicht explizit aufgezählt, sondern es wird eine definierende Eigenschaft angegeben.

Die allgemeine Form ist

$$M = \{x | p(x)\}$$

- Dabei ist x ein Platzhalter (eine Variable) für die Elemente der Menge,
- und $p(x)$ ist eine für x (informal oder formal) angegebene Eigenschaft.
- Genau die Dinge x, die die Eigenschaft $p(x)$ erfüllen, sind Elemente der Menge.
- Für die formale Definition solch einer Eigenschaft nutzen wir später die Prädikatenlogik.

Beispiel 1.3

$$
\begin{aligned}
A &= \{x | x \text{ ist eine Primzahl kleiner gleich } 11\} \\
B &= \{x | x \text{ ist eine positive ganze Zahl und } x + x = 10\} \\
C &= \{(x, y) | x \text{ und } y \text{ sind positive ganze Zahlen und } x + y = 6\} \\
T_{64} &= \{y | y \text{ ist ein positiver Teiler von } 64\} \\
S &= \{st | st \text{ studiert Informatik an der Hochschule Bonn-Rhein-Sieg}\}
\end{aligned}
$$

Aufzählende Darstellung für die ersten vier Mengen: ✎

Kardinalität

Enthält eine Menge M endlich viele Elemente, etwa m Stück, dann schreiben wir

$$|M| = m$$

und nennen M eine endliche Menge.

$|M|$ heißt die Kardinalität von M.

Nicht endliche Mengen heißen unendlich, und wir notieren

$$|M| = \infty.$$

Offensichtlich gilt

$$|\emptyset| = 0.$$

Bezeichner für Zahlenmengen

Natürliche Zahlen:

$\mathbb{N} = \{1, 2, 3, \ldots\}$	natürliche Zahlen
$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$	natürliche Zahlen mit 0
$\mathbb{N}_k = \{k, k+1, k+2, \ldots\}$	natürliche Zahlen ab k, $k \in \mathbb{N}_0$
$\mathbb{N}_{u,o} = \{u, u+1, u+2, \ldots, o\}$	natürliche Zahlen zwischen u und o
$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$	Primzahlen

Ganze Zahlen:

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$	ganze Zahlen
$\mathbb{G}_+ = \{0, 2, 4, \ldots\}$	nicht negative gerade Zahlen
$\mathbb{G}_- = \{-2, -4, \ldots\}$	negative gerade Zahlen
$\mathbb{G} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$	gerade Zahlen
$\mathbb{U}_+ = \{1, 3, 5, \ldots\}$	positive ungerade Zahlen
$\mathbb{U}_- = \{-1, -3, -5, \ldots\}$	negative ungerade Zahlen
$\mathbb{U} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$	ungerade Zahlen

Rationale, reelle und komplexe Zahlen:

$\mathbb{Q} = \left\{ \frac{p}{q} \middle\| p \in \mathbb{Z} \text{ und } q \in \mathbb{N} \right\}$	rationale Zahlen (Brüche)
$\mathbb{Q}_+, \mathbb{Q}_-$	rationale Zahlen größer gleich/kleiner 0
$\mathbb{R}, \mathbb{R}_+, \mathbb{R}_-$	reelle Zahlen/größer gleich/kleiner 0
$\mathbb{C} = \{a + \mathrm{i}b \| a, b, \in \mathbb{R}, \mathrm{i}^2 = -1\}$	komplexe Zahlen

Paradoxon

Sei S die Schlange, die all diejenigen Schlangen in den Schwanz beißt, die sich nicht selbst in den Schwanz beißen.

Beißt S sich selbst in den Schwanz?

- Es gibt nur zwei Möglichkeiten: S beißt sich selbst in den Schwanz oder nicht.
- Nehmen wir an, S beiße sich in den Schwanz.
  Dann gehört sie zu den Schlangen, die sich selber in den Schwanz beißen.
  Also wird sie nicht von S in den Schwanz gebissen.
  Also beißt sich S nicht selber in den Schwanz. Widerspruch!

- Nehmen wir an, S beiße sich nicht in den Schwanz.
  Dann gehört sie zu den Schlangen, die sich nicht selber in den Schwanz beißen.
  Diese Schlangen werden aber gerade von S gebissen.
  Also beißt sich S selber in den Schwanz. Widerspruch!
- In beiden möglichen Fällen führt die jeweilige Annahme zu einem Widerspruch.
- Somit kann die Frage „Beißt S sich selbst in den Schwanz?“ nicht beantwortet werden.
- Es liegt ein sogenanntes Paradoxon vor.

Russellsche Antinomie

Wir betrachten die Menge M' aller Mengen, die sich nicht selbst enthalten:

$$M' = \{A | A \notin A\}$$

Enthält M' sich selbst, also gilt $M' \in M'$?

- Annahme: $M' \in M'$
  Dann gehört M' zu den Mengen, die sich selbst enthalten.
  Daraus folgt aber nach Definition $M' \notin M'$. Widerspruch!
- Annahme: $M' \notin M'$
  Also enthält M' sich nicht selbst.
  Daraus folgt aber nach Definition $M' \in M'$. Widerspruch!
- Dieses Paradoxon ist die Russellsche Antinomie.
- Es zeigt die Unzulänglichkeit des Cantorschen Mengenbegriffs.

Diskussion zur Russellschen Antinomie

- Die Russellsche Antinomie zeigt die Unzulänglichkeit des Cantorschen Mengenbegriffs.
- Eine Mengendefinition sollte in jedem Fall die eindeutige Beantwortung der Frage ermöglichen, ob ein Ding in einer Menge enthalten ist oder nicht.

Stellt die Russellsche Antinomie die Mathematik insgesamt in Frage, da diese wesentlich auf der Mengenlehre basiert?

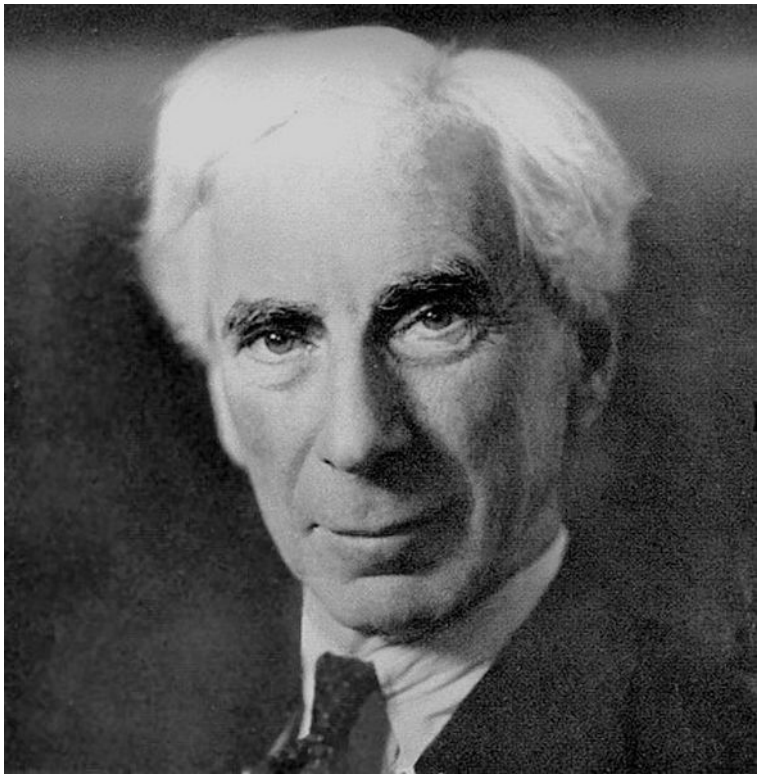
- Nein. Die axiomatische Mengenlehre vermeidet Antinomien.
- Eine axiomatische Herleitung würde aber den Rahmen dieser Vorlesung sprengen.
- Für unsere Zwecke ist der Cantorsche Mengenbegriff ausreichend.

Bertrand Russell

Bertrand Russell (1872-1970) war ein britischer Philosoph, Mathematiker und Logiker.

Er erhielt 1950 den Nobelpreis für Literatur.

Zusammen mit Alfred North Whitehead veröffentlichte er die Principia Mathematica, eines der bedeutendsten Werke des 20. Jahrhunderts über die Grundlagen der Mathematik.



Zusammenfassung

- Menge als Zusammenfassung von Dingen.
  Durch die Zusammenfassung entsteht ein neues Ding.
- Schachtelung: Mengen können Mengen enthalten.
- Notation:
  - aufzählend: $\{3, 4, 5, 6, 7\}$
  - beschreibend: $\{x | x \in \mathbb{N} \text{ und } 3 \leq x \leq 7\}$
- Kardinalität: Anzahl der Elemente in einer Menge
- Die Russellsche Antinomie zeigt die Unzulänglichkeit des Cantorschen Mengenbegriffs.

Kapitel 2

Aussagenlogik

Inhalt

Aussagenlogik als Sprache

Wir wollen die Aussagenlogik als formale Sprache einführen.

Eine (formale) Sprache wird festgelegt durch

- ein Alphabet, welches ein endlicher Zeichenvorrat ist, aus dem die Wörter und Sätze einer Sprache zusammengesetzt sind,
- die Syntax, die festlegt, welche mit den Elementen des Alphabets gebildete Zeichenketten als Wörter oder Sätze zur Sprache gehören,
- die Semantik, welche den Wörtern und Sätzen der Sprache eine Bedeutung zuordnet.

Alphabet der Aussagenlogik

Das Alphabet der Aussagenlogik besteht aus zwei Mengen:

- aus der Menge O der aussagenlogischen Operatorsymbole

$$O = \{\underline{0}, \underline{1}, \neg, \wedge, \vee, (,)\}$$

- sowie aus einer Menge V von aussagenlogischen Variablen.

  Wir nutzen als aussagenlogische Variablen Kleinbuchstaben vom Ende des deutschen Alphabets, z. B. p, q, r, v, x, y, z, bei Bedarf auch indiziert, also z. B. x_1, x_2, x_3.

Syntax aussagenlogischer Formeln

Die Sprache $\mathcal{A}$ der Aussagenlogik, deren Elemente aussagenlogische Formeln heißen, ist durch folgende Syntaxregeln festgelegt:

(i) Die Operatorsymbole $\underline{0}, \underline{1} \in O$, die so genannten aussagenlogischen Konstantenbezeichner, sind aussagenlogische Formeln: $\underline{0}, \underline{1} \in \mathcal{A}$.

(ii) Jede aussagenlogische Variable ist auch eine aussagenlogische Formel: Für alle $v \in V$ gilt $v \in \mathcal{A}$.

(iii) Als Variablenbezeichner für aussagenlogische Formeln verwenden wir kleine Buchstaben vom Anfang des griechischen Alphabets: $\alpha, \beta, \gamma, \ldots$, bei Bedarf auch indiziert, z. B. $\alpha_1, \alpha_2, \ldots$

Aus bereits vorhandenen aussagenlogischen Formeln werden mithilfe der Operator- und Klammersymbole neue Formeln gebildet: Sind $\alpha, \beta \in \mathcal{A}$, dann auch $(\alpha \wedge \beta), (\alpha \vee \beta), \neg\alpha \in \mathcal{A}$.

(iv) Genau die gemäß den Regeln (i) bis (iii) bildbaren Zeichenketten gehören zu $\mathcal{A}$.

- Aussagenlogische Konstantenbezeichner und Variablen heißen auch atomare Formeln.
- Die unter Verwendung von Regel (iii) gebildeten Formeln heißen zusammengesetzt.
- Formeln der Gestalt v sowie der Gestalt $\neg v$ mit $v \in V$ heißen Literale.

  Literale sind also aussagenlogische Variablen sowie mit dem Operator $\neg$ versehene aussagenlogische Variablen.

Beispiel 2.1

Es gilt:

(i) $(p \wedge q) \in \mathcal{A}$

(ii) $(((p \vee (q \wedge r)) \wedge \neg(q \vee \neg r)) \vee \underline{0}) \in \mathcal{A}$

(iii) $p(\neg q \vee r) \notin \mathcal{A}$

Wir zeigen, dass (ii) gilt:

(1) $\underline{0}, p, q, r \in \mathcal{A}$ gemäß Regel (i) bzw. Regel (ii)

(2) Gemäß (1) und Regel (iii) ist $\neg r \in \mathcal{A}$.

(3) Gemäß (1) und Regel (iii) ist $(q \wedge r) \in \mathcal{A}$.

(4) Gemäß (1,2) und Regel (iii) ist $(q \vee \neg r) \in \mathcal{A}$.

(5) Gemäß (4) und Regel (iii) ist $\neg(q \vee \neg r) \in \mathcal{A}$.

(6) Gemäß (1,3) und Regel (iii) ist $(p \vee (q \wedge r)) \in \mathcal{A}$.

Fortsetzung Beispiel.

(7) Gemäß (5,6) und Regel (iii) ist $((p \vee (q \wedge r)) \wedge \neg(q \wedge \neg r)) \in \mathcal{A}$.

(8) Gemäß (1,7) und Regel (iii) ist $(((p \vee (q \wedge r)) \wedge \neg(q \vee \neg r)) \vee \underline{0}) \in \mathcal{A}$.

Durch schrittweises Anwenden der Regeln (i) bis (iii) haben wir die aussagenlogische Formel

$$(((p \vee (q \wedge r)) \wedge \neg(q \vee \neg r)) \vee \underline{0})$$

konstruiert.

Diese Formel enthält die vier Literale $p, q, r, \neg r$.

Aussagenlogische Konstanten

- Die Bedeutung von aussagenlogischen Formeln wollen wir durch die Werte 0 für „falsch“ und 1 für „wahr“ angeben.
- Die Menge dieser beiden aussagenlogischen Konstanten bzw. Wahrheitswerte bezeichnen wir mit $\mathbb{B}$.
- Wir legen auf $\mathbb{B} = \{0, 1\}$ eine Ordnung fest: 0 sei kleiner als 1.
- Also $\max\{0, 1\} = 1$ und $\min\{0, 1\} = 0$.
- Außerdem legen wir als Operationen auf $\mathbb{B}$ fest:

$$1 - 1 = 0 \quad \text{sowie} \quad 1 - 0 = 1.$$

- Mit diesen Operationen gelten die folgenden Beziehungen:

$$\begin{aligned} \min\{x, y\} &= 1 - \max\{1 - x, 1 - y\} \\ \max\{x, y\} &= 1 - \min\{1 - x, 1 - y\} \end{aligned}$$

- Wir könnten also prinzipiell auf min oder max verzichten.

Abstrakte Logikmaschine

- Wir können $(\mathbb{B}, \max, \min, -)$ als eine abstrakte Maschine auffassen, die die Werte 0 und 1 zur Verfügung stellt und darauf die Operationen $\max, \min$ und $-$ ausführen kann.
- Solch eine abstrakte Maschine nennt man auch Rechenstruktur oder algebraische Struktur.
- Eine mehr praktische Sichtweise wäre, sich die abstrakte Maschine als speziellen Rechner vorzustellen.
- Eine aussagenlogische Formel ist dann sowas wie ein Programm: abhängig von Eingaben wird ein Ergebnis berechnet.
- Diese Eingabe besteht darin, den aussagenlogischen Variablen der Menge V konkrete Wahrheitswerte zuzuweisen.
- Wir benötigen jetzt noch eine Vorschrift, die exakt festlegt, wie eine aussagenlogische Formel – abhängig von den Eingaben – berechnet wird.

Rekursion

- Rekursion bezeichnet die Eigenschaft von Regeln, dass sie auf das, was durch die Regeln erzeugt wird, wieder angewendet werden können.
- Wir haben die Syntax der aussagenlogischen Formeln rekursiv definiert.
- Rekursion ist von fundamentaler Bedeutung für die Informatik.
- Wir können auch Mengen rekursiv definieren.

Beispiel 2.2

Die Menge M bestehe genau aus den Zahlen, die durch die folgenden Regeln erzeugt werden können:

(i) $5 \in M$

(ii) Gilt $x \in M$ und $2x + 1 \leq 50$, dann ist auch $2x + 1 \in M$.

(iii) Gilt $x \in M$ und $3x + 2 \leq 50$, dann ist auch $3x + 2 \in M$.

Vereinigung von Mengen

- Für zwei Mengen A und B bezeichnet $A \cup B$ die Vereinigung von A und B.
- Hierbei werden die Elemente von A und B zu einer Menge zusammengefasst.
- Dabei werden mehrfach vorkommende Elemente natürlich nur einmal aufgeführt.

Beispiel 2.3

Sei $A = \{1, 2, 5\}$ und $B = \{3, 5, 6\}$. Dann gilt

$$A \cup B = \{1, 2, 3, 5, 6\}.$$

Menge der Variablen einer aussagenlogischen Formel

Sei $\gamma \in \mathcal{A}$ eine aussagenlogische Formel.

Die Menge V_γ der aussagenlogischen Variablen in γ definieren wir rekursiv wie folgt:

(i) $V_\gamma = \emptyset$, falls $\gamma \in \{\underline{0}, \underline{1}\}$,

(ii) $V_\gamma = \{\gamma\}$, falls $\gamma \in V$,

(iii) $V_\gamma = V_\alpha$, falls $\gamma = \neg\alpha$,
$V_\gamma = V_\alpha \cup V_\beta$, falls $\gamma = (\alpha \wedge \beta)$ oder $\gamma = (\alpha \vee \beta)$.

Belegung

Sei $\gamma \in \mathcal{A}$ eine aussagenlogische Formel.

Mit einer Belegung $\mathcal{I}$ wird jeder Variablen $v \in V_\gamma$ genau ein Wahrheitswert zugewiesen.

$$\begin{aligned} \mathcal{I} \quad : \quad & V_\gamma \to \mathbb{B} \\ & v \mapsto \mathcal{I}(v) \end{aligned}$$

Dabei gibt es für jede Variable $v \in V_\gamma$ genau zwei mögliche Belegungen:

$$\mathcal{I}(v) = 0 \quad \text{oder} \quad \mathcal{I}(v) = 1$$

Gilt $|V_\gamma| = n$, dann gibt es 2^n mögliche Belegungen $\mathcal{I} : V_\gamma \to \mathbb{B}$.

$$\mathcal{I}_\gamma = \{\mathcal{I} | \mathcal{I} : V_\gamma \to \mathbb{B}\}$$

bezeichnet die Menge der möglichen Belegungen für γ.

Interpretation

Die Interpretation einer aussagenlogischen Formel $\gamma \in \mathcal{A}$ erfolgt rekursiv entlang der syntaktischen Regeln.

Mit einer gewählten Belegung $\mathcal{I} \in \mathcal{I}_\gamma$ wird die Interpretation $\mathcal{I}^*(\gamma)$ einer aussagenlogischen Formel $\gamma \in \mathcal{A}$ gemäß den folgenden Regeln berechnet:

(i) Für $\gamma \in \{\underline{0}, \underline{1}\}$ ist $\mathcal{I}^*(\underline{0}) = 0$ und $\mathcal{I}^*(\underline{1}) = 1$.
Die Konstantenbezeichner werden also unabhängig von der gegebenen Formel γ durch fest zugewiesene Wahrheitswerte interpretiert.

(ii) Für $v \in V_\gamma$: $\mathcal{I}^*(v) = \mathcal{I}(v)$
Die Variablen $v \in V_\gamma$ der Formel γ werden durch die gewählte Belegung $\mathcal{I}$ interpretiert.

(iii) Die Interpretation zusammengesetzter Formeln wird gemäß folgender Regeln berechnet:
Ist $\gamma = (\alpha \wedge \beta)$ mit $\alpha, \beta \in \mathcal{A}$, dann ist

$$\mathcal{I}^*(\gamma) = \mathcal{I}^*(\alpha \wedge \beta) = \min\{\mathcal{I}^*(\alpha), \mathcal{I}^*(\beta)\}.$$

Ist $\gamma = (\alpha \vee \beta)$ mit $\alpha, \beta \in \mathcal{A}$, dann ist

$$\mathcal{I}^*(\gamma) = \mathcal{I}^*(\alpha \vee \beta) = \max\{\mathcal{I}^*(\alpha), \mathcal{I}^*(\beta)\}.$$

Ist $\gamma = \neg\alpha$ mit $\alpha \in \mathcal{A}$, dann ist

$$\mathcal{I}^*(\gamma) = \mathcal{I}^*(\neg\alpha) = 1 - \mathcal{I}^*(\alpha).$$

Beispiel 2.4

Wir betrachten die Formel

$$\gamma = (((p \vee (q \wedge r)) \wedge \neg(q \vee \neg r)) \vee \underline{0})$$

aus Beispiel 2.1 (ii). Es ist $V_\gamma = \{p, q, r\}$. Wir wählen die Belegung

$$\mathcal{I}(p) = 1, \mathcal{I}(q) = 0, \mathcal{I}(r) = 1.$$

Mit dieser Belegung ergibt sich die Interpretation

$$\begin{aligned}
\mathcal{I}^*(\gamma) &= \mathcal{I}^*(((p \vee (q \wedge r)) \wedge \neg(q \vee \neg r)) \vee \underline{0}) \\
&= \max\{\mathcal{I}^*((p \vee (q \wedge r)) \wedge \neg(q \vee \neg r), \mathcal{I}^*(\underline{0})\} \\
&= \max\{\min\{\mathcal{I}^*(p \vee (q \wedge r)), \mathcal{I}^*(\neg(q \vee \neg r))\}, 0\} \\
&= \max\{\min\{\max\{\mathcal{I}^*(p), \mathcal{I}^*(q \wedge r)\}, 1 - \mathcal{I}^*(q \vee \neg r)\}, 0\} \\
&= \max\{\min\{\max\{\mathcal{I}(p), \min\{\mathcal{I}^*(q), \mathcal{I}^*(r)\}\}, \\
&\qquad 1 - \max\{\mathcal{I}^*(q), \mathcal{I}^*(\neg r)\}\}, 0\}
\end{aligned}$$

Fortsetzung Beispiel.

$$
\begin{aligned}
&= \max\{\min\{\max\{1, \min\{\mathcal{I}(q), \mathcal{I}(r)\}\}, 1 - \max\{\mathcal{I}(q), 1 - \mathcal{I}^*(r)\}\}, 0\} \\
&= \max\{\min\{\max\{1, \min\{0, 1\}\}, 1 - \max\{0, 1 - \mathcal{I}(r)\}\}, 0\} \\
&= \max\{\min\{\max\{1, \min\{0, 1\}\}, 1 - \max\{0, 1 - 1\}\}, 0\} \\
&= \max\{\min\{\max\{1, 0\}, 1 - 0\}, 0\} \\
&= \max\{\min\{1, 1\}, 0\} \\
&= \max\{1, 0\} \\
&= 1
\end{aligned}
$$

Syntaktische Vereinbarungen

- Da wir die Operatoren $\underline{0}$ und $\underline{1}$ mit festen Werten interpretieren, unterscheiden wir nicht mehr zwischen den Operatoren $\underline{0}$ bzw. $\underline{1}$ und den zugeordneten Werte 0 bzw. 1. Wir schreiben von nun an also in Formeln 0 bzw. 1 anstelle von $\underline{0}$ bzw. $\underline{1}$.
- Weiterhin vereinbaren wir, dass der Operator $\neg$ stärker bindet als der Operator $\wedge$, und dieser stärker als $\vee$. Dies hilft, Klammern einzusparen.
- Bei zusammengesetzten Formel können wir auch auf die äußeren Klammern verzichten.
- Wir dürfen also $\alpha \wedge \beta \vee \gamma$ anstelle von $((\alpha \wedge \beta) \vee \gamma)$ schreiben.
- Achtung: In $(\alpha \vee \beta) \wedge \gamma$ können wir nicht auf die Klammern verzichten.

