Universität Trier

Fachbereich IV - Informatik

Christoph Meinel:

Diskrete Strukturen und Logik

Vorlesungsskript WS 1999/00

Inhaltsverzeichnis

I Grundlagen **3**

1 Grundbegriffe der Aussagen- und Prädikatenlogik **4**
1.1 Aussagen und Aussageformen 4
1.2 Verknüpfung von Aussagen 5
1.3 Tautologien und Kontradiktionen 9
1.4 Prädikate und Quantoren 12

2 Mengen und Mengenoperationen **15**
2.1 Vereinigung und Durchschnitt von Mengen 22
2.2 Produkte von Mengen 26

3 Relationen **30**
3.1 Äquivalenzrelationen 35
3.2 Halbordnungsrelationen 43
3.3 Funktionen und Abbildungen 45

II Techniken **50**

4 Beweistechniken **51**
4.1 Theoreme 51
4.2 Beweismethoden 52
4.3 Theoreme und Quantoren 56
4.4 Abschließende Bemerkungen 57

5 Mathematische Induktion **59**
5.1 Einführung 59
5.2 Idee der mathematischen Induktion 59
5.3 Beispiele für Induktionsbeweise 60
5.4 Vollständige Mathematische Induktion 62

5.5 Rekursive Definitionen 62

6 Zählen **68**
6.1 Grundlegende Zählprinzipien 68
6.2 Inklusions–Exklusionsprinzip 70
6.3 Taubenschlagprinzip 70
6.4 Permutation und Kombination 72

7 Diskrete Wahrscheinlichkeit **78**

8 Rekursionsrelationen **86**

III Strukturen **92**

9 Boolesche Algebren **93**
9.1 Boolesche Funktionen und Ausdrücke 93
9.2 Boolesche Äquivalenzen 94
9.3 Boolesche Algebren 97

10 Aussagenlogik **103**
10.1 Äquivalenz und Normalformen 110
10.2 Resolution 119

11 Graphen **126**
11.1 Wegprobleme in Graphen 126
11.2 Allgemeines Wegproblem 129
11.3 Transitiver Abschluß 131
11.4 Kürzeste und kostengünstigste Wege 132
11.5 Wegprobleme und Matrizenmultiplikation 133

Teil I

Grundlagen

Kapitel 1

Grundbegriffe der Aussagen- und Prädikatenlogik

– Bedeutung und Ziel der mathematischen Logik

1.1 Aussagen und Aussageformen

Definition:
Eine Aussage ist ein Satz, der entweder w(ahr) oder f(alsch) ist.

Beispiele:

(1) "11 ist Primzahl." w

(2) "$\sqrt{2}$ ist rational." f

(3) "Zu keinem $n > 2$ existieren drei natürliche Zahlen x, y, z mit $x^n + y^n = z^n$ (Fermatsche Vermutung)" w
[1]

(4) "Dieser Satz ist falsch." keine Aussage
(Russelsches Paradoxon)

Definition:
Eine Aussageform ist ein Satz mit wenigstens einer Leerstelle oder Variablen, der durch Einsetzen in die Leerstelle bzw. für die Variablen zu einer Aussage wird.

Bezeichnung:
X sei die Gesamtheit der Objekte x, die in Aussageform eingesetzt werden können.

[1] 1995 wurde die Vermutung von Wiles bewiesen

$A(X)$ Aussageform über X.

Beispiele:

(1) "x ist durch 3 teilbar."
Für jedes $x \in \mathbb{Z}$ ergibt sich eine Aussage

(2) "$(x+y)^2 = x^2 + 2xy + y^2$"
ergibt für alle $x, y \in \mathbb{R}$ wahre Aussage

Bemerkung:
Wir können aus der Aussageform auch Aussagen gewinnen, durch Konstruktionen wie "Für alle x, ..." oder "Es existiert x, ..." $\longrightarrow$ Quantifizierung (wird später behandelt)

1.2 Verknüpfung von Aussagen

Wir können aus einfachen Aussagen kompliziertere aufbauen:
Seien p, q Aussagen

Negation: "nicht p"

Ist eine Aussage, die genau dann wahr ist, wenn p falsch ist.

Symbol: $\sim p$ (oder $\neg p$, $\overline{p}$)

Wahrheitstabelle:

p	$\neg p$
w	f
f	w

Beispiel:

- "11 ist keine Primzahl"
  gleichbedeutend: "Es gilt nicht, daß 11 eine Primzahl ist"

Konjunktion: "p und q"
Ist eine Aussage, die genau dann wahr ist, wenn sowohl p als auch q wahr sind.