Wahrheitstafeln

α	$\neg\alpha$
1	0
0	1

α	β	$\alpha \wedge \beta$
0	0	0
0	1	0
1	0	0
1	1	1

α	β	$\alpha \vee \beta$
0	0	0
0	1	1
1	0	1
1	1	1

- $\neg$ Negation
- $\wedge$ Konjunktion
- $\vee$ Disjunktion

Beispiel 2.5

Die Wahrheitstafel der Formel

$$\gamma = ((p \vee (q \wedge r)) \wedge \neg(q \vee \neg r)) \vee 0$$

ist:

p	q	r	$\underline{0}$	$\neg r$	$q \wedge r$	$q \vee \neg r$	$\neg(q \vee \neg r)$	$p \vee (q \wedge r)$	$(p \vee (q \wedge r)) \wedge \neg(q \vee \neg r)$	$((p \vee (q \wedge r)) \wedge \neg(q \vee \neg r)) \vee 0$
1	1	1	0	0	1	1	0	1	0	0
1	1	0	0	1	0	1	0	1	0	0
1	0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	0	1	0	1	0	0
0	1	1	0	0	1	1	0	1	0	0
0	1	0	0	1	0	1	0	0	0	0
0	0	1	0	0	0	0	1	0	0	0
0	0	0	0	1	0	1	0	0	0	0

Aussagenlogische Operationen

Wir führen weitere aussagenlogische Operationen ein:

- die Subjunktion $\rightarrow$ (aus α folgt β)
- die Bijunktion $\leftrightarrow$ (α genau dann, wenn β)
- das exklusive Oder $\oplus$ (entweder α oder β)

Die Operationen haben folgende Syntax und Semantik:

α	β	$\alpha \rightarrow \beta$
1	1	1
1	0	0
0	1	1
0	0	1

α	β	$\alpha \leftrightarrow \beta$
1	1	1
1	0	0
0	1	0
0	0	1

α	β	$\alpha \oplus \beta$
1	1	0
1	0	1
0	1	1
0	0	0

Folgerung 2.6

Für jede Belegung $\mathcal{I}$ der Variablen in aussagenlogischen Formeln α, β gilt:

$$\begin{aligned}
\mathcal{I}^*(\alpha \to \beta) &= \mathcal{I}^*(\neg\alpha \vee \beta) \\
\mathcal{I}^*(\alpha \leftrightarrow \beta) &= \mathcal{I}^*((\alpha \to \beta) \wedge (\beta \to \alpha)) \\
\mathcal{I}^*(\alpha \oplus \beta) &= \mathcal{I}^*((\alpha \wedge \neg\beta) \vee (\neg\alpha \wedge \beta))
\end{aligned}$$

Beweis.

Wir vergleichen einfach die Wahrheitstafeln der aussagenlogischen Formeln (hier nur für die erste Gleichung):

α	β	$\alpha \to \beta$
1	1	1
1	0	0
0	1	1
0	0	1

α	β	$\neg\alpha \vee \beta$
1	1	1
1	0	0
0	1	1
0	0	1

Bemerkung: $\mathcal{I}^*(\neg\alpha \vee \beta) = \max\{1 - \mathcal{I}^*(\alpha), \mathcal{I}^*(\beta)\}$

Beispiel 2.7

Für jede Belegung $\mathcal{I}$ der aussagenlogischen Formeln $\alpha, \beta \in \mathcal{A}$ gilt

$$\mathcal{I}^*(\alpha \wedge \neg\beta) = \mathcal{I}^*(\neg(\alpha \rightarrow \beta))$$

Beweis:

$$\begin{aligned}
\mathcal{I}^*(\alpha \wedge \neg\beta) &= \min\{\mathcal{I}^*(\alpha), 1 - \mathcal{I}^*(\beta)\} \\
&= 1 - \max\{1 - \mathcal{I}^*(\alpha), \mathcal{I}^*(\beta)\} \\
&= 1 - \mathcal{I}^*(\neg\alpha \vee \beta) \\
&= 1 - \mathcal{I}^*(\alpha \rightarrow \beta) \\
&= \mathcal{I}^*(\neg(\alpha \rightarrow \beta))
\end{aligned}$$

Erfüllbarkeit

Definition 2.8

Sei $\alpha \in \mathcal{A}$ eine aussagenlogische Formel und $\mathcal{F}$ eine endliche Menge aussagenlogischer Formeln aus $\mathcal{A}$.

(i) α heißt erfüllbar genau dann, wenn eine Belegung $\mathcal{I}$ von α existiert mit $\mathcal{I}^*(\alpha) = 1$.

(ii) α heißt Tautologie oder allgemeingültig genau dann, wenn für jede Belegung $\mathcal{I}$ von α gilt $\mathcal{I}^*(\alpha) = 1$.

(iii) α heißt Kontradiktion, widerspruchsvoll oder unerfüllbar genau dann, wenn für jede Belegung $\mathcal{I}$ von α gilt $\mathcal{I}^*(\alpha) = 0$.

(iv) $\mathcal{F}$ heißt erfüllbar genau dann, wenn es eine Belegung $\mathcal{I}$ von $\mathcal{F}$ gibt, so dass $\mathcal{I}^*(\gamma) = 1$ für alle $\gamma \in \mathcal{F}$ ist. $\mathcal{I}$ heißt dann Modell für $\mathcal{F}$.
Gibt es zu $\mathcal{F}$ kein Modell, dann heißt $\mathcal{F}$ unerfüllbar.

Beispiel 2.9

(i) Die Formeln

$$p \wedge q \quad \text{und} \quad (p \wedge q) \vee (q \to r)$$

sind erfüllbar aber keine Tautologien.

(ii) Die Formeln

$$p \vee \neg p \quad \text{und} \quad (p \to q) \leftrightarrow (\neg p \vee q)$$

sind Tautologien.

(iii) Die Formel $p \wedge \neg p$ ist eine Kontradiktion.

(iv) Die Menge

$$\mathcal{F}_1 = \{p \vee q, q \wedge \neg r, (p \wedge q) \vee (q \to r)\}$$

ist erfüllbar, denn $\mathcal{I}(p) = \mathcal{I}(q) = 1, \mathcal{I}(r) = 0$ ist ein Modell für $\mathcal{F}_1$.

(v) Die Menge $\mathcal{F}_2 = \{p, p \to q, \neg q\}$ ist unerfüllbar.

Erfüllbarkeit und Wahrheitstafel

Folgerung 2.10

(i) *Eine Formel ist genau dann erfüllbar, wenn in der Ergebnisspalte ihrer Wahrheitstafel mindestens eine* 1 *vorkommt.*

(ii) *Eine Formel ist genau dann eine Tautologie, wenn in der Ergebnisspalte ihrer Wahrheitstafel nur Einsen vorkommen.*

(iii) *Eine Formel ist genau dann widerspruchsvoll, wenn in der Ergebnisspalte ihrer Wahrheitstafel nur Nullen vorkommen.*

Logische Folgerung

Definition 2.11

Sei $\alpha \in \mathcal{A}$ eine aussagenlogische Formel und $\mathcal{F}$ eine endliche Menge aussagenlogischer Formeln aus $\mathcal{A}$.

α heißt logische Folgerung von $\mathcal{F}$ genau dann, wenn $\mathcal{I}^*(\alpha) = 1$ für jedes Modell $\mathcal{I}$ von $\mathcal{F}$ ist. Wir schreiben

$$\mathcal{F} \models \alpha$$

und sprechen „aus $\mathcal{F}$ folgt α (logisch)“.

Bemerkung: Statt von logischer Folgerung spricht man auch von semantischer Folgerung und sagt, dass „α aus $\mathcal{F}$ semantisch folgt“.

Beispiel 2.12

(i) Für $\mathcal{F} = \{p, q\}$ gilt $\mathcal{F} \models p \wedge q$, denn für jedes Modell $\mathcal{I}$ von $\mathcal{F}$ muss $\mathcal{I}(p) = 1$ und $\mathcal{I}(q) = 1$ gelten, damit gilt aber auch $\mathcal{I}^*(p \wedge q) = 1$.

(ii) Für $\mathcal{F} = \{p \to q, q \to r\}$ gilt $\mathcal{F} \models p \to r$, denn $\mathcal{F}$ besitzt die Modelle

$$\begin{array}{llll} (1) & \mathcal{I}(p) = 1 & \mathcal{I}(q) = 1 & \mathcal{I}(r) = 1 \\ (2) & \mathcal{I}(p) = 0 & \mathcal{I}(q) = 1 & \mathcal{I}(r) = 1 \\ (3) & \mathcal{I}(p) = 0 & \mathcal{I}(q) = 0 & \mathcal{I}(r) = 1 \\ (4) & \mathcal{I}(p) = 0 & \mathcal{I}(q) = 0 & \mathcal{I}(r) = 0 \end{array}$$

und für jedes dieser Modelle gilt $\mathcal{I}^*(p \to r) = 1$.

(iii) Für $\mathcal{F} = \{p \to r, q \vee r\}$ gilt nicht $\mathcal{F} \models p \wedge r$, denn die Belegung $\mathcal{I}(p) = 0, \mathcal{I}(q) = \mathcal{I}(r) = 1$ ist ein Modell von $\mathcal{F}$, aber $\mathcal{I}^*(p \wedge r) = 0$.

Bemerkung: Wenn aus $\mathcal{F}$ eine Formel α nicht gefolgert werden kann, notieren wir dies auch in der Form

$$\mathcal{F} \not\models \alpha.$$

Zusammenhang von logischer Folgerung und Unerfüllbarkeit

Satz 2.13

Sei $\mathcal{F} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ eine Menge aussagenlogischer Formeln und $\beta \in \mathcal{A}$.

Dann gilt $\mathcal{F} \models \beta$ genau dann, wenn $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \neg\beta\}$ unerfüllbar ist.

Bemerkung: Dieser Satz ist wichtig für die Programmierung von automatischen Beweisern, die die Gültigkeit von Formeln nachweisen wollen.

Beweis.

Wir zeigen:

(i) Wenn $\mathcal{F} \models \beta$ gilt, dann ist $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \neg\beta\}$ unerfüllbar.

(ii) Wenn $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \neg\beta\}$ unerfüllbar ist, dann gilt $\mathcal{F} \models \beta$.

Zu (i): Sei $\mathcal{I}$ ein Modell für $\mathcal{F}$.

- D. h. $\mathcal{I}^*(\alpha_i) = 1$ für alle i.
- Wegen $\mathcal{F} \models \beta$ gilt dann auch $\mathcal{I}^*(\beta) = 1$.
- Daraus folgt $\mathcal{I}^*(\neg\beta) = 0$.
- Somit gibt es keine Interpretation $\mathcal{I}$ mit $\mathcal{I}^*(\alpha_i) = 1$ für alle i und $\mathcal{I}^*(\neg\beta) = 1$.
- Also ist $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \neg\beta\}$ unerfüllbar.

Fortsetzung Beweis.

Zu (ii): Sei $\mathcal{I}$ ein beliebiges Modell für $\mathcal{F}$.

- D. h. $\mathcal{I}^*(\alpha_i) = 1$ für alle i.
- Da $\{\alpha_1, \alpha_2, \ldots, \alpha_n, \neg\beta\}$ unerfüllbar ist, muss $\mathcal{I}^*(\neg\beta) = 0$ gelten (ansonsten wäre die Menge erfüllbar).
- Damit gilt aber $\mathcal{I}^*(\beta) = 1$
- und somit $\mathcal{F} \models \beta$.

Folgerung 2.14

(i) *Eine Formel $\beta \in \mathcal{A}$ ist eine Tautologie genau dann, wenn $\neg\beta$ eine Kontradiktion ist.*

(ii) *$\beta \in \mathcal{A}$ ist eine Tautologie genau dann, wenn $\emptyset \models \beta$ gilt.*

(iii) *Ist $\mathcal{F}$ eine unerfüllbare Formelmenge, dann gilt $\mathcal{F} \models \beta$ für jede Formel $\beta \in \mathcal{A}$.*

Bemerkungen:

- Statt $\emptyset \models \beta$ schreibt man üblicherweise $\models \beta$.
- Aussage (iii) bedeutet, dass man aus einer unerfüllbaren Formelmenge jede beliebige Formel folgern kann.

Beweis.

(i) Folgt unmittelbar aus Definition 2.8.

(ii) Folgt aus Satz 2.13 mit $\mathcal{F} = \emptyset$.

(iii) Wenn $\mathcal{F} = \{\alpha_1, \ldots, \alpha_n\}$ unerfüllbar ist, dann ist auch $\{\alpha_1, \ldots, \alpha_n, \neg\beta\}$ unerfüllbar.

Mit Satz 2.13 folgt $\mathcal{F} \models \beta$.

Deduktion und Modus Ponens

Satz 2.15

(i) *Für jede Menge* $\mathcal{F} = \{\alpha_1, \ldots, \alpha_n\}$ *aussagenlogischer Formeln und für alle* $\beta, \gamma \in \mathcal{A}$ *gilt*

$$\{\alpha_1, \ldots, \alpha_n, \beta\} \models \gamma \text{ genau dann, wenn } \mathcal{F} \models \beta \to \gamma$$

gilt.

(ii) *Für alle Formeln* $\alpha, \beta \in \mathcal{A}$ *gilt*

$$\{\alpha, \alpha \to \beta\} \models \beta.$$

Beweis.

(i) Es gilt $\{\alpha_1, \ldots, \alpha_n\} \models \beta \to \gamma$

gdw.	$\{\alpha_1, \ldots, \alpha_n, \neg(\beta \to \gamma)\}$	unerfüllbar ist
gdw.	$\{\alpha_1, \ldots, \alpha_n, \beta \wedge \neg\gamma\}$	unerfüllbar ist
gdw.	$\{\alpha_1, \ldots, \alpha_n, \beta, \neg\gamma\}$	unerfüllbar ist
gdw.	$\{\alpha_1, \ldots, \alpha_n, \beta\} \models \gamma$	gilt.

(ii) Es gilt

$$\{\alpha, \alpha \to \beta\} \models \beta$$

genau dann, wenn

$$\{\alpha, \alpha \to \beta, \neg\beta\}$$

unerfüllbar ist. ✎

Satz 2.16

Es seien $\mathcal{F}$ eine Menge aussagenlogischer Formeln und $\alpha \in \mathcal{A}$. Dann gelten die folgenden Aussagen:

(i) *Gilt $\mathcal{F} \models \alpha$, dann auch $\mathcal{F} \cup \{\beta\} \models \alpha$ für alle Formeln $\beta \in \mathcal{A}$.*

(ii) *Gilt $\mathcal{F} \models \alpha$ und ist $\beta \in \mathcal{A}$ allgemeingültig, dann gilt $\mathcal{F} \setminus \{\beta\} \models \alpha$.*

Bemerkung: $\mathcal{F} \setminus \{\beta\}$ bedeutet, dass die Formel β aus der Formelmenge $\mathcal{F}$ entfernt wird.

Beweis.

Übungsaufgabe.

Implikation

Definition 2.17

Gilt für aussagenlogische Formeln $\alpha_1, \alpha_2, \ldots, \alpha_n$ und β, dass die Subjunktion

$$(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n) \rightarrow \beta$$

eine Tautologie ist, dann heißt diese Subjunktion Implikation, und wir schreiben

$$(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n) \Rightarrow \beta$$

und sprechen „$\alpha_1, \alpha_2, \ldots, \alpha_n$ implizieren β“.

Beispiel 2.18

Es seien $\alpha, \beta, \gamma \in \mathcal{A}$, dann gelten die folgenden Implikationen.

(i) Abschwächung der Nachbedingung:

$$\alpha \Rightarrow (\alpha \vee \beta)$$

(ii) Verschärfung der Vorbedingung:

$$(\alpha \wedge \beta) \Rightarrow \alpha$$

(iii) Kettenschluss:

$$(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma) \Rightarrow (\alpha \rightarrow \gamma)$$

Überprüfung: ✎

$\rightarrow$ vs. $\Rightarrow$

Auf den ersten Blick scheinen die Symbole „$\rightarrow$“ und „$\Rightarrow$“ dasselbe zu bedeuten. Dies ist aber nicht der Fall.

- $\rightarrow$ ist ein Symbol in der Sprache der Aussagenlogik. Es verknüpft zwei logische Formeln miteinander.
- Das Symbol $\Rightarrow$ verwenden wir dagegen metasprachlich, um eine Aussage über eine Eigenschaft aussagenlogischer Formeln zu machen.

Äquivalenz der Folgerungsbegriffe

Satz 2.19

Für aussagenlogische Formeln $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta$ *gilt*

$$\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \models \beta \text{ genau dann, wenn } (\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n) \Rightarrow \beta$$

gilt.

Beweis.

Wir setzen $\mathcal{F} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ und zeigen:

(i) Wenn $\mathcal{F} \models \beta$ gilt, dann gilt auch $(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n) \Rightarrow \beta$.

(ii) Wenn $(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n) \Rightarrow \beta$ gilt, dann gilt auch $\mathcal{F} \models \beta$.

Syntaktische Folgerung

- Syntaktische Folgerung heißt, dass eine Folgerung vorgenommen wird, ohne die Semantik der beteiligten Formeln zu berechnen.
- Die Folgerung geschieht, indem in einer Formel Teilformeln durch andere Formeln ersetzt werden.
- Diese Ersetzung von Formeln geschieht wiederum mithilfe sogenannter Inferenzregeln.

Inferenzregel

Definition 2.20

(i) Seien $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta$ aussagenlogische Formeln, für die die Implikation $(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n) \Rightarrow \beta$ gilt.

Dann heißt

$$\frac{\alpha_1, \alpha_2, \ldots, \alpha_n}{\beta}$$

Ableitungs- oder Inferenzregel. Die Formelmenge $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ heißt Prämisse und β heißt Konklusion dieser Inferenzregel.

Fortsetzung Definition.

(ii) Sei

- γ eine aussagenlogische Formel,
- $\mathcal{F} = \{\alpha_1, \ldots, \alpha_n\}$ eine Menge aussagenlogischer Formeln,
- $\{\beta_1, \ldots, \beta_k\}$ irgendeine Auswahl von Formeln aus $\mathcal{F}$ und
- $\{\gamma_1, \ldots, \gamma_m\}$ die Menge der nicht ausgewählten Formeln aus $\mathcal{F}$ sowie
- $$\frac{\beta_1, \beta_2, \ldots, \beta_k}{\gamma}$$

  eine Inferenzregel,

dann heißt $\{\gamma_1, \gamma_2, \ldots, \gamma_m, \gamma\}$ ableitbar aus $\mathcal{F}$, und wir schreiben

$$\mathcal{F} \vdash \{\gamma_1, \gamma_2, \ldots, \gamma_m, \gamma\}.$$

Fortsetzung Definition.

(iii) Eine aussagenlogische Formel γ ist ableitbar aus einer Menge $\mathcal{F}$ von aussagenlogischen Formeln, falls es Mengen aussagenlogischer Formeln $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_r, r \geq 0$ gibt mit

$$\mathcal{F} \vdash \mathcal{F}_1 \vdash \mathcal{F}_2 \vdash \cdots \vdash \mathcal{F}_r \vdash \{\gamma\}.$$

Wir notieren dann $\mathcal{F} \vdash \gamma$ und sagen, dass γ logisch aus $\mathcal{F}$ ableitbar ist.

Beispiel 2.21

(i) Modus Ponens als Inferenzregel:

$$\frac{\alpha, \alpha \to \beta}{\beta}$$

(ii) Modus Tollens:

$$\frac{\alpha \to \beta, \neg\beta}{\neg\alpha}$$

(iii) Reduction ad absurdum:

$$\frac{(\gamma \vee \alpha) \to \beta, (\gamma \vee \alpha) \to \neg\beta}{\neg\alpha}$$

(iv) Kettenschluss:

$$\frac{\alpha \to \beta, \beta \to \gamma}{\alpha \to \gamma}$$

Fortsetzung Beispiel.

(v) Es gilt

$$\{\alpha \to \beta, \neg\beta, \neg\alpha \to \gamma\} \vdash \{\neg\alpha, \neg\alpha \to \gamma\} \vdash \{\gamma\}$$

und damit

$$\{\alpha \to \beta, \neg\beta, \neg\alpha \to \gamma\} \vdash \gamma.$$

Die erste Ableitung erfolgt mithilfe des Modus Tollens, die zweite mithilfe des Modus Ponens.

Kalkül

- Die logische Ableitung geschieht, indem eine Menge von aussagenlogischen Formeln aufgrund von Inferenzregeln oder bereits durchgeführten logischen Ableitungen verändert wird.
- Die Semantik der Formeln wird dabei niemals betrachtet.
- Die korrekte Semantik wird nur einmalig für die benutzten Inferenzregeln vorausgesetzt (Definition 2.20).
- Solche syntaktischen Ableitungssysteme nennt man Kalküle.
- Kalküle sind gut geeignet für die Programmierung von logischen Schlussfolgerungsmechanismen auf Rechnern, z. B. in der Künstlichen Intelligenz.

Korrektheit und Vollständigkeit

Kriterien für einen Kalkül:

- Widerspruchsfreiheit bzw. Korrektheit:

  $$\text{Gilt } \mathcal{F} \vdash \alpha, \text{ dann gilt auch } \mathcal{F} \models \alpha.$$

  Jede syntaktisch abgeleitete Formel ist semantisch korrekt.
- Vollständigkeit:

  $$\text{Gilt } \mathcal{F} \models \alpha, \text{ dann gilt auch } \mathcal{F} \vdash \alpha.$$

  Jede semantisch korrekte Formel lässt sich auch syntaktisch ableiten.

Im übernächsten Abschnitt lernen Sie einen korrekten und vollständigen Kalkül für die Aussagenlogik kennen.

Logische Äquivalenz

Definition 2.22

Zwei aussagenlogische Formeln $\alpha, \beta \in \mathcal{A}$ heißen logisch äquivalent, falls für jede Belegung $\mathcal{I}$ von α und β gilt:

$$\mathcal{I}^*(\alpha) = \mathcal{I}^*(\beta).$$

Schreibweise: $\alpha \equiv \beta$.

Beispiel 2.23

Aus Folgerung 2.6 ergibt sich:

$$\begin{aligned} \alpha \to \beta &\equiv \neg\alpha \vee \beta \\ \alpha \leftrightarrow \beta &\equiv (\alpha \to \beta) \wedge (\beta \to \alpha) \\ \alpha \oplus \beta &\equiv (\alpha \wedge \neg\beta) \vee (\neg\alpha \wedge \beta) \end{aligned}$$

Wichtige aussagenlogische Äquivalenzen

Satz 2.24

Kommutativität

$$\begin{aligned} \alpha \vee \beta &\equiv \beta \vee \alpha \\ \alpha \wedge \beta &\equiv \beta \wedge \alpha \\ \alpha \oplus \beta &\equiv \beta \oplus \alpha \\ \alpha \leftrightarrow \beta &\equiv \beta \leftrightarrow \alpha \end{aligned}$$

Assoziativität

$$\begin{aligned} \alpha \vee (\beta \vee \gamma) &\equiv (\alpha \vee \beta) \vee \gamma \\ \alpha \wedge (\beta \wedge \gamma) &\equiv (\alpha \wedge \beta) \wedge \gamma \\ \alpha \oplus (\beta \oplus \gamma) &\equiv (\alpha \oplus \beta) \oplus \gamma \\ \alpha \leftrightarrow (\beta \leftrightarrow \gamma) &\equiv (\alpha \leftrightarrow \beta) \leftrightarrow \gamma \end{aligned}$$

Fortsetzung Satz.

Distributivität

$$\begin{aligned} \alpha \vee (\beta \wedge \gamma) &\equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma) \\ \alpha \wedge (\beta \vee \gamma) &\equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) \end{aligned}$$

De Morgansche Regeln

$$\begin{aligned} \neg(\alpha \vee \beta) &\equiv \neg\alpha \wedge \neg\beta \\ \neg(\alpha \wedge \beta) &\equiv \neg\alpha \vee \neg\beta \end{aligned}$$

Einführung der Negation

$$\begin{aligned} \neg\alpha &\equiv \alpha \rightarrow 0 \\ \neg\alpha &\equiv \alpha \leftrightarrow 0 \\ \neg\alpha &\equiv \alpha \oplus 1 \end{aligned}$$

Fortsetzung Satz.

Doppelte Negation

$$\neg\neg\alpha \equiv \alpha$$

Idempotenz

$$\begin{aligned} \alpha \vee \alpha &\equiv \alpha \\ \alpha \wedge \alpha &\equiv \alpha \end{aligned}$$

Absorption

$$\begin{aligned} 1 \wedge \alpha &\equiv \alpha \\ 0 \vee \alpha &\equiv \alpha \\ 1 \rightarrow \alpha &\equiv \alpha \\ 1 \leftrightarrow \alpha &\equiv \alpha \\ \alpha \vee (\alpha \wedge \beta) &\equiv \alpha \\ \alpha \wedge (\alpha \vee \beta) &\equiv \alpha \end{aligned}$$

Fortsetzung Satz.

Tautologien

$$
\begin{aligned}
1 \vee \alpha &\equiv 1 \\
\neg\alpha \vee \alpha &\equiv 1 \\
\alpha \rightarrow \alpha &\equiv 1 \\
\alpha \rightarrow 1 &\equiv 1 \\
0 \rightarrow \alpha &\equiv 1 \\
\alpha \leftrightarrow \alpha &\equiv 1
\end{aligned}
$$

Unerfüllbarkeitsregeln

$$
\begin{aligned}
0 \wedge \alpha &\equiv 0 \\
\neg\alpha \wedge \alpha &\equiv 0 \\
\alpha \oplus \alpha &\equiv 0
\end{aligned}
$$

Fortsetzung Satz.

Kontraposition

$$\alpha \rightarrow \beta \quad \equiv \quad \neg\beta \rightarrow \neg\alpha$$

Beweis.

Tafel ✎ und Übungsaufgabe.

Äquivalenz

Definition 2.25

Gilt für aussagenlogische Formeln α und β, dass die Bijunktion $\alpha \leftrightarrow \beta$ eine Tautologie ist, dann heißt diese Bijunktion Äquivalenz, und wir schreiben

$$\alpha \Leftrightarrow \beta.$$

Satz 2.26

Seien $\alpha, \beta \in \mathcal{A}$ aussagenlogische Formeln, dann gilt

$$\alpha \equiv \beta \text{ genau dann, wenn } \alpha \Leftrightarrow \beta$$

gilt.

Beweis.

Tafel ✎.

Folgerung 2.27

Eine aussagenlogische Formel $\alpha \in \mathcal{A}$ ist allgemeingültig genau dann, wenn

$$\alpha \equiv 1$$

oder

$$\alpha \Leftrightarrow 1$$

gilt.

NAND und NOR

Wir kennen bisher fünf zweistellige Verknüpfungen:

$$\vee, \wedge, \rightarrow, \leftrightarrow, \oplus$$

Wir führen noch zwei weitere Verknüpfungen ein:

- $\alpha \uparrow \beta$ (NAND)
- $\alpha \downarrow \beta$ (NOR)

definiert durch

α	β	$\alpha \uparrow \beta$
1	1	0
1	0	1
0	1	1
0	0	1

bzw.

α	β	$\alpha \downarrow \beta$
1	1	0
1	0	0
0	1	0
0	0	1

Folgerung 2.28

Für aussagenlogische Formeln $\alpha, \beta \in \mathcal{A}$ gilt:

(i)

$$\alpha \uparrow \beta \equiv \neg(\alpha \wedge \beta)$$

(ii)

$$\alpha \downarrow \beta \equiv \neg(\alpha \vee \beta)$$

Beweis.

Tafel ✎.

Anzahl aussagenlogischer Verknüpfungen

Satz 2.29

Es gibt $2^{(2^n)}$ n-stellige aussagenlogische Verknüpfungen.

Beweis.

- Eine Wahrheitstafel mit n aussagenlogischen Variablen hat 2^n Zeilen.
- Für jede Zeile kann die Ergebnisspalte die zwei Werte 0 oder 1 annehmen.
- Anzahl an Möglichkeiten: $2^{\text{Anzahl Zeilen}} = 2^{(2^n)}$.

Folgerung 2.30

Es gibt $2^{(2^2)} = 16$ verschiedene zweistellige aussagenlogische Verknüpfungen.

Verknüpfungen durch andere Verknüpfungen ausdrücken

- Nicht alle der 16 zweistelligen Verknüpfungen werden benötigt, denn
- wir können Verknüpfungen durch andere Verknüpfungen ausdrücken.
- Finde eine minimale Anzahl an Verknüpfungen, mit denen alle anderen ausgedrückt werden können!

Beispiel 2.31

(i) Aus Folgerung 2.6 kennen wir

$$\begin{aligned} \alpha \to \beta &\equiv \neg\alpha \vee \beta \\ \alpha \leftrightarrow \beta &\equiv (\neg\alpha \vee \beta) \wedge (\neg\beta \vee \alpha) \\ \alpha \oplus \beta &\equiv (\alpha \wedge \neg\beta) \vee (\neg\alpha \wedge \beta) \end{aligned}$$

Subjunktion, Bijunktion und exklusives Oder sind also durch Negation, Disjunktion und Konjunktion darstellbar.

Fortsetzung Beispiel.

(ii) Doppelte Negation und De Morgansche Regeln (siehe Satz 2.24) liefern:

$$\begin{array}{lcccl} \alpha \wedge \beta & \equiv & \neg\neg(\alpha \wedge \beta) & \equiv & \neg(\neg\alpha \vee \neg\beta) \\ \alpha \vee \beta & \equiv & \neg\neg(\alpha \vee \beta) & \equiv & \neg(\neg\alpha \wedge \neg\beta) \end{array}$$

Konjunktion lässt sich also durch Negation und Disjunktion, Disjunktion durch Negation und Konjunktion darstellen.

(iii) Idempotenz und Folgerung 2.28 liefern:

$$\neg\alpha \equiv \neg(\alpha \vee \alpha) \equiv \alpha \downarrow \alpha$$

Die Negation lässt sich also durch NOR ausdrücken.

(iv) Aus (ii) und (iii) ergibt sich mit Folgerung 2.28 (ii):

$$\alpha \wedge \beta \equiv \neg(\neg\alpha \vee \neg\beta) \equiv \neg\alpha \downarrow \neg\beta \equiv (\alpha \downarrow \alpha) \downarrow (\beta \downarrow \beta)$$

Die Konjunktion lässt sich also alleine durch NOR ausdrücken.

Aussagenlogische Basen

Es sei $\mathbb{B}^{(4)}$ die Menge aller zweistelligen aussagenlogischen Verknüpfungen und $\mathbb{B}^{(4)^*} = \mathbb{B}^{(4)} \cup \{\neg\}$ diese Menge einschließlich Negation.

Definition 2.32

Sei $\mathcal{O} \subseteq \mathbb{B}^{(4)^*}$ eine Auswahl von aussagenlogischen Verknüpfungen.

(i) Eine zweistellige aussagenlogische Verknüpfung $\circ \in \mathbb{B}^{(4)}$ heißt definierbar durch $\mathcal{O}$ genau dann, wenn für $\alpha, \beta, \gamma \in \mathcal{A}$ gilt:
- Ist $\alpha \circ \beta \equiv \gamma$, dann
- sind γ und die Teilformeln α und β allein mit Operatoren aus $\mathcal{O}$ zusammengesetzt.

(ii) Die Menge $\mathcal{O}$ heißt aussagenlogische Basis, falls jede Verknüpfung aus $\mathbb{B}^{(4)^*}$ durch $\mathcal{O}$ definierbar ist.

Satz 2.33

Die folgenden Mengen aussagenlogischer Verknüpfungen bilden aussagenlogische Basen:

Boolsche Basis	$\{\neg, \vee, \wedge\}$
De Morgan-Basis	$\{\neg, \vee\}$ und $\{\neg, \wedge\}$
Frege-Basis	$\{\neg, \rightarrow\}$
NOR-Basis	$\{\downarrow\}$
NAND-Basis	$\{\uparrow\}$

Gottlob Frege

Gottlob Frege (1848-1925) war ein deutscher Logiker, Mathematiker und Philosoph. Er gilt als Begründer der modernen Logik.

Seine herausragende Leistung auf dem Gebiet der Logik besteht darin, als erster eine formale Sprache und, damit zusammenhängend, formale Beweise entwickelt zu haben („Begriffsschrift“).

Er schuf dadurch eine wesentliche Grundlage für die Informatik, sowie für formale Methoden in der linguistischen Semantik.

Disjunktive und konjunktive Normalform

Definition 2.34

(i) Eine aussagenlogische Formel $\alpha \in \mathcal{A}$ ist in disjunktiver Normalform (DNF), falls gilt:

$$\alpha = \alpha_1 \vee \ldots \vee \alpha_n$$

mit $\alpha_i = \alpha_{i1} \wedge \ldots \wedge \alpha_{ik_i}$, $1 \leq i \leq n$, wobei alle $\alpha_{ij}, 1 \leq j \leq k_i$ Literale sind.

(ii) Eine aussagenlogische Formel $\alpha \in \mathcal{A}$ ist in konjunktiver Normalform (KNF), falls gilt:

$$\alpha = \alpha_1 \wedge \ldots \wedge \alpha_n$$

mit $\alpha_i = \alpha_{i1} \vee \ldots \vee \alpha_{ik_i}$, $1 \leq i \leq n$, wobei alle $\alpha_{ij}, 1 \leq j \leq k_i$ Literale sind.

Die konjunktiv verknüpften Teilformeln α_i heißen Klauseln von α.

Eine Formel,

- in disjunktiver Normalform ist eine Disjunktion von Konjunktionen von Literalen,
- in konjunktiver Normalform ist eine Konjunktion von Disjunktionen von Literalen.

Beispiel 2.35

(i) Die Formel

$$(p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q) \vee (p \wedge q \wedge r) \vee (\neg q \wedge \neg r)$$

ist in disjunktiver Normalform.

(ii) Die Formel

$$(\neg p \vee q \vee r) \wedge (\neg p \vee \neg q) \wedge (\neg p \vee q \vee \neg r)$$

ist in konjunktiver Normalform.

Satz 2.36

(i) *Jede aussagenlogische Formel lässt sich in eine äquivalente aussagenlogische Formel in konjunktiver Normalform transformieren.*

(ii) *Jede aussagenlogische Formel lässt sich in eine äquivalente aussagenlogische Formel in disjunktiver Normalform transformieren.*

Beweisskizze.

1. Ersetze jedes Vorkommen von 1 durch $p \vee \neg p$ und jedes Vorkommen von 0 durch $q \wedge \neg q$, mit zwei neuen Variablen p bzw. q.
2. Ersetze die Operatoren $\rightarrow, \leftrightarrow, \oplus$ oder sonstige durch ihre Darstellung mit $\neg, \wedge, \vee$ (boolsche Basis).
3. Ersetze jedes Vorkommen einer Formel der Form $\neg\neg\alpha$ durch α.
4. Ziehe $\neg$ ganz nach innen bis $\neg$ nur noch vor Aussagenvariablen vorkommt. Wende dabei, falls möglich, auch (3) an.
5. Ziehe mit den Distributivgesetzen alle $\wedge$ nach aussen (KNF) bzw. nach innen (DNF).

Beispiel 2.37

$$
\begin{aligned}
((\alpha \to \beta) \to \gamma) \vee \delta &\equiv ((\neg\alpha \vee \beta) \to \gamma) \vee \delta \\
&\equiv (\neg(\neg\alpha \vee \beta) \vee \gamma) \vee \delta \\
&\equiv ((\alpha \wedge \neg\beta) \vee \gamma) \vee \delta \\
&\equiv ((\alpha \vee \gamma) \wedge (\neg\beta \vee \gamma)) \vee \delta \\
&\equiv (\alpha \vee \gamma \vee \delta) \wedge (\neg\beta \vee \gamma \vee \delta)
\end{aligned}
$$

Somit ist die Formel in KNF.

Klauselmengen

Definition 2.38

Sei

$$\alpha = (p_{11} \vee \ldots \vee p_{1k_1}) \wedge \ldots \wedge (p_{n1} \vee \ldots \vee p_{nk_n})$$

eine in aussagenlogische Formel in KNF.

Dann heißen die Mengen $\{p_{i1}, \ldots, p_{ik_i}\}, 1 \leq i \leq n$, der jeweils disjunktiv verknüpften Literale die Klauseln von α und die Menge

$$M_\alpha = \{\{p_{11}, \ldots, p_{1k_1}\}, \ldots, \{p_{n1}, \ldots, p_{nk_n}\}\}$$

ihrer Klauseln heißt Klauselmenge von α.

Klauseln, die eine Variable und ihre Negation enthalten, heißen trivial.

Um leere Klauseln von leeren Klauselmengen zu unterscheiden, notieren wir erstere mit dem Symbol $\diamond$ und letztere wie üblich mit dem Symbol $\emptyset$.

Beispiel 2.39

Für die Formel

$$\alpha = (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q) \wedge (\neg p \vee q \vee \neg r)$$

in KNF ergibt sich die Klauselmenge

$$M_\alpha = \{\{\neg p, q, r\}, \{\neg p, \neg q\}, \{\neg p, q, \neg r\}\}.$$

Satz 2.40

(i) *Die leere Klausel $\diamond$ ist unerfüllbar.*

(ii) *Die leere Klauselmenge $\emptyset$ ist allgemeingültig.*

(iii) *Sei M eine Klauselmenge und K eine triviale Klausel mit $K \in M$. Dann gilt $M \equiv M \setminus \{K\}$.*

Beweis.

(i) Eine Klausel ist erfüllbar, wenn es eine Belegung $\mathcal{I}$ gibt, die mindestens ein Literal wahr macht.

Da die leere Klausel aber kein Literal enthält, kann auch keines wahr gemacht werden.

(ii) Eine Klauselmenge ist allgemeingültig, wenn jede Belegung der Variablen jede Klausel wahr macht.

Da die leere Klauselmenge keine Klauseln enthält, müssen auch keine Klauseln wahr gemacht werden.

(iii) Eine triviale Klausel ist eine Tautologie.

Resolution: einführendes Beispiel

Beispiel 2.41

Es sei

$$\alpha = (p \vee q \vee \neg r) \wedge (r \vee \neg s)$$

und damit

$$M_\alpha = \{\{p, q, \neg r\}, \{r, \neg s\}\}.$$

Ist α bzw. M_α erfüllbar?

- M_α ist genau dann erfüllbar, wenn $K_1 = \{p, q, \neg r\}$ und $K_2 = \{r, \neg s\}$ erfüllbar sind.
- r tritt in K_1 negiert und in K_2 nicht negiert auf.
- Gilt $\mathcal{I}(r) = 1$, dann kann K_1 nur durch p oder q erfüllt werden, also $\mathcal{I}(p) = 1$ oder $\mathcal{I}(q) = 1$.
- Gilt $\mathcal{I}(r) = 0$, dann kann K_2 nur durch $\mathcal{I}(s) = 0$ erfüllt werden.
- Also muss auf jeden Fall $p \vee q \vee \neg s$ gelten.

Resolution basiert auf der Tautologie:

$$((\alpha \to \beta) \wedge (\neg\alpha \to \gamma)) \to (\beta \vee \gamma)$$

Anschauliches Beispiel:

- Wenn die Sonne scheint, gehe ich ins Schwimmbad.
- Wenn nicht die Sonne scheint, gehe ich ins Kino.
- Also gehe ich ins Schwimmbad oder ins Kino.

Definition der Resolution

Definition 2.42

Die Resolution erfolgt mithilfe der Inferenzregel

$$\frac{p_1 \vee \ldots \vee p_m \vee r, q_1 \vee \ldots \vee q_n \vee \neg r}{p_1 \vee \ldots \vee p_m \vee q_1 \vee \ldots \vee q_n}$$

oder in „Klauselnotation“

$$\frac{\overbrace{\{p_1, \ldots, p_m, r\}}^{=K_1}, \overbrace{\{q_1, \ldots, q_n, \neg r\}}^{=K_2}}{\underbrace{\{p_1, \ldots, p_m, q_1, \ldots, q_n\}}_{=K}}.$$

K heißt Resolvente von K_1 und K_2. Schreibweise: $K = \text{Res}(K_1, K_2)$.
r und $\neg r$ heißen passende Literale.

Beispiel 2.43

(i) Es seien $K_1 = \{p, q, \neg r\}$ und $K_2 = \{r, \neg s\}$ die beiden Klauseln aus Beispiel 2.41. Dann ist

$$\text{Res}(K_1, K_2) = \{p, q, \neg s\}$$

die einzige Resolvente von K_1 und K_2.

(ii) Für $K_1 = \{p, \neg q, r\}$ und $K_2 = \{q, \neg r\}$ sind

$$\text{Res}(K_1, K_2) = \{p, r, \neg r\} \text{ und } \text{Res}(K_2, K_1) = \{p, q, \neg q\}$$

mögliche Resolventen.

(iii) Die Resolvente der Klauseln $K_1 = \{p\}$ und $K_2 = \{\neg p\}$ ist die leer:

$$\text{Res}(K_1, K_2) = \diamond.$$

Resolutionslemma

Satz 2.44

Seien $\alpha \in \mathcal{A}$ in KNF, $K_1, K_2 \in M_\alpha$ Klauseln von α und $K = \text{Res}(K_1, K_2)$ eine Resolvente von K_1 und K_2.

Dann gilt:

$$M_\alpha \equiv M_\alpha \cup \{K\}$$

Anschauliche Interpretation:

- Die Hinzunahme von Resolventen einer Klauselmenge ändert nicht die Semantik der Klauselmenge.

Beweis.

Es sei β die aussagenlogische Formel, die der Klauselmenge $M_\alpha \cup \{K\}$ entspricht. Wir müssen dann zeigen, dass

$$\mathcal{I}^*(\alpha) = \mathcal{I}^*(\beta)$$

für alle Belegungen $\mathcal{I}$ gilt.

- Sei $\mathcal{I}$ eine Belegung mit $\mathcal{I}^*(\alpha) = 0$.

  Dann wird eine Klausel von M_α nicht erfüllt.

  Diese Klausel ist aber auch in $M_\alpha \cup \{K\}$ und damit in β enthalten.

  Also gilt auch $\mathcal{I}^*(\beta) = 0$.
- Sei $\mathcal{I}$ eine Belegung mit $\mathcal{I}^*(\alpha) = 1$.

  D. h. $\mathcal{I}$ erfüllt alle Klauseln von M_α, insbesondere K_1 und K_2.

  Wegen $\{K_1, K_2\} \models K$ erfüllt $\mathcal{I}$ dann auch die Klausel K.

  Also erfüllt $\mathcal{I}$ alle Klauseln von $M_\alpha \cup \{K\}$.

  Damit gilt $\mathcal{I}^*(\beta) = 1$.

Fortgesetzte Anwendung des Resolutionsoperators

Definition 2.45

Sei M_α die Klauselmenge von $\alpha \in \mathcal{A}$ in KNF. Dann sei

$$\text{Res}(M_\alpha) = M_\alpha \cup \{\text{Res}(K_1, K_2) | K_1, K_2 \in M_\alpha\}.$$

Wir wenden nun den Operator Res wiederholt auf M_α an und definieren damit:

$$\begin{aligned} \text{Res}^0(M_\alpha) &= M_\alpha \\ \text{Res}^{n+1}(M_\alpha) &= \text{Res}(\text{Res}^n(M_\alpha)), n \geq 0 \end{aligned}$$

Folgerung 2.46

(i) $M_\alpha \equiv \text{Res}^i(M_\alpha)$ *für alle* $i \geq 0$.

(ii) $\text{Res}^i(M_\alpha) \equiv \text{Res}^j(M_\alpha)$ *für alle* $i, j \geq 0$.

Beispiel 2.47

Wir betrachten die Formel

$$\alpha = (\neg r \vee p \vee q) \wedge (p \vee q \vee r) \wedge (\neg q \vee p)$$

Es ist also $M_\alpha = \{\{p, q, \neg r\}, \{p, q, r\}, \{p, \neg q\}\}$ und es gilt

$$\begin{aligned}
\mathrm{Res}(M_\alpha) &= \{\{\{p, q, \neg r\}, \{p, q, r\}, \{p, \neg q\}, \{p, q\}, \{p, \neg r\}, \{p, r\}\} \\
\mathrm{Res}^2(M_\alpha) &= \mathrm{Res}(\mathrm{Res}(M_\alpha)) \\
&= \{\{\{p, q, \neg r\}, \{p, q, r\}, \{p, \neg q\}, \{p, q\}, \{p, \neg r\}, \{p, r\}, \{p\}\} \\
\mathrm{Res}^3(M_\alpha) &= \mathrm{Res}(\mathrm{Res}(\mathrm{Res}(M_\alpha))) \\
&= \{\{\{p, q, \neg r\}, \{p, q, r\}, \{p, \neg q\}, \{p, q\}, \{p, \neg r\}, \{p, r\}, \{p\}\}
\end{aligned}$$

Also $\mathrm{Res}^3(M_\alpha) = \mathrm{Res}^2(M_\alpha)$ und damit $\mathrm{Res}^l(M_\alpha) = \mathrm{Res}^2(M_\alpha)$ für alle $l \geq 2$.

Satz 2.48

Sei M_α die Klauselmenge von $\alpha \in \mathcal{A}$ in KNF.

Dann gibt es ein $t \in \mathbb{N}_0$, so dass $\text{Res}^t(M_\alpha) = \text{Res}^l(M_\alpha)$ ist für alle $l \geq t$.

Definition 2.49

Die Klauselmenge $\text{Res}^t(M_\alpha)$ aus Satz 2.48 bezeichnen wir mit $\text{Res}^*(M_\alpha)$.

Beispiel 2.50

In Beispiel 2.47 gilt $\text{Res}^*(M_\alpha) = \text{Res}^2(M_\alpha)$.

Folgerung 2.51

Sei M_α die Klauselmenge von $\alpha \in \mathcal{A}$ in KNF, dann ist

(i) $M_\alpha \equiv \text{Res}^*(M_\alpha)$

(ii) *M_α (un-)erfüllbar genau dann, wenn $\text{Res}^*(M_\alpha)$ (un-)erfüllbar ist.*

Beispiel 2.52

Für die Formel

$$\alpha = (p \vee q \vee \neg r) \wedge \neg p \wedge (p \vee q \vee r) \wedge (p \vee \neg q)$$

mit der Klauselmenge

$$M_\alpha = \{\{p, q, \neg r\}, \{\neg p\}, \{p, q, r\}, \{p, \neg q\}\}$$

gilt:

$$\begin{aligned}
\mathrm{Res}(M_\alpha) &= \{\{p, q, \neg r\}, \{\neg p\}, \{p, q, r\}, \{p, \neg q\}, \\
&\qquad \{q, \neg r\}, \{p, q\}, \{p, \neg r\}, \{q, r\}, \{\neg q\}, \{p, r\}\} \\
\mathrm{Res}^2(M_\alpha) &= \{\{p, q, \neg r\}, \{\neg p\}, \{p, q, r\}, \{p, \neg q\}, \\
&\qquad \{q, \neg r\}, \{p, q\}, \{p, \neg r\}, \{q, r\}, \{\neg q\}, \{p, r\} \\
&\qquad \{q\}, \{\neg r\}, \{r\}, \{p\}\}
\end{aligned}$$

Es folgt $\diamond \in \mathrm{Res}^3(M_\alpha)$. Damit ist M_α unerfüllbar.