Symbol: $p \wedge q$ (oder $p \cdot q$, pq)

Wahrheitstafel:

p	q	$p \wedge q$
w	w	w
w	f	f
f	w	f
f	f	f

Beispiel:

- "11 ist eine Primzahl und durch 3 teilbar."

Bemerkung:
Wir können durch $\wedge$ mehrere Aussagen verknüpfen.

Beispiel:

- $(p \wedge q) \wedge s, \quad p \wedge (q \wedge s)$.

Lemma 1.1

$\wedge$ ist assoziativ, dh.
$(p \wedge q) \wedge s$ hat stets gleichen Wahrheitswert wie $p \wedge (q \wedge s)$.

Beweis:
Betrachte Wahrheitstafeln:

p	q	s	$(p \wedge q)$	$(p \wedge q) \wedge s)$	$(q \wedge s)$	$p \wedge (q \wedge s)$
f	f	f	f	f	f	f
f	f	w	f	f	f	f
f	w	f	f	f	f	f
f	w	w	f	f	w	f
w	f	f	f	f	f	f
w	f	w	f	f	f	f
w	w	f	w	f	f	f
w	w	w	w	w	w	w

□

Definition: "p oder q"
Ist eine Aussage, die genau dann falsch ist, wenn sowohl p als auch q falsch sind.

Symbol: $p \vee q$ (oder $p + q$)

Wahrheitstafel:

p	q	$p \vee q$
w	w	w
w	f	w
f	w	w
f	f	f

Achtung: "oder" bedeutet also kein "entweder oder"

Beispiel:

- "11 ist eine Primzahl oder durch 3 teilbar."

Wir können durch $\vee$ mehrere Aussagen verknüpfen.
Beispiele:

(1) $(p \vee q) \vee s$

(2) $p \vee (q \vee s)$.

Lemma 1.2
$\vee$ ist assoziativ, dh. $(p \vee q) \vee s$ hat stets gleichen Wahrheitswert wie $p \vee (q \vee s)$.

Beweis: ÜA □
Bemerkung: Wir können $\neg, \wedge, \vee$ kombiniert anwenden.
Beispiele:

- $(a \wedge b) \wedge c, (\neg(a \vee c)) \wedge (b \vee c), \ldots$

Lemma 1.3

(1) $\neg(a \wedge b)$ und $(\neg a) \vee (\neg b)$ haben stets den gleichen Wahrheitswert.

(2) $(a \wedge b) \vee c$ and $(a \vee c) \wedge (b \vee c)$ haben stets den gleichen Wahrheitswert.

Beweis:
z.B. (1):

a	b	$a \wedge b$	$\neg(a \wedge b)$	$\neg a$	$\neg b$	$(\neg a) \vee (\neg b)$
w	w	w	f	f	f	f
w	f	f	w	f	w	w
f	w	f	w	w	f	w
f	f	f	w	w	w	w

□

Implikation: "aus p folgt q"
Ist eine Aussage, die genau dann falsch ist, wenn die Aussage p wahr und die Aussage q falsch ist.
Symbol: $p \Rightarrow q$

Wahrheitstafel:

p	q	$p \Rightarrow q$
w	w	w
w	f	f
f	w	w
f	f	w

Sprechweisen:
"p ist hinreichende Bedingung für q."
"q ist notwendige Bedingung für p."
"p ist Prämisse oder Voraussetzung für q."
"q ist Konklusion oder Folgerung für p."

Beispiel:

- $A(x) \Rightarrow B(x)$
  Z.B. "x ist durch 4 teilbar", "x ist durch 2 teilbar."

Äquivalenz: "p genau dann, wenn q"
Ist eine Aussage, die genau dann wahr ist, wenn p und q die gleichen Wahrheitswerte haben.
Symbol: $p \Leftrightarrow q$

Wahrheitstafel:

p	q	$p \Leftrightarrow q$
w	w	w
w	f	f
f	w	f
f	f	w

Sprechweise: "p und q sind logisch äquivalent."

Lemma 1.4
$(p \Rightarrow q) \wedge (q \Rightarrow p)$ *und* $p \Leftrightarrow q$ *haben stets gleichen Wahrheitswert.*

Beweis: durch Vergleich der Wahrheitstafeln $\square$

Lemma 1.5

(1) Es gilt $p \Leftrightarrow p$ für alle p (reflexiv).