Resolutionssatz der Aussagenlogik

Satz 2.53

Sei M_α die Klauselmenge von $\alpha \in \mathcal{A}$ in KNF.

Dann gilt: M_α (und damit α) ist unerfüllbar genau dann, wenn $\diamond \in \text{Res}^*(M_\alpha)$ ist.

Anschauliche Interpretation:

- Die Konstruktion von $\text{Res}^*(M_\alpha)$ entspricht einem vollständigen und korrekten Kalkül.

Resolutionsverfahren

Der Resolutionssatz ist die Grundlage für das Resolutionsverfahren:
Gegeben sei eine Formel $\alpha \in \mathcal{A}$ in KNF.

1. Bilde die Klauselmenge M_α.
2. Wende den Resolutionsoperator Res fortgesetzt auf M_α an, bis ein t erreicht ist mit $\text{Res}^l(M_\alpha) = \text{Res}^t(M_\alpha)$ für alle $l \geq t$. Solch ein t existiert gemäß Satz 2.48.

   Anders ausgedrückt: bilde $\text{Res}^*(M_\alpha)$.
3. Falls $\diamond \in \text{Res}^*(M_\alpha)$ ist, dann ist α unerfüllbar, sonst erfüllbar.

Deduktion der leeren Klausel

Definition 2.54

Eine Deduktion der leeren Klausel aus einer Klauselmenge $M_\alpha, \alpha \in \mathcal{A}$ in KNF, ist eine Folge $K_1, K_2, \ldots, K_t$ von Klauseln, so dass gilt:

(i) K_t ist die leere Klausel und

(ii) $K_i, 1 \leq i \leq t$, ist entweder eine Klausel aus M_α oder eine Resolvente von Klauseln $K_r, K_s (K_i = \text{Res}(K_r, K_s))$ mit $r, s \leq i$.

Aus dem Resolutionssatz folgt unmittelbar:

Folgerung 2.55

Eine Formel $\alpha \in \mathcal{A}$ in KNF ist unerfüllbar genau dann, wenn eine Deduktion der leeren Klausel aus M_α möglich ist.

Beispiel 2.56

Wir betrachten wieder die Formel

$$\alpha = (p \vee q \vee \neg r) \wedge \neg p \wedge (p \vee q \vee r) \wedge (p \vee \neg q)$$

Es ist also $M_\alpha = \{\{p, q, \neg r\}, \{\neg p\}, \{p, q, r\}, \{p, \neg q\}\}$.

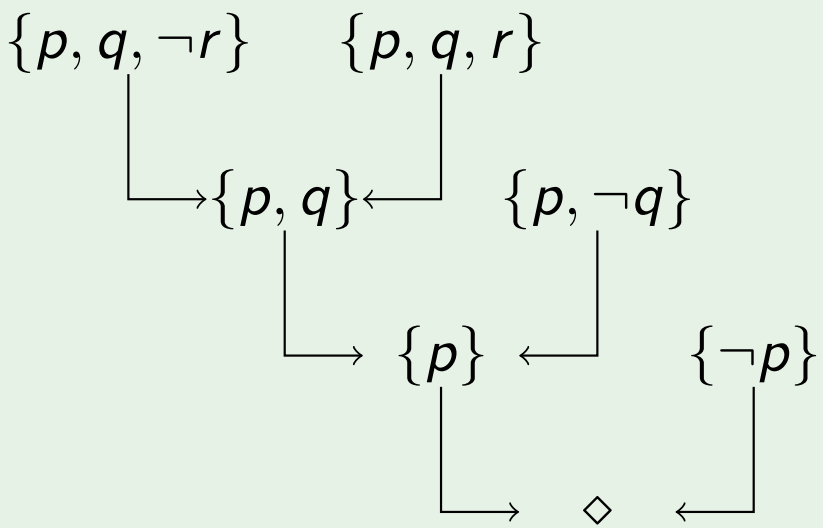
$$\begin{aligned} K_1 &= \{p, q, \neg r\} \\ K_2 &= \{p, q, r\} \\ K_3 &= \text{Res}(K_1, K_2) = \{p, q\} \\ K_4 &= \{p, \neg q\} \\ K_5 &= \text{Res}(K_3, K_4) = \{p\} \\ K_6 &= \{\neg p\} \\ K_7 &= \text{Res}(K_5, K_6) = \diamond \end{aligned}$$

Resolutionsgraph

Eine Deduktion können wir mithilfe eines Resolutionsgraphen darstellen.

Beispiel 2.57

Resolutionsgraph für die Deduktion von Beispiel 2.56:

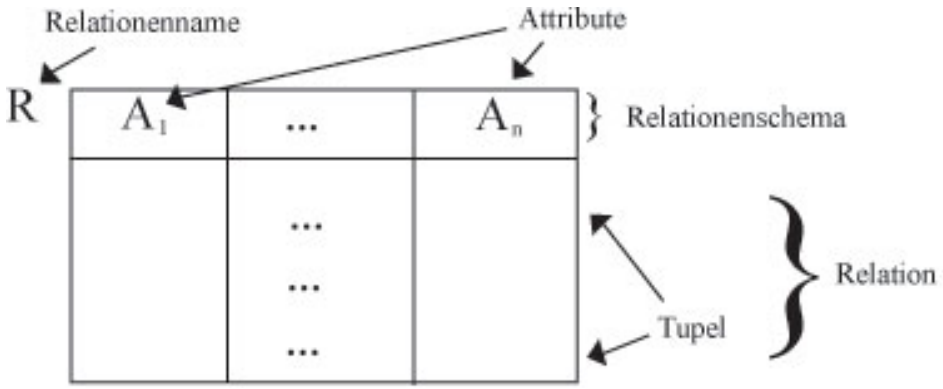


Zusammenfassung

- Aussagenlogik als formale Sprache: Syntax und Semantik durch Belegung $\mathcal{I}$ und Interpretationsfunktion $\mathcal{I}^*$.
- Logische Folgerung $\mathcal{F} \models \alpha$: Jedes Modell für $\mathcal{F}$ ist auch ein Modell für α.
- Syntaktische Folgerung $\mathcal{F} \vdash \alpha$: α ist mittels Inferenzregeln aus $\mathcal{F}$ herleitbar.
- Konjunktive Normalform sowie Klauselmengen als kanonische Darstellung von Formeln.
- Resolutionskalkül: Syntaktische Ableitung auf der Basis von Klauseln.
- Das Resolutionskalkül ist korrekt und vollständig.

Kapitel 3

Relationen und Prädikatenlogik



Inhalt

Kartesisches Produkt

Definition 3.1

Für Mengen $A_1, \ldots, A_n, n \geq 1$ heißt die Menge

$$A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) | x_i \in A_i, 1 \leq i \leq n\}$$

n-stelliges kartesisches Produkt von $A_1, \ldots, A_n$.

Anstelle von $A_1 \times \cdots \times A_n$ schreiben wir auch $\bigtimes_{i=1}^{n} A_i$.

$(x_1, \ldots, x_n)$ heißt *n*-Tupel. Ein 2-Tupel heißt auch Paar, ein 3-Tupel Tripel und ein 4-Tupel Quadrupel.

$x_i, 1 \leq i \leq n$ heißt die *i*-te Komponente von $(x_1, \ldots, x_n)$.

Bemerkung:

- Falls $A_i = \emptyset$ für mindestens ein $i, 1 \leq i \leq n$, dann gilt $\bigtimes_{i=1}^{n} A_i = \emptyset$.

Beispiel 3.2

Für die Mengen $A = \{1, 2\}, B = \{a, b, c\}$ und $C = \{2, 3\}$ ist

$$\begin{aligned} A \times B &= \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\} \\ A \times B \times C &= \{(1, a, 2), (1, a, 3), (1, b, 2), (1, b, 3), (1, c, 2), (1, c, 3), \\ &\quad (2, a, 2), (2, a, 3), (2, b, 2), (2, b, 3), (2, c, 2), (2, c, 3)\} \end{aligned}$$

Folgerung 3.3

Ist $|A_i| < \infty$ *für* $1 \leq i \leq n$, *dann gilt*

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|.$$

n-faches kartesisches Produkt

Definition 3.4

Sind alle A_i identisch, also $A_i = A$ für $1 \leq i \leq n$, dann heißt

$$A_1 \times \cdots \times A_n = A \times \cdots \times A$$

n-faches kartesisches Produkt von A.

Abkürzend benutzen wir für das n-fache kartesische Produkt auch die Potenzschreibweise:

$$A^n = A \times \cdots \times A$$

Folgerung 3.5

Für A mit $|A| < \infty$ gilt $|A^n| = |A|^n$.

Teilmenge

Definition 3.6

Eine Menge A ist Teilmenge einer Menge B, falls jedes Element von A auch Element von B ist, d. h. wenn

$$x \in A \Rightarrow x \in B$$

gilt. Wir schreiben hierfür $A \subseteq B$. B heißt dann auch Obermenge von A.

Zwei Mengen A, B sind gleich, wenn jede Teilmenge der anderen ist, also wenn

$$A \subseteq B \wedge B \subseteq A$$

gilt. Wir schreiben dann $A = B$. Sind zwei Mengen nicht gleich, schreiben wir $A \neq B$.

Eine Menge A ist eine echte Teilmenge von B (Schreibweise $A \subset B$), wenn gilt:

$$A \subseteq B \wedge A \neq B.$$

Beispiel 3.7

Es gilt:

(i) $\{2,3,4,7\} \subseteq \{1,2,3,4,7,13\}$

(ii) $\{1,2,3\} = \{3,2,1\}$ und $\{1,2,3\} \subseteq \{3,2,1\}$.

(iii) $\{2,3,4,7\} \subset \{1,2,3,4,7,13\}$

Beziehungen zwischen Mengen

Satz 3.8

(i) *Für jede Menge A gilt $\emptyset \subseteq A$.*

(ii) *Für jede Menge A gilt $A \subseteq A$.*

(iii) *Seien A, B, C Mengen. Dann gilt:*

$$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$$

Beweis.

(i) Nach Definition müssen wir

$$x \in \emptyset \Rightarrow x \in A$$

zeigen. Diese Implikation gilt genau dann, wenn die Subjunktion

$$x \in \emptyset \rightarrow x \in A$$

eine Tautologie ist, also immer wahr. Da $x \in \emptyset$ immer falsch ist, ist diese Subjunktion immer erfüllt.

(ii) $x \in A \rightarrow x \in A$ ist eine Tautologie, also gilt $x \in A \Rightarrow x \in A$ und damit gemäß der Teilmengendefintion $A \subseteq A$.

(iii) Mit dem Kettenschluss ergibt sich

$$(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in C) \Rightarrow (x \in A \Rightarrow x \in C)$$

Relation

Definition 3.9

Jede Teilmenge $R \subseteq A_1 \times \ldots \times A_n$ heißt *n*-stellige Relation über $A_1, \ldots, A_n$.

Sind alle Mengen A_i identisch, dann heißt R homogen, sonst heterogen.

Bei einer n-stelligen homogenen Relation $R \subseteq A \times \ldots \times A$ heißt A auch die Grundmenge von R.

Beispiel 3.10

Es sei $A = \{-3, -2, -1, 0, 1, 2, 3\}$.

(i) Für $R_1 = \{(x, y) \in A \times A | x \cdot y > 2\} \subseteq A \times A$ gilt

$$\begin{aligned} R_1 = \{&(-3,-3),(-3,-2),(-3,-1),(-2,-3),(-2,-2),\\ &(-1,-3),(1,3),(2,2),(2,3),(3,1),(3,2),(3,3)\}. \end{aligned}$$

Fortsetzung Beispiel.

(ii) Für $R_2 = \{(x, y, z) \in A^3 | x + y = z\}$ gilt

$$\begin{aligned} R_2 = \{&(-3,0,-3),(-3,1,-2),(-3,2,-1),(-3,3,0),\\ &(-2,-1,-3),(-2,0,-2),(-2,1,-1),(-2,2,0),(-2,3,1),\\ &(-1,-2,-3),(-1,-1,-2),(-1,0,-1),(-1,1,0),\\ &(-1,2,1),(-1,3,2),\\ &(0,-3,-3),(0,-2,-2),(0,-1,-1),(0,0,0),(0,1,1),\\ &(0,2,2),(0,3,3),\\ &(1,-3,-2),(1,-2,-1),(1,-1,0),(1,0,1),(1,1,2),(1,2,3),\\ &(2,-3,-1),(2,-2,0),(2,-1,1),(2,0,2),(2,1,3),\\ &(3,-3,0),(3,-2,1),(3,-1,2),(3,0,3)\} \end{aligned}$$

R_1 und R_2 sind homogene Relationen.

Darstellung Relationen durch Matrizen

Endliche zweistellige Relationen $R \subseteq A \times B$ lassen sich auch als Boolsche Matrizen darstellen:

- Die Zeilen werden mit den Elementen aus $A = \{a_1, \ldots, a_m\}$ gekennzeichent,
- die Spalten mit den Elementen aus $B = \{b_1, \ldots, b_n\}$.
- Gilt $(a_i, b_j) \in R$, dann steht in Spalte i und Zeile j eine 1, ansonsten eine 0.

Beispiel 3.11

Die Relation R_1 von Beispiel 3.10 als Boolsche Matrix:

	-3	-2	-1	0	1	2	3
-3	1	1	1	0	0	0	0
-2	1	1	0	0	0	0	0
-1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1
2	0	0	0	0	0	1	1
3	0	0	0	0	1	1	1

Rechtseindeutige und totale Relationen

Definition 3.12

Eine zweistellige Relation $R \subseteq A \times B$ heißt rechtseindeutig, wenn gilt

$$(x_1, y_1) \in R \wedge (x_2, y_2) \in R \wedge (y_1 \neq y_2 \Rightarrow x_1 \neq x_2).$$

Anschaulich: Für jedes $x \in A$ gibt es höchstens ein $y \in B$, so dass $(x, y) \in R$ gilt.

R heißt total, wenn gilt: Für alle $x \in A$ existiert ein $y \in B$ mit $(x, y) \in R$.
Anschaulich: Für jedes $x \in A$ gibt es mindestens ein $y \in B$, so dass $(x, y) \in R$ gilt.

Alternative Bedingung für die Rechtseindeutigkeit:

$$(x_1, y_1) \in R \wedge (x_2, y_2) \in R \wedge (x_1 = x_2 \Rightarrow y_1 = y_2)$$

Beispiel 3.13

- Die Relation
$$R_1 = \{(x, y) \in \mathbb{N} \times \mathbb{N} | y = x^2\}$$
ist rechtseindeutig und total, denn für jedes $x \in \mathbb{N}$ ist x^2 eindeutig definiert: Für jedes $x \in \mathbb{N}$ gibt es genau ein $y \in \mathbb{N}$ mit $y = x^2$.
- Die Relation
$$R_2 = \{(x, y) \in \mathbb{N} \times \mathbb{N} | y \leq x\}$$
ist nicht rechtseindeutig. Beispielsweise gilt sowohl $(3, 1) \in R_2$ als auch $(3, 2) \in R_2$.
- Die Relation
$$R_3 = \{(x, y) \in \mathbb{Z} \times \mathbb{Q} | y = \frac{1}{x}\}$$
ist zwar rechtseindeutig, aber nicht total, denn für $x = 0$ gibt es kein entsprechendes y.

Funktion

Definition 3.14

Eine zweistellige, totale, rechtseindeutige Relation $f \subseteq A \times B$ heißt Funktion oder Abbildung.

Die Menge A ist der Definitionsbereich der Funktion f, die Menge B der Wertebereich.

Bei Funktionen schreibt man anstelle von $f \subseteq A \times B$ auch

$$f : A \to B$$

bzw. mit Funktionsvorschrift

$$f : A \to B, x \mapsto f(x)$$

und anstelle von $(x, y) \in f$ schreibt man

$$y = f(x).$$

Beispiel 3.15

Sei $f : \mathbb{N} \to \mathbb{N}, x \mapsto x + 1$. Dann ist f als Relation

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

also

$$f(1) = 2, f(2) = 3, f(3) = 4, \ldots$$

Definitions- und Wertebereich von f sind jeweils die natürlichen Zahlen.

Alphabet der Prädikatenlogik

Das Alphabet der Prädikatenlogik besteht aus

- Individuenvariablen
  Dafür verwenden wir kleine Buchstaben vom Ende des deutschen Alphabets, auch indiziert, z. B. $x, y, z, x_1, y_2, \ldots$.
- Individuenkonstanten
  Dafür verwenden wir kleine Buchstaben vom Anfang des deutschen Alphabets oder auch Namen oder Objektbezeichner, z. B.:
  $a, b, c, \texttt{martin}, \texttt{klaus}, \texttt{object4711}, \ldots$
- k-stelligen Funktionssymbolen
  mit $k \in \mathbb{N}$. Hierzu nutzen wir kleine Buchstaben aus der Mitte des deutschen Alphabets, auch indiziert, z. B. $f, g, h, f_1, f_2, \ldots$

- k-stelligen Prädikatensymbolen
  mit $k \in \mathbb{N}_0$. Hierzu nutzen wir große Buchstaben oder großgeschriebene Wörter, z. B. $P, Q, R, \texttt{Informatiker}, \texttt{Mann}, \ldots$
- logischen Junktoren
  $\neg, \wedge, \vee$
- Quantoren
  $\forall$ ist der Allquantor, $\exists$ der Existenzquantor.
- Klammersymbolen
  (und)
- Bezeichner für Wahrheitswerte
  0 und 1

Prädikatenlogische Terme

Definition 3.16

Die Menge der prädikatenlogischen Terme ist gegeben durch:

(i) Jede Individuenvariable und jede Individuenkonstante ist ein prädikatenlogischer Term.

(ii) Sind $t_1, \ldots, t_n$ prädikatenlogische Terme und ist f ein n-stelliges Funktionssymbol, dann ist auch $f(t_1, \ldots, t_n)$ ein prädikatenlogischer Term.

(iii) Genau die mit den Regeln (i) und (ii) bildbaren Zeichenketten sind prädikatenlogische Terme.

Beispiel 3.17

Die Individuenvariable x und die Individuenkonstante b sind Terme ebenso wie $f(x, b)$, $f(x, f(b, x))$ und $g(x, f(b, b), h(x, y, a, z))$.

Atomare Formeln

Definition 3.18

Die Menge der atomaren Formeln ist gegeben durch:

(i) Sind $t_1, \ldots, t_n$ prädikatenlogische Terme und ist P ein n-stelliges Prädikatensymbol, dann ist $P(t_1, \ldots, t_n)$ eine atomare Formel.

(ii) Genau die Zeichenketten, die mit Regel (i) gebildet werden können, sind atomare Formeln.

Beispiel 3.19

Die Zeichenketten $P(a, b)$, $Q(a, g(x, y, z, x), f(z))$, $R(x, y, h(h(x, a), z))$ und $S(h(x, y), h(y, x))$ sind atomare Formeln.

Prädikatenlogische Formeln

Definition 3.20

Die Menge der prädikatenlogischen Formeln ist gegeben durch:

(i) Jede atomare Formel ist eine prädikatenlogische Formel.

(ii) Sind α und β prädikatenlogische Formeln, dann auch $\neg\alpha$, $(\alpha \wedge \beta)$ und $(\alpha \vee \beta)$.

(iii) Ist α eine prädikatenlogische Formel und x eine Individuenvariable, dann sind auch $(\forall x\, \alpha)$ und $(\exists x\, \alpha)$ prädikatenlogische Formeln.

(iv) Genau die Zeichenketten, die mit den Regeln (i) bis (iii) gebildet werden können, sind prädikatenlogische Formeln.

Beispiel 3.21

Die Zeichenketten

$$(\forall x\, \neg P(x))$$
$$(\forall x(Q(a, f(a, b)) \wedge R(x, a, c)))$$
$$(\forall x(\exists y\, R(x, y, z)))$$
$$(\forall x(\forall y\, Q(f(x, y), f(y, x))))$$

sind prädikatenlogische Formeln.

Geschlossene Formeln

- Variablen, die sich im Wirkungsbereich eines Quantors befinden, heißen gebunden, nicht gebundene Variablen heißen frei.
- So sind in der Formel

$$(\forall x(\exists y\, P(x, y, z)))$$

die Variablen x, y gebunden, z ist frei.

- Eine Formel, die keine freien Variablen enthält, ist geschlossen. Die Formel

$$(\forall x(\forall y\, Q(f(x, y), f(y, x))))$$

ist ein Beispiel für eine geschlossene Formel.

Vereinbarung: Eine Formel, die nicht Teil einer größeren Formel ist, muss immer geschlossen sein.

Weitere Vereinbarungen

- Gebundene Variablen können beliebig umbenannt werden, wenn dabei keine Kollision mit anderen Variablen auftritt.
- So kann in der Formel

$$(\exists x\, P(f(x,y),z))$$

  die Variable x in q umbenannt werden: $(\exists q\, P(f(q,y),z))$.
- Wir führen wie in der Aussagenlogik $\rightarrow$ und $\leftrightarrow$ ein.
- Wir können Klammern auch weglassen, sofern Bindungen von Quantoren und Junktoren eindeutig sind.
- Die Priorität der Junktoren untereinander sei wie in der Aussagenlogik. Quantoren haben die niedrigste Priorität.

Prädikatenlogische Belegung

Um die Bedeutung einer prädikatenlogischen Formel zu bestimmen, müssen wir wie in der Aussagenlogik eine Belegung vornehmen.

In der Prädikatenlogik besteht solch eine Belegung $\mathcal{I}$ aus:

- Einer Grundmenge U auch Universum genannt. Dies ist die Menge der Dinge, über die wir Aussagen treffen wollen.
- Jeder Individuenkonstante wird ein Element aus dem Universum U zugeordnet.
- Jedem k-stelligen Funktionssymbol wird eine k-stellige Funktion über dem Universum U zugeordnet.
- Jedem k-stelligen Prädikatensymbol wird eine k-stellige Relation über dem Universum U zugeordnet.

Beispiel 3.22

Universum:

$$U = \{ \text{  }, \text{  }, \text{  }, \text{  } \}$$

Unsere Individuenkonstanten seien: `helga`, `martin`, `klaus` und `jupp`.
Zuordnung für die Individuenkonstanten:

$\mathcal{I}(\texttt{helga}) =$ 

$\mathcal{I}(\texttt{martin}) =$ 

$\mathcal{I}(\texttt{klaus}) =$ 

$\mathcal{I}(\texttt{jupp}) =$ 

Wir nutzen im Folgenden keine Funktionssymbole.

Fortsetzung Beispiel.

Unsere Prädikatensymbole seien `Informatiker` und `Programmieren`, jeweils einstellig.

Einstellige Relationen sind einfache Mengen. Wir müssen daher die beiden Prädikatensymbole `Informatiker` und `Programmieren` mit Mengen belegen.

Es sei

$$\mathcal{I}(\texttt{Informatiker}) = \{ \text{  }, \text{  } \}$$

$$\mathcal{I}(\texttt{Programmieren}) = \{ \text{  }, \text{  }, \text{  } \}$$

Fortsetzung Beispiel.

Die folgenden Zeichenketten sind dann prädikatenlogische Formeln:

$$(\texttt{Informatiker}(\texttt{martin}) \wedge \texttt{Informatiker}(\texttt{klaus}))$$
$$(\forall x\,(\texttt{Informatiker}(x) \rightarrow \texttt{Programmieren}(x)))$$

Sie entsprechen den Aussagen:

- Martin und Klaus sind Informatiker.
- Jeder Informatiker kann programmieren.

Sind diese Formeln bzw. Aussagen nun wahr oder falsch?

Semantik Prädikatenlogischer Formeln

Auf Basis einer Belegung $\mathcal{I}$ mit Grundmenge U geschieht die Berechnung $\mathcal{I}^*$ des Wahrheitswertes einer prädikatenlogischen Formel wie folgt:

(i) Für einen prädikatenlogischen Term $f(t_1, \ldots, t_n)$ gilt

$$\mathcal{I}^*(f(t_1, \ldots, t_n)) = \mathcal{I}(f)(\mathcal{I}^*(t_1), \ldots, \mathcal{I}^*(t_n)).$$

Die Belegung $\mathcal{I}(f)$ des Funktionssymbols f wird auf das Ergebnis der Interpretationen der Terme $t_1, \ldots, t_n$ angewendet.

Man beachte: Die Interpretation eines Terms liefert keinen Wahrheitswert, sondern ein Element aus U.

(ii) Für eine atomare Formel $P(t_1, \ldots, t_n)$ gilt

$$\mathcal{I}^*(P(t_1, \ldots, t_n)) = \begin{cases} 1 & \text{falls } (\mathcal{I}^*(t_1), \ldots, \mathcal{I}^*(t_n)) \in \mathcal{I}(P) \\ 0 & \text{sonst} \end{cases}$$

Durch die Interpretation der Terme $t_1, \ldots, t_n$ entsteht ein n-Tupel. Wenn dieses n-Tupel Element der Relation ist, die dem Prädikatensymbol P zugeordnet wurde, dann ist die atomare Formel wahr, ansonsten falsch.

(iii) Interpretation zusammengesetzter Formeln: Seien α, β prädikatenlogische Formeln, dann gilt:

(1) $\mathcal{I}^*(\neg\alpha) = 1 - \mathcal{I}^*(\alpha)$
(2) $\mathcal{I}^*(\alpha \wedge \beta) = \min\{\mathcal{I}^*(\alpha), \mathcal{I}^*(\beta)\}$
(3) $\mathcal{I}^*(\alpha \vee \beta) = \max\{\mathcal{I}^*(\alpha), \mathcal{I}^*(\beta)\}$

(4)

$$\mathcal{I}^*(\exists x\,\alpha) = \begin{cases} 1 & \text{falls ein } a \in U \text{ existiert mit } \mathcal{I}^*(\alpha[x/a]) = 1 \\ 0 & \text{sonst} \end{cases}$$

$$= \max_{a \in U} \mathcal{I}^*(\alpha[x/a])$$

(5)

$$\mathcal{I}^*(\forall x\,\alpha) = \begin{cases} 1 & \text{falls für alle } a \in U \text{ gilt: } \mathcal{I}^*(\alpha[x/a]) = 1 \\ 0 & \text{sonst} \end{cases}$$

$$= \min_{a \in U} \mathcal{I}^*(\alpha[x/a])$$

Dabei bedeutet $\alpha[x/a]$, dass im Wirkungsbereich des Quantors innerhalb der Formel α jedes Vorkommen von x durch (eine Individuenkonstante für) a ersetzt wird.

Beispiel 3.23

Wir überprüfen, ob die Formeln aus Beispiel 3.22 mit der dort definierten Belegung wahr sind.

$$
\begin{aligned}
& \mathcal{I}^*(\texttt{Informatiker(martin)} \wedge \texttt{Informatiker(klaus)}) \\
= \; & \min\{\mathcal{I}^*(\texttt{Informatiker(martin)}), \mathcal{I}^*(\texttt{Informatiker(klaus)})\} \\
= \; & \min\{\mathcal{I}^*(\texttt{martin}) \in \mathcal{I}(\texttt{Informatiker}), \mathcal{I}^*(\texttt{klaus}) \in \mathcal{I}(\texttt{Informatiker}) \\
= \; & \min\{\mathcal{I}(\texttt{martin}) \in \mathcal{I}(\texttt{Informatiker}), \mathcal{I}(\texttt{klaus}) \in \mathcal{I}(\texttt{Informatiker})\} \\
= \; & \min\{\text{  } \in \mathcal{I}(\texttt{Informatiker}), \text{  } \in \mathcal{I}(\texttt{Informatiker})\} \\
= \; & \min\{1, 1\} = 1
\end{aligned}
$$

Fortsetzung Beispiel.

$$
\begin{aligned}
& \mathcal{I}^*(\forall x\,(\texttt{Informatiker}(x) \rightarrow \texttt{Programmieren}(x))) \\
= \;& \min\{\mathcal{I}^*(\texttt{Informatiker}(\texttt{helga}) \rightarrow \texttt{Programmieren}(\texttt{helga})), \\
& \quad \mathcal{I}^*(\texttt{Informatiker}(\texttt{martin}) \rightarrow \texttt{Programmieren}(\texttt{martin})), \\
& \quad \mathcal{I}^*(\texttt{Informatiker}(\texttt{klaus}) \rightarrow \texttt{Programmieren}(\texttt{klaus})), \\
& \quad \mathcal{I}^*(\texttt{Informatiker}(\texttt{jupp}) \rightarrow \texttt{Programmieren}(\texttt{jupp}))\} \\
= \;& \min\{\max\{1 - \mathcal{I}^*(\texttt{Informatiker}(\texttt{helga})), \mathcal{I}^*(\texttt{Programmieren}(\texttt{helga}) \\
& \quad \max\{1 - \mathcal{I}^*(\texttt{Informatiker}(\texttt{martin})), \mathcal{I}^*(\texttt{Programmieren}(\texttt{marti} \\
& \quad \max\{1 - \mathcal{I}^*(\texttt{Informatiker}(\texttt{klaus})), \mathcal{I}^*(\texttt{Programmieren}(\texttt{klaus}) \\
& \quad \max\{1 - \mathcal{I}^*(\texttt{Informatiker}(\texttt{jupp})), \mathcal{I}^*(\texttt{Programmieren}(\texttt{jupp}))\} \\
= \;& \min\{\max\{1-0,0\}, \max\{1-1,1\}, \max\{1-1,1\}, \max\{1-0,1\}\} \\
= \;& \min\{1,1,1,1\} = 1
\end{aligned}
$$

Übertragung von Begriffen aus der Aussagenlogik

Wir können nun die meisten Begriffe aus der Aussagenlogik auf die Prädikatenlogik übertragen.

- Ein (prädikatenlogisches) Modell ist eine Belegung, die eine Formel bzw. eine Formelmenge wahr macht.
- Eine Formel α bzw. eine Formelmenge $\mathcal{F}$ heißt erfüllbar, wenn es ein Modell für α bzw. $\mathcal{F}$ gibt.
- Eine Formel, die für jede Belegung wahr ist, ist eine Tautologie.
- Logische Folgerung: Wenn jedes Modell für eine Formelmenge $\mathcal{F}$ auch eine Modell für α ist, dann gilt

$$\mathcal{F} \models \alpha$$

- Auch die Begriffe der Implikation ($\Rightarrow$) und Äquivalenz ($\Leftrightarrow$) werden wie in der Aussagenlogik definiert.

Logische Äquivalenzen

- Wie in der Aussagenlogik sind zwei Formel α und β logisch äquivalent ($\alpha \equiv \beta$), wenn für alle Belegungen $\mathcal{I}^*(\alpha) = \mathcal{I}^*(\beta)$ gilt.
- Alle logischen Äquivalenzen der Aussagenlogik gelten auch in der Prädikatenlogik (siehe Satz 2.24).

Satz 3.24

$$\begin{aligned} \neg(\forall x\, \alpha) &\equiv \exists x\, \neg\alpha \\ \neg(\exists x\, \alpha) &\equiv \forall x\, \neg\alpha \\ (\forall x\, \alpha) \wedge (\forall x\, \beta) &\equiv \forall x\, (\alpha \wedge \beta) \\ (\exists x\, \alpha) \vee (\exists x\, \beta) &\equiv \exists x\, (\alpha \vee \beta) \end{aligned}$$

Fortsetzung Satz.

$$\begin{aligned} \forall x \forall y\, \alpha &\equiv \forall y \forall x\, \alpha \\ \exists x \exists y\, \alpha &\equiv \exists y \exists x\, \alpha \\ \forall x\, \alpha &\equiv \forall y\, \alpha[x/y] \\ \exists x\, \alpha &\equiv \exists y\, \alpha[x/y] \end{aligned}$$

Für die Ersetzungen muss y eine Variable sein, die im Wirkungsbereich der Quantoren nicht verwendet wird.

Achtung:

$$\begin{aligned} (\forall x\, \alpha) \vee (\forall x\, \beta) &\not\equiv \forall x\, (\alpha \vee \beta) \\ (\exists x\, \alpha) \wedge (\exists x\, \beta) &\not\equiv \exists x\, (\alpha \wedge \beta) \\ \exists x \forall y\, \alpha &\not\equiv \forall y \exists x\, \alpha \end{aligned}$$

Pragmatische Verwendung der Prädikatenlogik als Sprache

- Wir werden ab jetzt mathematische Sachverhalte sehr oft in prädikatenlogischer Form beschreiben.
- Um die Lesbarkeit zu vereinfachen, verwenden wir die Sprache der Prädikatenlogik pragmatisch.
- Eingeführte Notationen werden direkt verwendet (also ohne Prädikate zu definieren). Beispiel:

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

- Zur besseren Lesbarkeit trennt : Quantor und Variable vom Rest der Formel.
- $\Rightarrow$ und $\Leftrightarrow$ statt $\rightarrow$ und $\leftrightarrow$

- Einschränkende Bedingungen zu Mengen oft direkt bei den Quantoren.
  Beispiel: Die Aussage „Alle natürlichen Zahlen sind positiv.“

$$\forall n \in \mathbb{N} : n > 0$$

  statt

$$\forall n : n \in \mathbb{N} \Rightarrow n > 0$$

- Generell beim Allquantor:

$$\forall x \in A : P(x) \quad \text{steht für} \quad \forall x : x \in A \Rightarrow P(x)$$

- Beim Existenzquantor:

$$\exists x \in A : P(x) \quad \text{steht für} \quad \exists x : x \in A \wedge P(x)$$

- Weitere Informationen ergeben sich oft aus dem Kontext.

Definition neuer Begriffe

Es sei α ein neuer Begriff oder neues Symbol das wir definieren wollen und β eine prädikatenlogische Formel.

Für die Definition von α nutzen wir die Schreibweise

$$\alpha :\Leftrightarrow \beta$$

Semantik: α liegt genau dann vor, wenn die Aussage β wahr ist.

Beispiel: Wir könnten so den Begriff Teilmenge bzw. das Symbol $\subseteq$ definieren durch:

$$A \subseteq B \quad :\Leftrightarrow \quad \forall x : x \in A \Rightarrow x \in B$$

Beispiel 3.25

Die wichtigste Definition der Mathematik des 2. Semesters:

$a \in \mathbb{R}$ *ist* *Grenzwert* *einer Folge* $(a_n) :\Leftrightarrow$

$$\forall \epsilon > 0 \, \exists n_0 \in \mathbb{N} \, \forall n \geq n_0 : |a_n - a| < \epsilon$$

- Aus dem Kontext: $\epsilon \in \mathbb{R}$ und $n \in \mathbb{N}$.
- $-$ entspricht einer zweistelligen Funktion.
- $|\ |$ entspricht einer einstelligen Funktion.
- $<$ entspricht einem zweistelligen Prädikat.

Zusammenfassung

- Kartesisches Produkt $A \times B$
- Relation $R \subseteq A \times B$
- Funktion als spezielle Relation (total, rechtseindeutig)
- Prädikatenlogik als Sprache: Einführung von Quantoren und Variablen
- prädikatenlogische Belegung: Universum als Grundmenge, Prädikate als Relationen über dem Universum
- prädikatenlogische Interpretation: $\forall x$ entspricht einer Minimierung über dem Universum, $\exists x$ einer Maximierung.
- pragmatischer Umgang mit der Sprache in der Praxis

Kapitel 4

Beweismethoden

$$\frac{A(1), \forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)}{\forall n \in \mathbb{N} : A(n)}$$

Inhalt

Beweismethoden

- Die meisten mathematischen Sätze oder Folgerungen haben die Form

$$\alpha \Rightarrow \beta$$

  Dabei sind α und β (prädikatenlogische) Formeln.
- α heißt Voraussetzung und β Behauptung eines Satzes.
- Sätze, die $\alpha \Leftrightarrow \beta$ behaupten, sind äquivalent zu $\alpha \Rightarrow \beta \wedge \beta \Rightarrow \alpha$. Daher beschränken wir uns auf Implikationen.
- Wir betrachten folgende Beweisverfahren:
  1. direkter Beweis
  2. indirekter Beweis
  3. Widerspruchsbeweis
  4. Beweis durch Ringschluss
  5. vollständige Induktion

Direkter Beweis

Ein direkter Beweis eines Satzes $\alpha \Rightarrow \beta$ ist eine Folge

$$\gamma_1, \gamma_2, \ldots, \gamma_n = \beta$$

von Aussagen, wobei für jedes i mit $1 \leq i \leq n$ gilt:

- $\gamma_i = \alpha$ oder
- γ_i ist eine bereits bewiesene bekannte Aussage oder
- $\gamma_{j_1} \wedge \gamma_{j_2} \wedge \ldots \wedge \gamma_{j_r} \Rightarrow \gamma_i$ mit $j_1, j_2, \ldots, j_r < i$.

Bei den Zwischenschritten können also Kombinationen von vorher etablierten Aussagen verwendet werden.

Teiler

Definition 4.1

Es seien $p, q \in \mathbb{N}$.

p heißt Teiler von q oder p teilt q (Schreibweise: $p|q$) genau dann, wenn ein $a \in \mathbb{N}$ existiert, so dass $a \cdot p = q$ gilt.

Wir schreiben $p \nmid q$, wenn p kein Teiler von q ist.

Kurz:

$$\begin{aligned} p|q &:\Leftrightarrow \exists a \in \mathbb{N} : a \cdot p = q \\ p \nmid q &:\Leftrightarrow \forall a \in \mathbb{N} : a \cdot p \neq q \end{aligned}$$

Beispiel 4.2

Wir zeigen mit einem direkten Beweis:

$$p|q \wedge q|r \Rightarrow p|r$$

In Worten: Wenn p Teiler von q ist und wenn q Teiler von r ist, dann ist auch p Teiler von r.

γ_1	$=$	$p\|q \wedge q\|r$	Voraussetzung
γ_2	$=$	$p\|q$	folgt aus γ_1
γ_3	$=$	$\exists a \in \mathbb{N} : a \cdot p = q$	folgt aus γ_2 nach Def. für $\|$
γ_4	$=$	$q\|r$	folgt aus γ_1
γ_5	$=$	$\exists b \in \mathbb{N} : b \cdot q = r$	folgt aus γ_4 nach Def. für $\|$
γ_6	$=$	$b \cdot (a \cdot p) = r$	folgt aus γ_3 und γ_5
γ_7	$=$	$(b \cdot a) \cdot p = r$	folgt aus γ_6 mit Assoziativgesetz
γ_8	$=$	$\exists c \in \mathbb{N} : c \cdot p = r$	folgt aus γ_7 mit $c = b \cdot a$
γ_9	$=$	$p\|r$	folgt aus γ_8 nach Def. für $\|$

Indirekter Beweis

Ein indirekter Beweis nutzt die Äquivalenz:

$$(\alpha \Rightarrow \beta) \Leftrightarrow (\neg\beta \Rightarrow \neg\alpha)$$

Manchmal ist es einfacher, die rechte anstelle der linken Folgerung zu beweisen.

Beispiel 4.3

Wir beweisen eine weitere Teilbarkeitsregel:

> *Wenn die letzten beiden Ziffern einer natürlichen Zahl z als Zahl betrachtet durch 4 teilbar sind, dann ist auch z durch 4 teilbar.*

Wir formalisieren:

$$\begin{aligned} \alpha &= x \in \mathbb{N}_{0,99} \wedge 4 | x \wedge y \in \mathbb{N}_0 \\ \beta &= 4 | (100y + x) \end{aligned}$$

Hinweis: $z = 100y + x$

Wir zeigen jetzt $\neg\beta \Rightarrow \neg\alpha$. Es ist:

$$\begin{aligned} \neg\alpha &= x \notin \mathbb{N}_{0,99} \vee 4 \nmid x \vee y \notin \mathbb{N}_0 \\ \neg\beta &= 4 \nmid (100y + x) \end{aligned}$$

Fortsetzung Beispiel.

Wenn $x \notin \mathbb{N}_{0,99}$ oder $y \notin \mathbb{N}_0$ gilt, dann ist $\neg\alpha$ erfüllt. Daher genügt es

$$x \in \mathbb{N}_{0,99} \wedge y \in \mathbb{N}_0 \wedge 4 \nmid (100y + x) \Rightarrow 4 \nmid x$$

zu beweisen. Dies tun wir direkt:

$$\begin{aligned}
4 \nmid (100y + x) &\Rightarrow \tfrac{100y+x}{4} \notin \mathbb{N}_0 \\
&\Rightarrow \tfrac{100y}{4} + \tfrac{x}{4} \notin \mathbb{N}_0 \\
&\Rightarrow 25y + \tfrac{x}{4} \notin \mathbb{N}_0 \\
&\Rightarrow \tfrac{x}{4} \notin \mathbb{N}_0 && \text{weil } y \in \mathbb{N}_0 \\
&\Rightarrow 4 \nmid x && \text{weil } x \in \mathbb{N}_{0,99}
\end{aligned}$$

Widerspruchsbeweis

Ein Widerspruchsbeweis nutzt die Äquivalenz:

$$(\alpha \Rightarrow \beta) \Leftrightarrow ((\alpha \wedge \neg\beta) \Rightarrow 0)$$

Wir nehmen also sowohl α als auch die Negation der Folgerung β, also $\neg\beta$, als wahr an und versuchen, daraus einen Widerspruch zu folgern.

Beispiel 4.4

Ein klassisches Beispiel für einen Widerspruchsbeweis ist zu zeigen, dass $\sqrt{2}$ keine rationale Zahl ist.

Annahme: $\sqrt{2} \in \mathbb{Q}$

Dann existieren teilerfremde Zahlen $p, q \in \mathbb{N}$ mit $\sqrt{2} = \frac{p}{q}$.

$$\begin{aligned} & \sqrt{2} = \frac{p}{q} \\ \Rightarrow \quad & 2 = \frac{p^2}{q^2} \\ \Rightarrow \quad & 2q^2 = p^2 \\ \Rightarrow \quad & 2 | p^2 \end{aligned}$$

p^2 hat aber die gleichen Primfaktoren wie p. Da 2 eine Primzahl ist, muss also auch $2|p$ gelten. Also existiert ein a mit $p = 2 \cdot a$.

Fortsetzung Beispiel.

$$
\begin{aligned}
& p = 2 \cdot a \\
\Rightarrow \quad & 2q^2 = (2a)^2 \\
\Rightarrow \quad & 2q^2 = 4a^2 \\
\Rightarrow \quad & q^2 = 2a^2 \\
\Rightarrow \quad & 2 | q^2 \\
\Rightarrow \quad & 2 | q
\end{aligned}
$$

Widerspruch zu p und q sind teilerfremd.

Ringschluss

Einen Ringschluss können wir nutzen, um die paarweise Äquivalenz von mehr als zwei Aussagen zu zeigen.

Statt

$$\alpha_1 \Leftrightarrow \alpha_2 \Leftrightarrow \cdots \Leftrightarrow \alpha_k$$

zeigen wir

$$\alpha_1 \Rightarrow \alpha_2 \Rightarrow \cdots \Rightarrow \alpha_k \Rightarrow \alpha_1$$

Für jede der Implikationen können wir wiederum eine der schon vorgestellten Techniken nutzen (direkter Beweis, indirekter Beweis, Widerspruchsbeweis).

Vollständige Induktion

- Angenommen, wir wollen zeigen, dass eine Aussage $P(n)$ für alle $n \in \mathbb{N}$ wahr ist.
- Anders ausgedrückt: Es gilt

$$\forall n \in \mathbb{N} : P(n)$$

- Hierzu können wir die Technik der vollständigen Induktion verwenden.
  - Wir zeigen, dass $P(1)$ gilt.
  - Wir zeigen: $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$

Induktionsbeweis

Ein Beweis mit vollständiger Induktion verläuft dementsprechend nach folgendem Schema:

- Induktionsanfang
  Zeige, dass $P(1)$ gilt.
- Induktionsschritt
  Zeige: $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$
- Die Aussage $P(n)$ heißt dabei Induktionsvoraussetzung oder Induktionsannahme.
- Die Aussage $P(n+1)$ ist die Induktionsbehauptung.

Warum funktioniert vollständige Induktion?

Wir haben:

- $P(1)$
- $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$

Angewendet auf den Induktionsanfang $P(1)$ und den Induktionsschritt für $n = 1$ erhalten wir mithilfe des Modus Ponens:

$$(P(1) \wedge (P(1) \Rightarrow P(2))) \Rightarrow P(2)$$

Jetzt verwenden wir $P(2)$ und den Induktionsschritt für $n = 2$:

$$(P(2) \wedge (P(2) \Rightarrow P(3))) \Rightarrow P(3)$$

Dies können wir immer weiter fortsetzen.

Summationssymbol

- Zur Notation der Summe von mehreren Summanden $x_1, x_2, \ldots, x_n$ verwenden wir das Summationssymbol $\sum$:

$$x_1 + x_2 + \cdots + x_n = \sum_{i=1}^{n} x_i$$

- Der Summationsindex kann dabei auch zwischen $u, o \in \mathbb{N}_0$ laufen:

$$x_u + x_{u+1} + \ldots + x_o = \sum_{i=u}^{o} x_i$$

- u heißt untere und o obere Index- oder Summationsgrenze.
- Für den Fall $u > o$ legen wir fest:

$$\sum_{i=u}^{o} x_i = 0$$

Beispiel 4.5

Wir wollen zeigen, dass für alle $n \in \mathbb{N}$ gilt:

$$1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Für ein $n \in \mathbb{N}$ ist diese Gleichung entweder wahr oder falsch. Also stellt diese Gleichung ein Prädikat $P(n)$ dar.

Wir wollen zeigen, dass die Gleichung (und damit das Prädikat $P(n)$) für alle $n \in \mathbb{N}$ wahr ist.

- Induktionsanfang: $n = 1$

$$\sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2} = \frac{n(n+1)}{2}$$

Also gilt die Gleichung für $n = 1$, d. h. $P(1)$ ist wahr.

Fortsetzung Beispiel.

(ii) Induktionsschritt: $n \to n+1$

Gemäß Induktionsvoraussetzung (I.V.) dürfen wir $P(n)$ als wahr annehmen, d. h. die Gleichung gilt für n.

Wir müssen nun zeigen, dass sie dann auch für $n+1$ gilt, also dass auch $P(n+1)$ wahr ist.

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= (n+1) + \sum_{i=1}^{n} i \\
&\overset{\text{I.V.}}{=} (n+1) + \frac{n(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}$$

Damit haben wir nun bewiesen, dass $P(n)$ für alle $n \in \mathbb{N}$ gilt.

Verschiebung des Induktionsanfangs

- Was tun, wenn ein Prädikat nicht ab $n = 1$ sondern erst ab $n = k$ wahr ist?
- Wir definieren ein neues Prädikat Q mit

$$Q(n) :\Leftrightarrow P(n + k - 1)$$

- Somit gilt:

$$\forall n \in \mathbb{N}_k : P(n) \quad \Leftrightarrow \quad \forall n \in \mathbb{N} : Q(n)$$

- Praktisch genügt es, einfach den Induktionsanfang auf k zu legen.
- Dies geht natürlich auch in die andere Richtung. Um

$$\forall n \in \mathbb{N}_0 : R(n)$$

zu zeigen, legen wir den Induktionsanfang auf $n = 0$.

Beispiel 4.6

(i) Für alle $n \in \mathbb{N}_0$ gilt:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

(ii) Für alle $n \in \mathbb{N}$ gilt:

$$\sum_{i=1}^{n} (2i-1) = n^2$$

(iii) Für alle $n \in \mathbb{N}_0$ und alle $x \in \mathbb{R} \setminus \{1\}$ gilt:

$$\sum_{i=0}^{n} x^i = \frac{x^{n+1}-1}{x-1}$$

Fortsetzung Beispiel.

(iv) Für alle $n \in \mathbb{N}$ gilt:

$$7^n - 1 \text{ ist ein Vielfaches von } 6$$

(v) Für alle natürlichen Zahlen $n \geq 4$ gilt:

$$n! > 2^n$$

Beweise an der Tafel. ✎

Fibonacci-Zahlen

Definition 4.7

Die Fibonacci-Zahlen F_n sind für $n \in \mathbb{N}_0$ wie folgt definiert:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \text{ für } n \geq 2 \end{aligned}$$

Leonardo da Pisa

Auch Fibonacci genannt (1170–1240), war Rechenmeister in Pisa und gilt als einer der bedeutendsten Mathematiker des Mittelalters.

Die Fibonacci-Zahlen gehen auf eine Übungsaufgabe von Fibonacci zur Vermehrung von Kaninchen zurück.

Formel von Moivre-Binet

Satz 4.8

Für alle $n \in \mathbb{N}_0$ gilt:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

Beweis.

Mittels vollständiger Induktion, Übungsaufgabe.

- Der Beweis für die Korrektheit einer expliziten Formel ist i.d.R. viel einfacher als die Herleitung solch einer expliziten Formel.
- Im nächsten Semester lernen Sie einen ersten Ansatz zur Herleitung solch expliziter Formeln kennen.

Strukturelle Induktion

- Wir können vollständige Induktion auch anwenden, um zu zeigen, dass eine Eigenschaft $P(x)$ für alle Elemente einer rekursiv definierten Menge M gilt.
- Der Induktionsanfang entspricht dabei dem Nachweis, dass $P(x)$ für alle explizit angegebenen Elemente von M gilt und
- der Induktionsschritt entspricht dem Nachweis, dass $P(y)$ gilt, wenn sich y aus den Elementen $x_1, \ldots, x_k \in M$ erzeugen lässt.
- Dabei dürfen wir $P(x_1) \wedge \ldots \wedge P(x_k)$ als Induktionsvoraussetzung annehmen.

Beispiel 4.9

Wir betrachten die Menge M, die definiert ist durch:

(i) $7 \in M$

(ii) Gilt $x, y \in M$, dann gilt auch $3x \in M$ und $x + y \in M$.

Wir wollen zeigen, dass alle Elemente von M durch 7 teilbar sind, also:

$$\forall x \in M : 7|x$$

Induktionsanfang: $7|7$ ist wahr.
Induktionsschritt: Es gelte $x, y \in M$. Mit Induktionsvoraussetzung folgt $7|x$ und $7|y$, d. h.

$$\exists a \in \mathbb{N} : 7a = x$$
$$\exists b \in \mathbb{N} : 7b = y$$

Aus der ersten Aussage folgt $7 \cdot 3a = 3x$, also gilt auch $7|3x$.

Fortsetzung Beispiel.

Wenn wir die Gleichungen der beiden Aussagen addieren, erhalten wir

$$\begin{aligned} & 7a + 7b = x + y \\ \Rightarrow \quad & 7(a + b) = x + y \end{aligned}$$

Also gilt auch $7|(x + y)$.

Bemerkungen:

- Die Induktion geht hier über die Anzahl der Ableitungsschritte, um ein Element x herzuleiten.
- Wir beweisen praktisch, dass die Aussage

$$Q(n) \quad :\Leftrightarrow \quad \text{Eigenschaft } P \text{ gilt für alle Elemente, die mit } n \text{ Schritten abgeleitet werden können}$$

für alle $n \in \mathbb{N}_0$ gilt.

Strukturelle Induktion für formale Sprachen

- Die wichtigsten Mengen in der Informatik, die rekursiv definiert sind, sind formale Sprachen.
- Strukturelle Induktion erlaubt es uns nun, Spracheigenschaften induktiv entlang der Syntaxregeln nachzuweisen.

Beispiel 4.10

Wir wollen zeigen:

> *In jeder aussagenlogischen Formel ist die Anzahl der öffnenden Klammern gleich der Anzahl der schließenden Klammern.*

Zur Vereinfachung führen wir folgende Notation ein:

> *Für ein Zeichen c und eine aussagenlogische Formel α bezeichnet α_c die Anzahl der Vorkommen von c in α.*

Die Menge $\mathcal{A}$ der aussagenlogischen Formeln ist rekursiv definiert (siehe Folie 43).

Induktionsanfang: Atomare Formeln sind die aussagenlogischen Konstanten 0 und 1 und die Aussagenvariablen. Diese Formeln enthalten keine Klammern, also

$$\begin{aligned} 0_(&= 0 = 0_) \\ 1_(&= 0 = 1_) \\ x_(&= 0 = x_) \text{ für alle } x \in V \end{aligned}$$

Fortsetzung Beispiel.

Somit gilt die zu beweisende Aussage für alle atomaren Formeln.
Induktionsschritt: Für gegebene Formeln $\alpha, \beta \in \mathcal{A}$ können gemäß Definition von $\mathcal{A}$ die Formeln

$$\gamma = (\alpha \wedge \beta), \delta = (\alpha \vee \beta), \epsilon = \neg\alpha$$

gebildet werden.
Nach Induktionsvoraussetzung gilt $\alpha_(= \alpha_)$ und $\beta_(= \beta_)$.
Wir erhalten

$$\gamma_(= \alpha_(+ \beta_(+ 1 = \alpha_) + \beta_) + 1 = \gamma_)$$

$$\delta_(= \alpha_(+ \beta_(+ 1 = \alpha_) + \beta_) + 1 = \delta_)$$

$$\epsilon_(= \alpha_(= \alpha_) = \epsilon_)$$

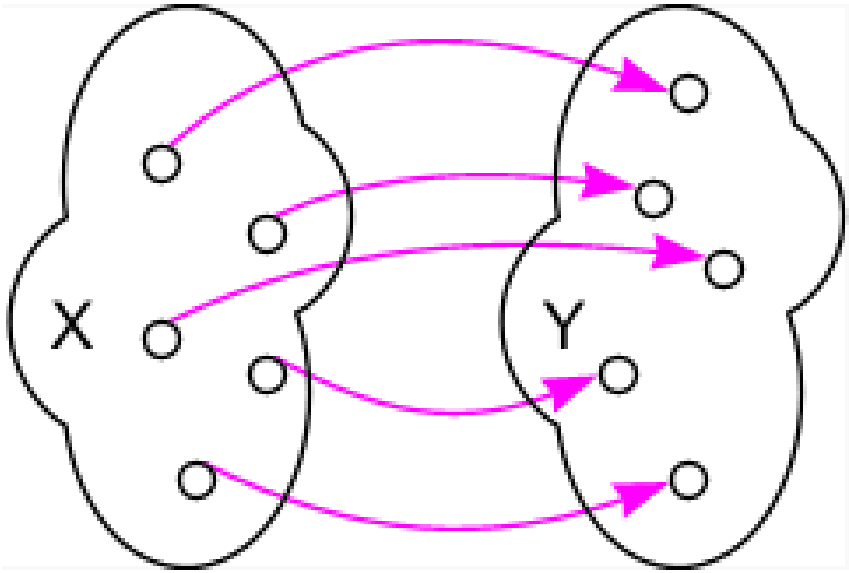
Damit ist der Induktionsschritt für alle Fälle bewiesen.

Zusammenfassung

- Beweisverfahren: direkter Beweis, indirekter Beweis, Widerspruchsbeweis, Ringschluss
- Vollständige Induktion um zu zeigen, dass eine Aussage $P(n)$ für alle $n \in \mathbb{N}$ wahr ist.
- vollständige Induktion = Induktionsanfang plus Induktionsschritt
- Induktionsanfang kann verschoben werden, um die Gültigkeit von $P(n)$ für alle $n \in \mathbb{N}_k$ zu zeigen.
- Strukturelle Induktion: Vollständige Induktion für formale Sprachen

Kapitel 5

Eigenschaften von Mengen, Relationen und Funktionen



Inhalt

Potenzmengen

Definition 5.1

Sei M eine Menge. Dann heißt

$$\mathcal{P}(M) = \{A | A \subseteq M\}$$

die Potenzmenge von M.

Bemerkungen:

- Die Potenzmenge $\mathcal{P}(M)$ ist also die Menge aller Teilmengen von M.
- Es gilt also: $A \in \mathcal{P}(M) :\Leftrightarrow A \subseteq M$.
- Anstelle von $\mathcal{P}(M)$ schreibt man auch 2^M.

Beispiel 5.2

Sei $M = \{a, b, c\}$, dann gilt

$$\mathcal{P}(M) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Folgerung 5.3

Für jede Menge M gilt $\emptyset \in \mathcal{P}(M)$ und $M \in \mathcal{P}(M)$.

Beweis.

Folgt direkt aus Satz 3.8.

Kardinalität der Potenzmenge

Satz 5.4

Es sei M eine Menge mit m Elementen, also $|M| = m$.

Dann hat $\mathcal{P}(M)$ 2^m Elemente, also $|\mathcal{P}(M)| = 2^{|M|}$.

Beweis.

Es sei $M = \{a_1, \ldots, a_m\}$.

- Zur Konstruktion einer Teilmenge A von M haben wir für jedes Element a_i genau zwei Möglichkeiten:
  - Wir nehmen a_i in A auf, also $a_i \in A$.
  - Wir nehmen a_i nicht auf, also $a_i \notin A$.
- Für jedes a_i können wir diese Entscheidung unabhängig von den anderen Elementen treffen.
- Unterschiedliche Entscheidungen führen zu unterschiedlichen Teilmengen.
- Ergibt insgesamt 2^m verschiedene Teilmengen.

Verknüpfung von Mengen

Definition 5.5

Es seien A und B zwei Mengen.

(i) Die Menge

$$A \cup B = \{x | x \in A \vee x \in B\}$$

heißt Vereinigung von A und B.

(ii) Die Menge

$$A \cap B = \{x | x \in A \wedge x \in B\}$$

heißt Durchschnitt oder Schnittmenge von A und B.

(iii) Gilt $A \cap B = \emptyset$, dann heißen A und B disjunkt.

(iv) Die Menge

$$A \setminus B = \{x | x \in A \wedge x \notin B\}$$

heißt Differenz von A und B.

Fortsetzung Definition.

(v) Für $A \subseteq B$ heißt $B \setminus A$ das Komplement von A bezüglich B. Falls die Menge B aus dem Zusammenhang heraus klar ist, schreiben wir stattdessen A^C.

Beispiel 5.6

Es sei $A = \{1, 2, 3, 4\}$ und $B = \{3, 4, 5\}$. Dann gilt:

(i) $A \cup B = \{1, 2, 3, 4, 5\}$

(ii) $A \cap B = \{3, 4\}$

(iii) $A \setminus B = \{1, 2\}$

Es sei nun $B = \mathbb{N}$. Dann gilt

(iv) $A^C = \{5, 6, 7, \ldots\} = \mathbb{N}_5$

Weitere Schreibweisen für Mengen

Für die Vereinigung bzw. den Durchschnitt von n Mengen $A_1, A_2, \ldots, A_n$ führen wir folgende Schreibweisen ein:

$$A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i$$

$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i$$

Dies verallgemeinern wir noch für den Fall, dass die Indizes nicht die Zahlen $1, \ldots, n$ sind, sondern Elemente einer (möglicherweise unendlichen) Indexmenge I:

$$\bigcup_{i \in I} A_i \quad \text{bzw.} \quad \bigcap_{i \in I} A_i$$

Beispiel 5.7

Sei

$$T = \{mo, di, mi, do, fr, sa\}$$

eine Indexmenge, und sei K_t die Menge der Kunden, die am Tag $t \in T$ gekauft haben. Dann bezeichnet

$$\bigcup_{t \in T} K_t$$

die Menge der Kunden, die irgendwann mal gekauft haben, und

$$\bigcap_{t \in T} K_t$$

bezeichnet die Menge der Kunden, die jeden Tag gekauft haben.

Da als Indexmenge auch unendliche Mengen erlaubt sind, können wir auch

$$\bigcup_{i \in \mathbb{N}} A_i \quad \text{und} \quad \bigcap_{i \in \mathbb{N}} A_i$$

bilden. Hierfür schreiben wir üblicherweise

$$\bigcup_{i=1}^{\infty} A_i \quad \text{bzw.} \quad \bigcap_{i=1}^{\infty} A_i.$$

Beispiel 5.8

Für $i \in \mathbb{N}$ sei $A_i = \{x \in \mathbb{R} | 1 - \frac{1}{i} \leq x \leq 2 + \frac{1}{i}\}$. Dann gilt:

$$\bigcap_{i=1}^{\infty} A_i = \{x \in \mathbb{R} | 1 \leq x \leq 2\}.$$

Verknüpfungseigenschaften

Satz 5.9

Für alle Mengen A, B, C gelten die folgenden Gesetze:

(1) Kommutativität:

$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \end{aligned}$$

(2) Für $A \subseteq B$ gilt:

$$\begin{aligned} A \cup B &= B \\ A \cap B &= A \\ A \setminus B &= \emptyset \end{aligned}$$

(3) Idempotenz:

$$\begin{aligned} A \cup A &= A \\ A \cap A &= A \end{aligned}$$

(4) Aus (1) bis (3) folgt:

$$\begin{aligned} A \cup \emptyset &= A \\ A \cap \emptyset &= \emptyset \\ A \setminus A &= \emptyset \\ \emptyset \setminus A &= \emptyset \\ A \setminus \emptyset &= A \end{aligned}$$

Fortsetzung Satz.

(5) Für $\cup, \cap, \setminus$ gilt:

$$\begin{aligned} A &\subseteq A \cup B \\ B &\subseteq A \cup B \\ A \cap B &\subseteq A \\ A \cap B &\subseteq B \\ A \setminus B &\subseteq A \end{aligned}$$

(6) Assoziativität:

$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C \\ A \cap (B \cap C) &= (A \cap B) \cap C \end{aligned}$$

(10) Doppelte Komplementbildung:

$$\left(A^C\right)^C = A$$

(7) Distributivität:

$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \end{aligned}$$

(8) De Morgansche Regeln:

$$\begin{aligned} (A \cup B)^C &= A^C \cap B^C \\ (A \cap B)^C &= A^C \cup B^C \end{aligned}$$

(9) Absorptionsgesetze:

$$\begin{aligned} A \cup (B \cap A) &= A \\ A \cap (B \cup A) &= A \end{aligned}$$

Bemerkung:

- Beachten Sie: Die Verknüpfungseigenschaften von Mengen sind sehr ähnlich zu den logischen Äquivalenzen in der Aussagenlogik (siehe Satz 2.24).
- Dies ist kein Zufall.

Beweis.

- Mit Ausnahme der Eigenschaft (5) ist immer die Gleichheit von Mengen zu zeigen.
- Zwei Mengen sind nach Definition gleich, wenn jede Teilmenge der anderen ist.
- Mit dieser Methode zeigen wir die erste Gleichheit von (8).
- Alle anderen Beweise sind Übung und teilweise Übungsaufgabe.
- Fast alle Gleichheiten lassen sich auf die Bedingungen zurückführen, mithilfe derer die Mengenoperationen definiert sind (siehe Definition 5.5).

Fortsetzung Beweis.

Wir zeigen $(A \cup B)^C \subseteq A^C \cap B^C$:

$$\begin{aligned} x \in (A \cup B)^C &\Rightarrow x \notin A \cup B \\ &\Rightarrow \neg(x \in A \cup B) \\ &\Rightarrow \neg(x \in A \vee x \in B) \\ &\Rightarrow x \notin A \wedge x \notin B \\ &\Rightarrow x \in A^C \wedge x \in B^C \\ &\Rightarrow x \in A^C \cap B^C \end{aligned}$$

Der Beweis von $A^C \cap B^C \subseteq (A \cup B)^C$ erfolgt durch Umkehrung der Implikationen.

Partition

Folgerung 5.10

(i) *Für zwei endliche Mengen A und B gilt:*

$$|A \cup B| = |A| + |B| - |A \cap B|$$

(ii) *Sind A und B endlich und disjunkt, dann gilt:*

$$|A \cup B| = |A| + |B|$$

Definition 5.11

Sei A eine nicht leere Menge, I eine Indexmenge und $A_i \subseteq A, i \in I$, eine Familie von nicht leeren Teilmengen von A.
Dann heißt $\{A_i\}_{i \in I}$ eine Partition von A genau dann, wenn gilt:

(i) $A_i \cap A_j = \emptyset$ für $i, j \in I$ mit $i \neq j$,

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

Beispiel 5.12

(i) Für $A = \{1, 2, 3, 4, 5, 6\}$ ist $\{A_i\}_{i \in \{1,2,3\}}$ mit $A_1 = \{1, 4, 6\}$, $A_2 = \{2\}$ und $A_3 = \{3, 5\}$ eine Partition.

(ii) Die Mengen $\mathbb{G}_+$ und $\mathbb{U}_+$ bilden eine Partition von $\mathbb{N}_0$.

(iii) Die Mengen

$$\begin{array}{rcccl} [0]_3 & = & \{0, 3, 6, \ldots\} & = & \{z | z = 3k, k \in \mathbb{N}_0\} \\ [1]_3 & = & \{1, 4, 7, \ldots\} & = & \{z | z = 3k + 1, k \in \mathbb{N}_0\} \\ [2]_3 & = & \{2, 5, 8, \ldots\} & = & \{z | z = 3k + 2, k \in \mathbb{N}_0\} \end{array}$$

bilden eine Partition von $\mathbb{N}_0$.

Verfeinerung einer Partition

Definition 5.13

Es gelten die Bezeichnung von Definition 5.11. Außerdem sei $J \subseteq I$ eine weitere Indexmenge und $\{B_j\}_{j \in J}$ eine weitere Partition von A.

Dann heißt die Partition $\{A_i\}_{i \in I}$ feiner als die Partition $\{B_j\}_{j \in J}$, falls zu jedem $i \in I$ ein $j \in J$ existiert mit $A_i \subseteq B_j$.

Weiterhin heißt dann $\{B_j\}_{j \in J}$ gröber als $\{A_i\}_{i \in I}$.

Beispiel 5.14

Die Mengen

$$[i]_6 = \{z | z = 6k + i, k \in \mathbb{N}_0\}$$

für $0 \leq i \leq 5$ bilden eine feinere Partition von $\mathbb{N}_0$ als die Partition von Beispiel 5.12.

Schreibweisen für Relationsbeziehungen

Wir wollen die Tatsache, dass ein Paar $(x, y) \in A \times B$ zu einer Relation $R \subseteq A \times B$ gehört („in der Beziehung R stehen“), ausdrücken, indem wir die

- normale Elementschreibweise $(x, y) \in R$,
- die Präfixschreibweise $R(x, y)$ oder
- die Infixschreibweise xRy verwenden.

Spezielle Relationen

Definition 5.15

(i) Ist $R = \emptyset$, dann heißt R Nullrelation.

(ii) Ist $R = A \times B$, dann heißt R vollständig.

(iii) Die Relation

$$R = \{(x, x) | x \in A\} \subseteq A \times A$$

heißt identische Relation über A. Sie wird in der Regel mit id_A bezeichnet.

Relationseigenschaften

Definition 5.16

Sei $R \subseteq A \times A$ eine zweistellige homogene Relation über der Grundmenge A. Dann heißt R

(i) reflexiv genau dann, wenn xRx für alle $x \in A$,

(ii) irreflexiv genau dann, wenn $(x, x) \notin R$ für alle $x \in A$,

(iii) symmetrisch genau dann, wenn gilt: $xRy \Rightarrow yRx$,

(iv) asymmetrisch genau dann, wenn gilt: $xRy \Rightarrow \neg yRx$,

(v) antisymmetrisch genau dann, wenn gilt: $xRy \wedge yRx \Rightarrow x = y$,

(vi) transitiv genau dann, wenn gilt: $xRy \wedge yRz \Rightarrow xRz$.

Beispiel 5.17

Wir definieren die Relation $\leq \subseteq \mathbb{N}_0 \times \mathbb{N}_0$ durch

$$x \leq y \text{ genau dann, wenn } c \in \mathbb{N}_0 \text{ existiert, so dass } x + c = y.$$

Es gilt z. B. $3 \leq 5$, denn mit $c = 2$ gilt $3 + c = 5$.

- $\leq$ ist reflexiv, denn für jedes $x \in \mathbb{N}_0$ gibt es $c = 0$ mit $x + c = x$.
- $\leq$ ist nicht symmetrisch, denn es gilt z. B. $3 \leq 5$, aber nicht $5 \leq 3$.
- $\leq$ ist antisymmetrisch: ✎
- Da die Relation reflexiv ist, ist sie nicht asymmetrisch.
- $\leq$ ist transitiv: ✎

Noch mehr Relationseigenschaften

Definition 5.18

Sei $R \subseteq A \times B$ eine zweistellige Relation. Dann heißt R:

(i) linkseindeutig oder injektiv genau dann, wenn gilt: Ist $x_1 R y_1, x_2 R y_2$ und $x_1 \neq x_2$, dann muss $y_1 \neq y_2$ gelten.

(ii) rechtseindeutig genau dann, wenn gilt: Ist $x_1 R y_1, x_2 R y_2$ und $y_1 \neq y_2$, dann muss $x_1 \neq x_2$ gelten.

(iii) linkstotal oder total genau dann, wenn gilt: Für alle $a \in A$ existiert ein $y \in B$ mit xRy.

(iv) rechtstotal oder surjektiv genau dann, wenn gilt: Für alle $y \in B$ existiert ein $x \in A$ mit xRy.

(v) bijektiv genau dann, wenn R total, injektiv und surjektiv ist.

Beispiel 5.19

Wir untersuchen weitere Eigenschaften der Relation $\leq$ von Beispiel 5.17.

- $\leq$ ist nicht injektiv, denn es gilt z. B. $3 \leq 5$ und $4 \leq 5$. Damit ist die Relation auch nicht bijektiv.
- $\leq$ ist nicht rechtseindeutig und damit keine Funktion, denn es gilt z. B. $3 \leq 4$ und $3 \leq 5$.
- Da $\leq$ reflexiv ist, ist sie auch total und surjektiv.

Partielle Ordnung

Definition 5.20

Eine Relation $R \subseteq A \times A$ heißt partielle Ordnung über A genau dann, wenn R reflexiv, antisymmetrisch und transitiv ist.

Partielle Ordnungen werden auch einfach nur Ordnungen genannt.

Ist R eine partielle Ordnung über A, dann schreibt man dafür auch (A, R) und nennt A eine geordnete Menge.

Beispiel 5.21

(i) Die Relation $\leq$ aus Beispiel 5.17 ist eine partielle Ordnung.

(ii) Die Teilbarkeitsrelation $|$ bildet eine partielle Ordnung auf $\mathbb{N}$.

(iii) Es sei M eine Menge. Dann bildet die Teilmengenrelation $\subseteq$ eine partielle Ordnung über $\mathcal{P}(M)$.

Begriffe im Kontext partieller Ordnungen

Definition 5.22

Sei (A, R) eine partielle Ordnung und $x, y \in A$.

(i) Gilt xRy oder yRx, dann heißen x und y vergleichbar, ansonsten unvergleichbar.

(ii) Sei $B \subseteq A, B \neq \emptyset$. $x \in B$ heißt minimales Element von B, falls xRy für alle $y \in B$ gilt. $x \in B$ heißt maximales Element von B, falls yRx für alle $y \in B$ gilt.

(iii) $K \subseteq A, K \neq \emptyset$ heißt Kette genau dann, wenn für alle $x, y \in K$ gilt, dass x und y vergleichbar sind.

(iv) (A, R) heißt totale Ordnung oder auch lineare Ordnung genau dann, wenn A eine Kette bildet.

(v) Eine totale Ordnung (A, R) ist eine Wohlordnung genau dann, wenn jede Teilmenge $K \subseteq A, K \neq \emptyset$ ein minimales Element besitzt.

Beispiel 5.23

(i) Die Teilbarkeitsrelation bildet keine totale Ordnung auf $\mathbb{N}$, denn es gibt Zahlen p, q, für die sowohl $p \nmid q$ als auch $q \nmid p$ gilt.

(ii) Die partielle Ordnung $(\mathcal{P}(\{a, b, c\}), \subseteq)$ ist ebenfalls nicht total, denn bspw. $\{a, b\}$ und $\{b, c\}$ sind unvergleichbar.

(iii) Die partielle Ordnung $(\mathcal{P}(\{a, b, c\}), \subseteq)$ enthält unter anderem die Kette $\{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$, denn

$$\emptyset \subseteq \{a\} \subseteq \{a, b\} \subseteq \{a, b, c\}$$

(iv) $\{a, b, c\}$ ist ein maximales Element von $\mathcal{P}(\{a, b, c\})$ und $\emptyset$ ein minimales Element.

(v) Die Relation $\leq$ aus Beispiel 5.17 ist eine totale Ordnung und eine Wohlordnung.

Fortsetzung Beispiel.

(vi) Wenn wir die Ordnung $\leq$ aus Beispiel 5.17 auf die ganzen Zahlen erweitern, dann bildet $(\mathbb{Z}, \leq)$ zwar eine totale Ordnung, aber keine Wohlordnung.

Begründung: Bspw. hat die Teilmenge $\mathbb{G}$ der geraden Zahlen kein minimales Element in $\mathbb{Z}$.

(vii) Wir können für $\mathbb{Z}$ aber eine andere Ordnung definieren, die dann auch eine Wohlordnung ist. Wir definieren $\phi : \mathbb{Z} \to \mathbb{N}_0$ durch

$$\phi(x) = \begin{cases} 2x & \text{falls } x \geq 0 \\ -(2x+1) & \text{falls } x < 0 \end{cases}$$

und für $x, y \in \mathbb{Z}$ gelte

$$x \leq_\phi y :\Leftrightarrow \phi(x) \leq \phi(y).$$

Dann ist $(\mathbb{Z}, \leq_\phi)$ eine Wohlordnung.

$\leq$ als Prototyp einer totalen Ordnung

- Da die Relation $\leq$ auf allen Zahlenmengen eine totale Ordnung festlegt, gilt sie als Prototyp für totale Ordnungen.
- Deshalb benutzt man das Symbol $\leq$ auch ganz allgemein als Symbol für totale Ordnungen.
- Wird also $(A, \leq)$ für irgendeine Menge A notiert, soll dies bedeuten, dass eine total geordnete Menge A vorliegt.

Dichte Ordnungen

Definition 5.24

Sei $(A, \leq)$ eine totale Ordnung.

A heißt dicht bezüglich $\leq$ genau dann, wenn für alle $x, y \in A$ mit $x \neq y$ und $x \leq y$ ein $z \in A$ existiert mit $z \neq x, z \neq y$ und $x \leq z \leq y$.

- $\forall x \in A \forall y \in A : x < y \Rightarrow \exists z : x < z < y$
- Eine geordnete Menge ist also dicht, wenn zwischen zwei Elementen dieser Menge immer noch ein drittes liegt.

Beispiel 5.25

(i) $(\mathbb{N}_0, \leq)$ und $(\mathbb{Z}, \leq)$ sind nicht dicht.

Begründung: Zwischen zwei benachbarten natürlichen bzw. ganzen Zahlen x und $y = x + 1$ liegt keine weitere ganze bzw. natürliche Zahl.

(ii) Die Menge $\mathbb{Q}$ der rationalen Zahlen ist dicht.

Begründung: Sei $a, b \in \mathbb{Q}$ mit $a \leq b$ und $a \neq b$.

- $\frac{a+b}{2} \in \mathbb{Q}$
- $a \neq \frac{a+b}{2}$ und $b \neq \frac{a+b}{2}$
- $a = \frac{a+a}{2} \leq \frac{a+b}{2} \leq \frac{b+b}{2} = b$

Äquivalenzrelationen

Definition 5.26

Eine Relation $R \subseteq A \times A$ heißt Äquivalenzrelation über A genau dann, wenn R reflexiv, symmetrisch und transitiv ist.

Beispiel 5.27

Die Relation $\equiv_3 \subseteq \mathbb{Z} \times \mathbb{Z}$ sei definiert durch

$$x \equiv_3 y \quad :\Leftrightarrow \quad \frac{x-y}{3} \in \mathbb{Z}$$

$\equiv_3$ ist eine Äquivalenzrelation.

Begründung: Tafel ✎

Äquivalenzklasse

Definition 5.28

Sei $R \subseteq A \times A$ eine Äquivalenzrelation und $x \in A$. Dann heißt die Menge

$$[x]_R = \{y \in A | xRy\}$$

Äquivalenzklasse von R. x heißt Repräsentant der Äquivalenzklasse $[x]_R$.
Die Anzahl der Äquivalenzklassen von R heißt Index von R.

Beispiel 5.29

$$\begin{array}{lcll} [0]_{\equiv_3} & = & \{0, 3, -3, 6, -6, \ldots\} & = \{x | x = 3y, y \in \mathbb{Z}\} \\ [1]_{\equiv_3} & = & \{1, -2, 4, -5, 7, -8, \ldots\} & = \{x | x = 3y + 1, y \in \mathbb{Z}\} \\ [2]_{\equiv_3} & = & \{2, -1, 5, -4, 8, -7, \ldots\} & = \{x | x = 3y + 2, y \in \mathbb{Z}\} \end{array}$$

Eigenschaften von Äquivalenzrelationen

Satz 5.30

Sei $R \subseteq A \times A$ mit $A \neq \emptyset$ eine Äquivalenzrelation. Dann gilt:

(i) *Für alle $x \in A$ ist $[x]_R \neq \emptyset$.*

Äquivalenzklassen sind niemals leer.

(ii) *Für alle $y \in [x]_R$ gilt $[x]_R = [y]_R$.*

Äquivalenzklassen sind unabhängig von ihrem Repräsentanten.

(iii) *Falls $(x, y) \notin R$ ist, dann ist $[x]_R \cap [y]_R = \emptyset$.*

Die Äquivalenzklassen nicht in Beziehung stehender Repräsentanten sind disjunkt.

(iv) *Für $x, y \in A$ gilt entweder $[x]_R = [y]_R$ oder $[x]_R \cap [y]_R = \emptyset$.*

Zwei Elemente der Grundmenge repräsentieren entweder dieselbe oder zwei disjunkte Äquivalenzklassen.

Fortsetzung Satz.

(v) $A = \bigcup_{x \in A} [x]_R$.

Die Äquivalenzklassen bilden eine Überdeckung von A.

Beweis.

(i) Folgt aus der Reflexivität.

(ii) Folgt aus der Symmetrie.

(iii) Folgt aus Symmetrie und Transitivität mit Widerspruchsbeweis.

(iv) Folgt unmittelbar aus (ii) und (iii).

(v) Folgt aus $x \in [x]_R$.

Genaueres: Tafel ✎

Partitionen für Äquivalenzrelationen

Folgerung 5.31

(i) *Jede Äquivalenzrelation $R \subseteq A \times A$ legt eine Partition von A fest.*

(ii) *Jede Partition von A definiert eine Äquivalenzrelation auf A.*

(iii) *Die identische Relation id_A legt die feinste Partition von A fest.*

(iv) *Die vollständige Relation $R = A \times A$ legt die gröbste Partition auf A fest.*

Umkehrrelationen

Definition 5.32

Für eine Relation $R \subseteq A \times B$ heißt die Relation $R^{-1} \subseteq B \times A$ definiert durch

$$yR^{-1}x \text{ genau dann, wenn } xRy$$

die Umkehrrelation zu R.

Folgerung 5.33

(i) $R^{-1} = \{(y, x) \in B \times A | (x, y) \in R\}$

(ii) *$R \subseteq A \times B$ ist linkseindeutig genau dann, wenn R^{-1} rechtseindeutig ist.*

(iii) *$R \subseteq A \times B$ ist bijektiv genau dann, wenn R^{-1} bijektiv ist.*

(iv) *Ist $R \subseteq A \times A$ eine Äquivalenzrelation, dann gilt $R = R^{-1}$.*

Komposition von Relationen

Definition 5.34

Seien A, B, C Mengen sowie $R \subseteq A \times B$ und $S \subseteq B \times C$ Relationen.

Dann heißt die Relation $R \circ S \subseteq A \times C$ definiert durch

$$R \circ S = \{(x, z) | \exists y \in B : xRy \wedge ySz\}$$

die Komposition von R und S.

Beispiel 5.35

Die Relationen $R_1, R_2 \subseteq \mathbb{N} \times \mathbb{N}$ seien definiert durch

$$R_1 = \{(x,y) | x,y \in \mathbb{N} \wedge y = 2x\} = \{(1,2),(2,4),(3,6),\ldots\}$$
$$R_2 = \{(x,y) | x,y \in \mathbb{N} \wedge y = 3x\} = \{(1,3),(2,6),(3,9),\ldots\}$$

Die Komposition von R_1 und R_2 ergibt

$$\begin{aligned} R_1 \circ R_2 &= \{(1,6),(2,12),(3,18),\ldots\} \\ &= \{(x,y) | x,y \in \mathbb{N} \wedge y = 6x\} \end{aligned}$$

Eigenschaften der Komposition (1)

Verknüpfung mit der identischen Relation, total, surjektiv.

Satz 5.36

Seien A, B Mengen und $R \subseteq A \times B$ eine Relation. Dann gilt:

(i) $\mathrm{id}_A \circ R = R$,

(ii) $R \circ \mathrm{id}_B = R$,

(iii) *ist R total, dann ist* $\mathrm{id}_A \subseteq R \circ R^{-1}$, *und*

(iv) *ist R surjektiv, dann ist* $\mathrm{id}_B \subseteq R^{-1} \circ R$.

Eigenschaften der Komposition (2)

Komposition und Umkehrrelation, Assoziativgesetz, Distributivgesetze für Komposition, Vereinigung und Durchschnitt.

Satz 5.37

Sei $R \subseteq A \times B, S \subseteq B \times C, T \subseteq C \times D$. *Dann gilt:*

(i) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$

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

Sei $R \subseteq A \times B, S \subseteq B \times C, T \subseteq B \times C$. *Dann gilt:*

(iii) $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$
$R \circ (S \cap T) \subseteq (R \circ S) \cap (R \circ T)$

Eigenschaften der Komposition (3)

Komposition und Teilmengeneigenschaft.

Satz 5.38

Es seien $R_1, R_2 \subseteq A \times B$ *und* $S_1, S_2 \subseteq B \times C$ *Relationen. Dann gilt:*

$$R_1 \subseteq R_2 \wedge S_1 \subseteq S_2 \quad \Longrightarrow \quad R_1 \circ S_1 \subseteq R_2 \circ S_2$$

Relationseigenschaften anders formuliert

Satz 5.39

Sei $R \subseteq A \times A$ eine Relation. Dann gilt:

(i) *R ist reflexiv genau dann, wenn $\mathrm{id}_A \subseteq R$,*

(ii) *R ist irreflexiv genau dann, wenn $\mathrm{id}_A \cap R = \emptyset$,*

(iii) *R ist symmetrisch genau dann, wenn $R = R^{-1}$,*

(iv) *R ist asymmetrisch genau dann, wenn $R \cap R^{-1} = \emptyset$,*

(v) *R ist antisymmetrisch genau dann, wenn $R \cap R^{-1} \subseteq \mathrm{id}_A$,*

(vi) *R ist transitiv genau dann, wenn $R \circ R \subseteq R$,*

(vii) *R ist injektiv genau dann, wenn $R \circ R^{-1} \subseteq \mathrm{id}_A$,*

(viii) *R ist rechtseindeutig genau dann, wenn $R^{-1} \circ R \subseteq \mathrm{id}_A$,*

(ix) *R ist total genau dann, wenn $\mathrm{id}_A \subseteq R \circ R^{-1}$,*

(x) *R ist surjektiv genau dann, wenn $\mathrm{id}_A \subseteq R^{-1} \circ R$,*

(xi) *R ist bijektiv genau dann, wenn $R \circ R^{-1} \subseteq R^{-1} \circ R$.*

Reflexiv-transitive Hülle

Definition 5.40

Sei $R \subseteq A \times A$ eine zweistellige Relation über A. Für R definieren wir:

(i) $R^0 = \mathrm{id}_A$

(ii) $R^n = R^{n-1} \circ R$ für $n \geq 1$

(iii) $R^+ = R^1 \cup R^2 \cup \ldots = \bigcup_{i=1}^{\infty} R^i$

(iv) $R^* = R^0 \cup R^+ = \bigcup_{i=0}^{\infty} R^i$

R^+ heißt die transitive Hülle von R und R^* die reflexiv-transitive Hülle von R.

Beispiel 5.41

- Es sei M die Menge der Menschen, die bisher auf der Erde gelebt haben.
- Die Relation $K \subseteq M \times M$ sei definiert durch:

$$x \, K \, y :\Leftrightarrow x \text{ ist ein Kind von } y$$

- Dann enthält K^2 alle Enkel-Beziehungen, K^3 alle Urenkel-Beziehungen usw.
- K^+ enthält alle Nachkommen-Beziehungen über alle Generationen hinweg.

Beispiel 5.42

Sei $R \subseteq \mathbb{N} \times \mathbb{N}$ definiert durch:

$$x \, R \, y :\Leftrightarrow y = 2x$$

Damit gilt:

(i) $R^0 = \mathrm{id}_{\mathbb{N}} = \{(1,1),(2,2),(3,3),\ldots\} = \{(x,x) | x \in \mathbb{N}\}$

(ii) $R^1 = R^0 \circ R = \mathrm{id}_{\mathbb{N}} \circ R = \{(1,2),(2,4),(3,6),\ldots\} = \{(x,y) | y = 2x\}$

(iii) Fortgesetzte Komposition von R:

$$\begin{array}{lllll}
R^2 & = & R \circ R & = & \{(1,4),(2,8),(3,12),\ldots\} & = & \{(x,y) | y = 4x\} \\
R^3 & = & R^2 \circ R & = & \{(1,8),(2,16),(3,24),\ldots\} & = & \{(x,y) | y = 8x\} \\
\vdots & & \vdots & & & \vdots & \\
R^n & = & R^{n-1} \circ R & = & \{(1,2^n \cdot 1),(2,2^n \cdot 2),\ldots\} & = & \{(x,y) | y = 2^n x\}
\end{array}$$

(iv) $R^* = \{(x,y) | y = 2^n x, n \in \mathbb{N}_0\}$

(v) $R^+ = \{(x,y) | y = 2^n x, n \in \mathbb{N}\}$

Funktionsbegriff

- Zur Erinnerung: Funktion definiert in Definition 3.14
- zweistellige, totale, rechtseindeutige Relation
- Schreibweise:

$$f : A \to B$$

bzw.

$$f : A \to B, x \mapsto f(x)$$

und $y = f(x)$ statt $(x, y) \in f$.

- A ist der Definitionsbereich, B der Wertebereich von f.
- Begriff der Abbildung: Kombination aus Funktionsvorschrift f und den Mengen A und B.
- Wir gebrauchen die beiden Begriffe synonym.

Bild und Urbild

Definition 5.43

Sei $f : A \to B$ eine Funktion, $x \in A, y \in B, C \subseteq A$ und $D \subseteq B$.

Dann heißt:

(i) $y = f(x)$ das Bild des Arguments x unter f.

(ii) $f(C) = \{f(x) | x \in C\}$ das Bild von C unter f.

(iii) $f^{-1}(y) = \{x \in A | f(x) = y\}$ die Urbildmenge von y unter f.

(iv) $f^{-1}(D) = \{x \in A | f(x) \in D\}$ die Urbildmenge von D unter f.

Funktionseigenschaften

Folgerung 5.44

Sei $f : A \to B$ eine Funktion. Dann gilt:

(a) *f ist injektiv genau dann, wenn $|f^{-1}(y)| \leq 1$ für alle $y \in B$ ist.*
Jedes Element des Wertebereichs hat höchstens ein Urbild.

(b) *f ist surjektiv genau dann, wenn $|f^{-1}(y)| \geq 1$ für alle $y \in B$ ist.*
Jedes Element des Wertebereichs hat mindestens ein Urbild.

(c) *f ist bijektiv genau dann, wenn $|f^{-1}(y)| = 1$ für alle $y \in B$ ist.*
Jedes Element des Wertebereichs hat genau ein Urbild.

(d) *f ist genau dann bijektiv, wenn f^{-1} bijektiv ist.*

Beispiel 5.45

(i) Wir betrachten die Funktion $f : \mathbb{R} \to \mathbb{R}$ mit

$$f(x) = 3x + 5$$

Ist f surjektiv, injektiv, bijektiv? Ist f^{-1} eine Funktion?

(ii) Wir betrachten die Funktion $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ mit

$$f(x) = \frac{1}{x}$$

Ist f surjektiv, injektiv, bijektiv? Ist f^{-1} eine Funktion?

(iii) Wir betrachten die Funktion $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ mit

$$f(x) = \frac{1}{x^2}$$

Ist f surjektiv, injektiv, bijektiv? Ist f^{-1} eine Funktion?

Komposition von Funktionen

- Wie Relationen können auch Funktionen komponiert werden.
- Für $f : A \to B$ und $g : B \to C$ schreiben wir

$$g \circ f : A \to C$$

- Achtung: andere Reihenfolge als bei Relationen
- Begründung: Auswertung von innen nach außen:

$$(g \circ f)(x) = g(f(x))$$

Beispiel 5.46

Sei
$f : \mathbb{N}_0 \to \mathbb{N}_0$ definiert durch $f(x) = 2x + 1$ und
$g : \mathbb{N}_0 \to \mathbb{N}_0$ definiert durch $g(x) = x^2$.

Dann gilt:

$$(g \circ f)(x) = g(f(x)) = g(2x + 1) = (2x + 1)^2 = 4x^2 + 4x + 1$$

und

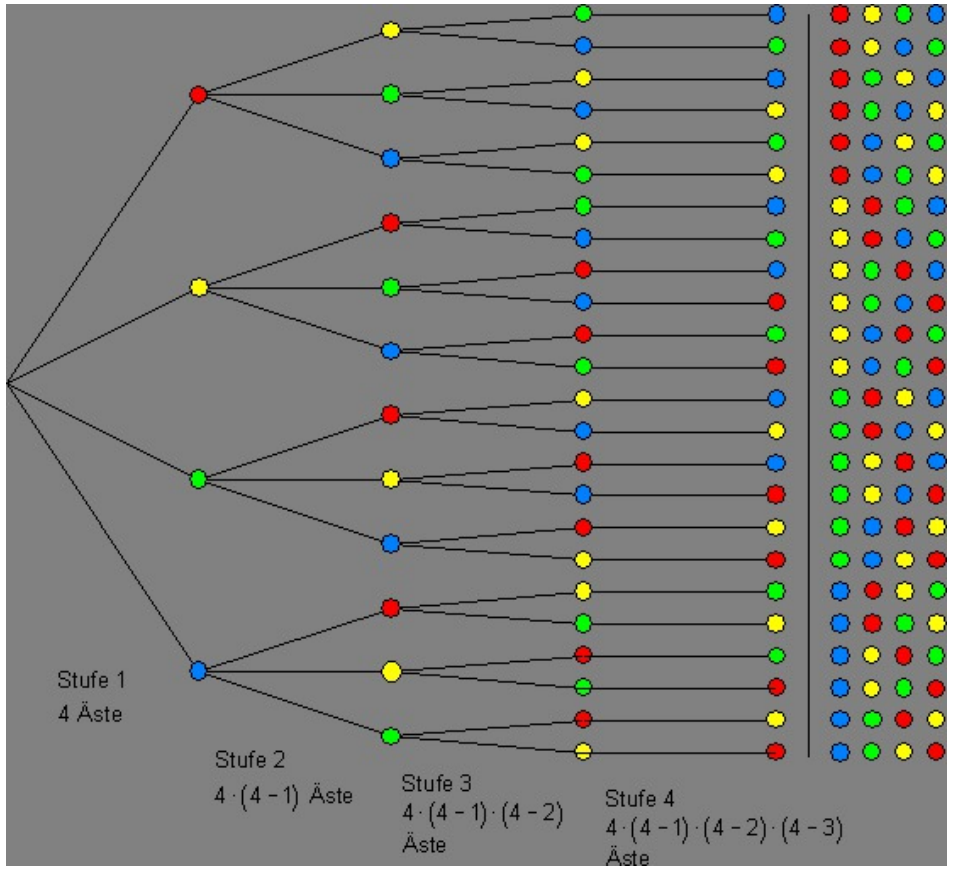
$$(f \circ g)(x) = f(g(x)) = f(x^2) = 2x^2 + 1$$

Zusammenfassung

- Potenzmenge als Menge aller Teilmengen
- Verknüpfungseigenschaften der Mengenoperationen ähnlich zur Aussagenlogik
- wichtige Relationseigenschaften: Reflexivität, Symmetrie, Transitivität
- spezielle Relationen: Partielle Ordnung und Äquivalenzrelation
- Komposition von Relationen und die transitive Hülle
- Funktion und Funktionseigenschaften: Surjektivität, Injektivität, Bijektivität, Bild und Urbild, Umkehrfunktion
- Komposition von Funktionen

Kapitel 6

Elementare Kombinatorik und Abzählbarkeit



Inhalt

Multiplikationssymbol

- Zur Notation eines Produktes mehrerer Faktoren $x_1, x_2, \ldots, x_n$ verwenden wir das Symbol $\prod$:

$$x_1 \cdot x_2 \cdot \ldots \cdot x_n = \prod_{i=1}^{n} x_i$$

- Der Multiplikationsindex kann dabei auch zwischen $u, o \in \mathbb{N}_0$ laufen:

$$x_u \cdot x_{u+1} \cdot \ldots \cdot x_o = \prod_{i=u}^{o} x_i$$

- Für den Fall $u > o$ legen wir fest:

$$\prod_{i=u}^{o} x_i = 1$$

Fakultät

Definition 6.1

Für $n \in \mathbb{N}$ heißt das Produkt

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

Fakultät von n. Wir setzen $0! = 1$.

Beispiel 6.2

$$\begin{aligned} 5! &= 120 \\ 10! &= 3628800 \\ 20! &= 2432902008176640000 \\ 30! &= 265252859812191058636308480000000 \end{aligned}$$

Permutation

Definition 6.3

Es sei $X = \{x_1, x_2, \ldots, x_n\}$ eine n-elementige Menge. Dann heißt eine bijektive Abbildung

$$\sigma : X \to X$$

Permutation.

Satz 6.4

Für eine n-elementige Menge X gibt es n! verschiedene Permutationen.

- Für die mathematische Betrachtung von Permutationen beschränkt man sich üblicherweise auf $X = \{1, 2, \ldots, n\}$.
- Für uns ist eine Permutation also stets eine bijektive Abbildung

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}.$$

Schreibweise von Permutationen

Eine Permutation $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ stellt man üblicherweise in Form einer zweizeiligen Matrix

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

oder verkürzt in Tupelform

$$\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

dar.

Beispiel 6.5

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 & 2 \end{pmatrix}$$

Symmetrische Gruppe

Definition 6.6

S_n bezeichne die Menge aller Permutationen auf der Menge $\{1, 2, \ldots, n\}$.

Bemerkung:

- $(S_n, \circ)$ bildet mit der Komposition $\circ$ von Abbildungen als Verknüpfung eine Gruppe.
- S_n wird auch als symmetrische Gruppe bezeichnet.
- Eine Permutationsgruppe ist eine Untergruppe von S_n.
- Nach dem sogenannten Satz von Cayley ist jede endliche Gruppe isomorph zu einer Permutationsgruppe (siehe Algebra).

Binomialkoeffizient

Definition 6.7

Sei $n, k \in \mathbb{N}_0$. Dann heißt der Ausdruck

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Binomialkoeffizient von n über k.

Rechenregeln für Binomialkoeffizienten

Satz 6.8

Es gilt:

(i)

$$\binom{n}{k} = \binom{n}{n-k}$$

(ii)

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Beweis.

Übungsaufgabe.

Anzahl k-elementiger Teilmengen

Satz 6.9

Es sei M eine n-elementige Menge.
Dann gibt es $\binom{n}{k}$ verschiedene k-elementige Teilmengen von M, also:

$$|\{A \in \mathcal{P}(M) \,|\, |A| = k\}| = \binom{n}{k}$$

Beweis.

Vollständige Induktion über n. Induktionsanfang bei $n = 0$ für die leere Menge.

Binomischer Lehrsatz

Satz 6.10

Für alle $a, b \in \mathbb{R}$ und alle $n \in \mathbb{N}_0$ gilt:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Beweis.

Vollständige Induktion, Übungsaufgabe.
Hinweis: Indexverschiebung

$$\sum_{k=0}^{n} a_k = \sum_{k=1}^{n+1} a_{k-1}$$

Schubfachprinzip

Satz 6.11

Es seien n Elemente auf m (paarweise disjunkte) Mengen verteilt und es gelte $n > m$.
Dann gibt es mindestens eine Menge, die mindestens zwei Elemente enthält.

Beweis.

Wenn jede der m Mengen höchstens ein Element enthalten würde, dann gäbe es insgesamt höchstens m Elemente. Widerspruch zu $n > m$.

Andere Bezeichnungen für das Schubfachprinzip: Taubenschlagprinzip, engl.: pigeonhole principle

Anwendungen des Schubfachprinzips

Beispiel 6.12

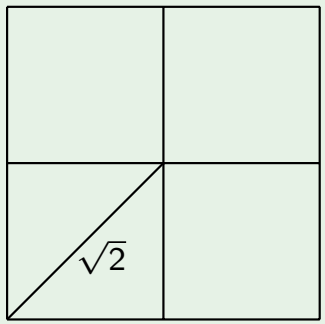
(i) Prof. B. hat in seiner Sockenkiste weiße, schwarze und grüne Socken.

Wenn er vier Socken aus der Kiste nimmt, hat er mindestens zwei Socken mit der gleichen Farbe.

$n = 4$ Elemente verteilt auf $m = 3$ Mengen.

(ii) Unter je fünf Punkten, die in einem Quadrat der Seitenlänge 2 liegen, gibt es stets zwei, die einen Abstand $\leq \sqrt{2}$ haben.

- Wir unterteilen das Quadrat durch halbieren der Seitenlänge in vier Unterquadrate mit Seitenlänge 1.
- $n = 5$ Punkte verteilen sich auf $m = 4$ Unterquadrate.
- Dann muss mindestens ein Unterquadrat zwei Punkte enthalten.



Bijektionsprinzip

Satz 6.13

Seien A und B endliche Mengen.
Dann gilt $|A| = |B|$ genau dann, wenn eine bijektive Funktion $f : A \to B$ existiert.

Beweis.

„$\Rightarrow$“: Es gelte $|A| = |B| =: n$.
Sei $A = \{a_1, \ldots, a_n\}$ und $B = \{b_1, \ldots, b_n\}$. Dann ist $f : A \to B$ definiert durch

$$f(a_i) = b_i$$

eine bijektive Abbildung.

Fortsetzung Beweis.

„$\Leftarrow$“: Sei $f : A \to B$ eine bijektive Abbildung.
Annahme: $|A| \neq |B|$. Dann muss entweder $|B| < |A|$ oder $|B| > |A|$ gelten.

1. Sei $|B| < |A|$.
   Mit dem Schubfachprinzip folgt, dass es a_i und a_j mit $i \neq j$ und $f(a_i) = f(a_j)$ geben muss.
   Widerspruch zur Injektivität von f.
2. Sei $|B| > |A|$.
   Da f bijektiv ist, muss auch $f^{-1} : B \to A$ bijektiv sein (siehe Folgerung 5.44).
   Mit dem Schubfachprinzip folgt, dass es b_i und b_j mit $i \neq j$ und $f^{-1}(b_i) = f^{-1}(b_j)$ geben muss.
   Widerspruch zur Injektivität von f^{-1}.

Also ist die Annahme falsch. Damit folgt $|A| = |B|$.

Anwendungen des Bijektionsprinzips

Aus Satz 5.4 wissen wir, dass eine n-elementige Menge 2^n verschiedene Teilmengen hat. Hier ein anderer Beweis mit dem Bijektionsprinzip.

Beispiel 6.14

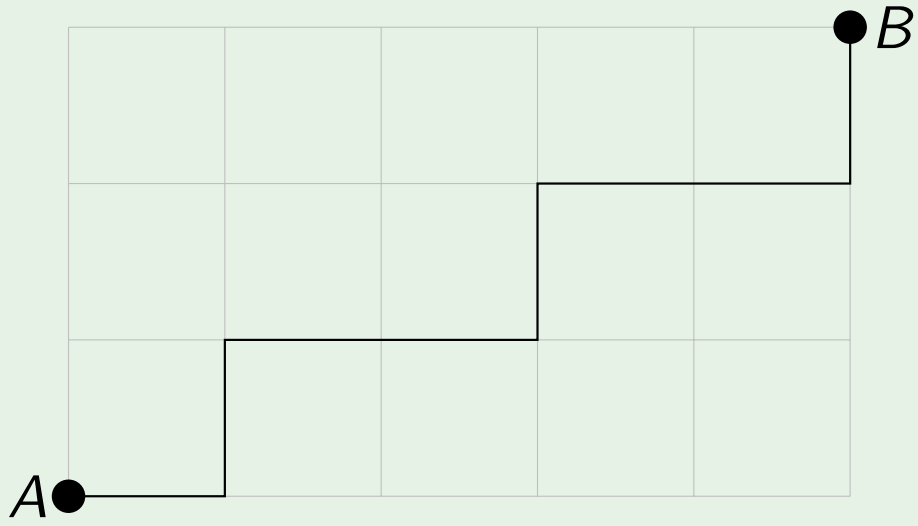
- Sei $A = \{a_1, \ldots, a_n\}$ eine n-elementige Menge.
- Sei $\mathcal{S} = \{s_1 \cdots s_n | s_i \in \{0, 1\}\}$ die Menge der Bitstrings der Länge n.
- Wir konstruieren eine bijektive Abbildung $f : \mathcal{P}(A) \to \mathcal{S}$ wie folgt: Für $B \subseteq A$ ist $f(B) = s_1 \cdots s_n$ mit

$$s_i = \begin{cases} 1 & \text{falls } a_i \in B \\ 0 & \text{sonst} \end{cases}$$

- Es gibt 2^n verschiedene Bitstrings der Länge n.
- Mit dem Bijektionsprinzip folgt, dass es auch 2^n verschiedene Teilmengen einer n-elementigen Menge geben muss.

Beispiel 6.15

- Gegeben sei ein Gitter der Breite m und der Höhe n.
- Wie viele verschiedene Wege gibt es von links unten (A) nach rechts oben (B), wenn man in einem Schritt nur nach rechts und oben gehen darf?



- Beispiel für $m = 5$ und $n = 3$:
- Lösung: $\binom{n+m}{n}$
- Beweis durch Konstruktion einer Bijektion zwischen den verschiedenen Wegen und den n-elementigen Teilmengen einer $n + m$-elementigen Menge.

Prinzip des doppelten Abzählens

- Wir stellen eine Relation $R \subseteq A \times B$ mithilfe einer boolschen Matrix dar (siehe Folie 138).
- Dann bilden wir die Summe der Zeilensummen und die Summe der Spaltensummen.
- Die beiden Summen müssen identisch sein.
- Durch Gleichsetzung der Summen erhalten wir eine Formel, die wir zur Berechnung einer fraglichen Anzahl nutzen können.

Beispiel 6.16

Dekan H. setzt fest, dass jeder Student genau 4 der 7 angebotenen Vorlesungen hören muss. Die Dozenten melden 45, 36, 30, 20, 25, 12 und 16 Zuhörer. Wie viele Studenten gibt es?

- Sei $S = \{s_1, \ldots, s_n\}$ die Menge der Studenten.
- Sei $V = \{v_1, \ldots, v_7\}$ die Menge der Vorlesungen.
- Es gelte $(s, v) \in R \subseteq S \times V$ genau dann, wenn Student s Vorlesung v hört.

	v_1	v_2	v_3	v_4	v_5	v_6	v_7	Σ
s_1	0	1	1	1	0	1	0	4
s_2	1	1	0	1	1	0	0	4
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
s_n	0	1	0	1	1	0	1	4
Σ	45	36	30	20	25	12	16	$= 4n$

- Also $n = \dfrac{\sum_{v \in V} \text{Zuhörer in } v}{4}$, hier $n = 46$.

Gleichmächtige Mengen

Definition 6.17

- Zwei Mengen A und B heißen gleichmächtig genau dann, wenn eine bijektive Funktion $f : A \to B$ existiert.
- Sind die Mengen A und B gleichmächtig, dann schreiben wir dafür auch $|A| = |B|$.
- Wir notieren $|A| \leq |B|$ und nennen A höchstens gleichmächtig zu B genau dann, wenn es eine injektive Abbildung $f : A \to B$ gibt,
- und wir notieren $|A| < |B|$ und nennen B mächtiger als A genau dann, wenn $|A| \leq |B|$ und $|A| \neq |B|$ gelten.

Diskussion

- Eine Folgerung aus dem Bijektionsprinzip ist, dass endliche Mengen genau dann gleichmächtig sind, wenn sie die gleiche Anzahl an Elementen haben (siehe Satz 6.13).
- Somit verallgemeinert Definition 6.17 den Vergleich von Mengenkardinalitäten auf nicht endliche Mengen.
- Aus $|A| = \infty$ und $|B| = \infty$ können wir nicht $|A| = |B|$ schließen.
- In der Definition von mächtiger ist ganz wesentlich, dass dort $|A| \neq |B|$ steht, und nicht $A \neq B$.
- Anders ausgedrückt: A ist mächtiger als B bedeutet, dass es zwar eine injektive Abbildung $f : A \to B$ gibt, aber keine bijektive.

Beispiel 6.18

(i) Obwohl $\mathbb{N}_0$ ein Element mehr als $\mathbb{N}$ enthält, gilt

$$|\mathbb{N}| = |\mathbb{N}_0|,$$

denn $f : \mathbb{N}_0 \to \mathbb{N}$ mit

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

ist eine bijektive Abbildung.

(ii) Es gilt sogar $|\mathbb{G}_+| = |\mathbb{N}_0|$, denn $f : \mathbb{N}_0 \to \mathbb{G}_+$ mit

$$f(n) = 2n$$

ist bijektiv.

Fortsetzung Beispiel.

(iii) Ebenso gilt $|\mathbb{Z}| = |\mathbb{N}_0|$. Die Funktion $f : \mathbb{Z} \to \mathbb{N}_0$ mit

$$f(z) = \begin{cases} 0 & \text{falls } z = 0 \\ 2z & \text{falls } z > 0 \\ -(2z+1) & \text{falls } z < 0 \end{cases}$$

ist bijektiv.

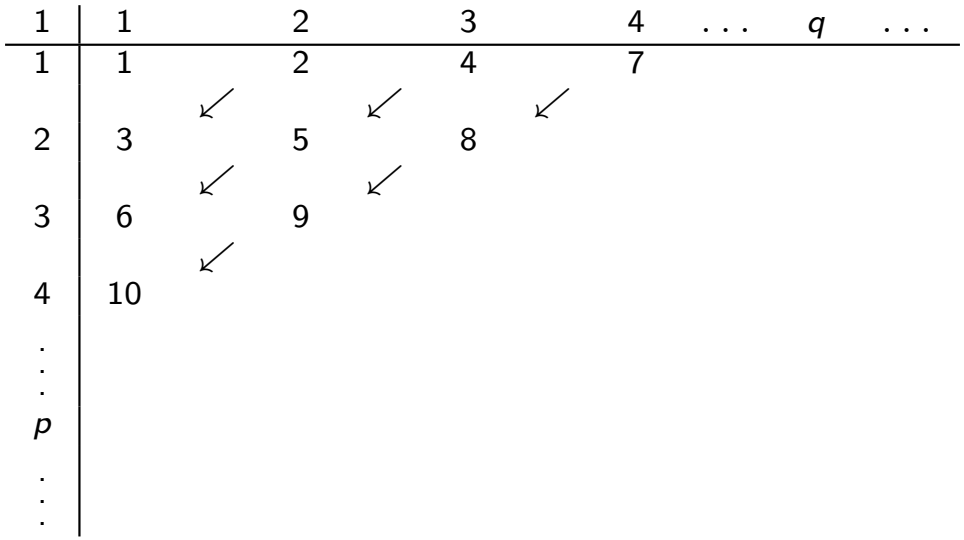
Cantorsche Tupelfunktion

Satz 6.19

Es gilt:

$$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|.$$

Anschauliche Begründung:



Beweis.

Wir konstruieren eine bijektive Funktion $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Sei $(i, j) \in \mathbb{N} \times \mathbb{N}$. Welche Nummer bekommt (i, j)?

- (i, j) liegt in der $i + j - 1$-ten Diagonale.
- Wie viele Paare sind in den Diagonalen $1, \ldots, i + j - 1$? Antwort:

$$\sum_{k=1}^{i+j-1} k = \frac{(i + j - 1)(i + j)}{2}$$

- Damit erhält das Paar $(i + j - 1, 1)$ die Nummer $\frac{(i+j-1)(i+j)}{2}$.
- Für größere Werte von j in der gleichen Diagonalen verringert sich diese Nummer entsprechend.
- Also erhält (i, j) die Nummer

$$f(i, j) = \frac{(i + j - 1)(i + j)}{2} - (j - 1).$$

Definition 6.20

Es sei f die Funktion aus dem Beweis von Satz 6.19.

Die Funktion

$$c_2 : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$$

mit

$$c_2(i,j) = f(i,j+2) = \frac{(i+j+1)(i+j+2)}{2} - (j+1)$$

heißt Cantorsche Paarungsfunktion.

- Die Cantorsche Paarungsfunktion definiert eine bijektive Abbildung.
- Auf Basis von c_2 können wir allgemein bijektive Abbildungen $c_k : \mathbb{N}_0^k \to \mathbb{N}_0$ für $k \geq 3$ wie folgt definieren:

$$c_k(i_1, \ldots, i_{k-1}, i_k) = c_2(c_{k-1}(i_1, \ldots, i_{k-1}), i_k)$$

Folgerung 6.21

Es gilt:

$$|\mathbb{Q}| = |\mathbb{N}|$$

Abzählbarkeit

Definition 6.22

Eine Menge M heißt abzählbar genau dann, wenn M endlich ist oder wenn $|M| = |\mathbb{N}_0|$ gilt.

Eine nicht abzählbare Menge heißt überabzählbar.

Folgerung 6.23

(i) *Jede Teilmenge einer abzählbaren Menge ist abzählbar.*

(ii) *Jede Obermenge einer nicht abzählbaren Menge ist nicht abzählbar.*

Beispiele für abzählbare Mengen

Beispiel 6.24

(i) $\mathbb{Z}$ ist abzählbar.

(ii) $\mathbb{Q}$ ist abzählbar.

(iii) $\mathbb{N}^k$ ist für alle $k \in \mathbb{N}$ abzählbar.

(iv) Sei X eine endliche Menge. Dann ist die Menge der Funktionen $f : X \to X$ endlich und damit abzählbar.

Wie viele solche Funktionen gibt es? $|X|^{|X|}$

(v) Ist auch die Menge $\mathbb{N}^{\mathbb{N}}$ der Funktionen $f : \mathbb{N} \to \mathbb{N}$ abzählbar?

Diagonalisierung

Satz 6.25

Die Menge $\mathbb{N}^{\mathbb{N}}$ der Funktionen $f : \mathbb{N} \to \mathbb{N}$ ist überabzählbar.

Beweis.

Annahme: Die Menge $\mathbb{N}^{\mathbb{N}}$ ist abzählbar.

- Also gibt es eine bijektive Abbildung $g : \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$, die $\mathbb{N}^{\mathbb{N}}$ abzählt.
- Sei $\phi_1, \phi_2, \phi_3, \ldots$ die durch g festgelegte Abzählung von $\mathbb{N}^{\mathbb{N}}$.
- Jetzt betrachten wir folgende Matrix:

	1	2	3	$\cdots$	j	$\cdots$
ϕ_1	$\phi_1(1)$	$\phi_1(2)$	$\phi_1(3)$	$\cdots$	$\phi_1(j)$	$\cdots$
ϕ_2	$\phi_2(1)$	$\phi_2(2)$	$\phi_2(3)$	$\cdots$	$\phi_2(j)$	$\cdots$
ϕ_3	$\phi_3(1)$	$\phi_3(2)$	$\phi_3(3)$	$\cdots$	$\phi_3(j)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	
ϕ_i	$\phi_i(1)$	$\phi_i(2)$	$\phi_i(3)$	$\cdots$	$\phi_i(j)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	

Fortsetzung Beweis.

- Wir definieren mithilfe der Diagonalen dieser Matrix die Funktion $\phi_D : \mathbb{N} \to \mathbb{N}$ wie folgt:

$$\phi_D(k) = \phi_k(k) + 1$$

- Jetzt muss $\phi_D \in \mathbb{N}^{\mathbb{N}}$ gelten.
- Also existiert ein s mit $\phi_D = \phi_s$.
- Daraus folgt:

$$\phi_s(s) = \phi_D(s) = \phi_s(s) + 1$$

Widerspruch!

Das Beweisprinzip, welches wir hier verwendet haben, heißt Diagonalisierung.

Konsequenz: $\mathbb{R}$ ist überabzählbar

- Schon die Menge $\{0, \ldots, 9\}^{\mathbb{N}}$ der Funktionen

$$f : \mathbb{N} \to \{0, 1, \ldots, 9\}$$

ist überabzählbar.

- Ein Beweis hierfür erfolgt analog zum Beweis von Satz 6.25 mit

$$\phi_D(k) = (\phi_k(k) + 1) \bmod 10$$

- Analog beweist man auch, dass die Menge $\{0, 1\}^{\mathbb{N}}$ der Funktionen

$$f : \mathbb{N} \to \{0, 1\}$$

überabzählbar ist.

- Die Menge $\{0, \ldots, 9\}^{\mathbb{N}}$ entspricht (bijektiv) aber der Menge $[0, 1] = \{x \in \mathbb{R} | 0 \leq x \leq 1\}$.

- Begründung: Jede Zahl $x \in [0,1]$ können wir als

$$x = 0, z_1 z_2 \ldots$$

  mit einer unendlichen Ziffernfolge $z_1, z_2, \ldots$ betrachten.
- Beachten Sie dabei: $0,999\ldots = 1$.
- Eine Ziffernfolge entspricht somit eineindeutig einer Abbildung $f : \mathbb{N} \to \{0,1,\ldots,9\}$.
- Da die Menge $\{0,\ldots,9\}^{\mathbb{N}}$ überabzählbar ist, muss somit auch die Menge $[0,1]$ überabzählbar sein und
- damit ist auch $\mathbb{R}$ überabzählbar (siehe Folgerung 6.23).

Folgerung 6.26

$\mathbb{R}$ ist mächtiger als $\mathbb{N}$.

Abschlusseigenschaften abzählbarer Mengen

Satz 6.27

(i) *Es seien A und B abzählbare Mengen, dann sind auch $A \cap B$, $A \setminus B$ und $A \cup B$ abzählbar.*

(ii) *Es sei I eine unendliche, abzählbare Indexmenge und die Mengen $A_i, i \in I$ seien alle abzählbar. Dann ist auch $\bigcup_{i \in I} A_i$ abzählbar.*

Beweis.

(i) Die Abzählbarkeit von $A \cap B$ und $A \setminus B$ folgt aus 6.23.

Da A, B abzählbar sind, existieren bijektive Funktionen $f : A \to \mathbb{N}$ und $g : B \to \mathbb{N}$. Damit ist die Funktion $h : A \cup B \to \mathbb{Z}$ mit

$$h(x) = \begin{cases} f(x) & \text{falls } x \in A \\ -g(x) & \text{falls } x \in B \setminus A \end{cases}$$

injektiv, also $|A \cup B| \leq |\mathbb{Z}| = |\mathbb{N}|$.

Fortsetzung Beweis.

(ii)

- O.B.d.A. seien die Mengen A_i paarweise disjunkt.
- Da die Indexmenge I abzählbar ist, können wir auch $\mathbb{N}$ als Indexmenge nehmen.
- Wir betrachten also $\bigcup_{i=1}^{\infty} A_i$.
- Jede Menge A_i ist abzählbar, also $A_i = \{a_{i1}, a_{i2}, \ldots\}$.
- Für eine Abzählung nutzen wir die Matrix wie bei der Cantorschen Tupelfunktion:

1	1		2		3		4	...	q	...
A_1	a_{11}	↙	a_{12}	↙	a_{13}	↙	a_{14}			
A_2	a_{21}	↙	a_{22}	↙	a_{23}					
A_3	a_{31}	↙	a_{32}							
A_4	a_{41}									
⋮										

- Damit liefert uns die Cantorsche Paarungsfunktion eine Abzählung der a_{ij}.

Zusammenfassung

- Wichtige kombinatorische Elemente: Fakultät, Permutation, Binomialkoeffizient, Binomischer Lehrsatz
- Prinzipien zum Abzählen endlicher Mengen: Schubfachprinzip, Bijektionsprinzip, Prinzip des doppelten Abzählens
- Gleichmächtige Mengen sind bijektiv aufeinander abbildbar.
- Unendliche abzählbare Mengen sind gleichmächtig zu $\mathbb{N}$.
- $\mathbb{N} \times \mathbb{N}$ und $\mathbb{Q}$ sind abzählbar.
- $\mathbb{R}$ ist überabzählbar.
- Abzählbare Mengen sind abgeschlossen bzgl. $\cap$, $\cup$ und $\setminus$.