(2) Aus $p \Leftrightarrow q$ folgt $q \Leftrightarrow p$ (symmetrisch).

(3) Aus $p \Leftrightarrow q, q \Leftrightarrow r$ folgt $p \Leftrightarrow r$ (transitiv).

□

Bemerkung:
Wir können alle definierten Operationen anstelle von Aussagen auch auf Aussageverknüpfungen anwenden.

1.3 Tautologien und Kontradiktionen

Wir hätten Lemma 1.5 auch anders formulieren können:

Lemma 1.6
Die Aussage $((p \Rightarrow q) \vee (q \Rightarrow p)) \Leftrightarrow (p \Leftrightarrow q)$ ist stets wahr.

Definition:
Eine Aussageverbindung $a(p_1, \ldots, p_n)$ von n Aussagen $p_1, \ldots, p_n$ heißt Tautologie, wenn sie unabhängig vom Wahrheitswert der p_i stets wahr ist. Ist $a(p_1, \ldots, p_n)$ stets falsch, so heißt $a(p_1, \ldots, p_n)$ Kontradiktion.

Beispiele für Tautologien:

(1) $p \vee (\neg p)$ ("Prinzip vom ausgeschlossenen Dritten")

Beweis:

p	$\neg p$	$p \vee (\neg p)$
w	f	w
f	w	w

(2) $((p \Rightarrow q) \wedge (q \Rightarrow p)) \Leftrightarrow (p \Leftrightarrow q)$ (Lemma 1.6)

Beispiel für eine Kontradiktion:

(1) $p \wedge (\neg p)$ ("Prinzip vom ausgeschlossenen Widerspruch")

Lemma 1.7

Die folgenden Aussageverbindungen sind Tautologien:

(1) $(p \Rightarrow \neg p) \Rightarrow (\neg p)$

(2) $(p \wedge (p \Rightarrow q)) \Rightarrow q$

(3) $(p \wedge q) \Rightarrow p, (p \wedge q) \Rightarrow q$

(4) $p \Rightarrow (p \vee q), q \Rightarrow (p \vee q)$

(5) $(p \Rightarrow q) \Rightarrow [(q \Rightarrow r) \Rightarrow (p \Rightarrow r)]$

(6) $((p \Rightarrow q) \wedge (q \Rightarrow r)) \wedge p) \Rightarrow r$

Beweis: z.B. durch Wahrheitstafel, ... □

Definition:

Zwei Aussageverbindungen $a_1(p_1, \ldots p_n)$ und $a_2(p_1, \ldots, p_n)$ heißen logisch äquivalent wenn die Aussageverbindung $a_1(p_1, \ldots, p_n) \Leftrightarrow a_2(p_1, \ldots, p_n)$ eine Tautologie ist.

Bezeichnung:

$a_1 \equiv a_2$

Bemerkung:

$\equiv$ ist reflexiv, symmetrisch und transitiv.

Beweis:

$\Leftrightarrow$ hat entsprechende Eigenschaften. □

Lemma 1.8

Die folgenden Aussageverbindungen sind logisch äquivalent:

(1) $(p \wedge q) \equiv (q \wedge p), (p \vee q) \equiv (q \vee p)$ *(Kommutativgesetz)*

(2) $(p \wedge (q \wedge r)) \equiv ((p \wedge q) \vee r)$
$(p \vee (q \vee r)) \equiv ((p \vee q) \vee r)$
(Assoziativgesetz)

(3) $(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$
$(p \vee (q \wedge r)) = ((p \vee q) \wedge (p \vee r))$
(Distributivgesetz)

(4) $(p \Rightarrow q) \equiv (\neg p \vee q)$

(5) $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$ *(Kontraposition)*
$(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$

(6) $(p \Leftrightarrow q) \equiv ((p \wedge q) \vee (\neg p \wedge \neg q))$

(7) $\neg(p \wedge q) = \neg p \vee \neg q$
$\neg(p \vee q) = \neg p \wedge \neg q$
(de Morgansche Regeln)

(8) $((p \Rightarrow q) \wedge (r \Rightarrow q)) \equiv ((p \vee r) \Rightarrow q)$

(9) $(p \vee (q \wedge \neg q)) \equiv p$
$(p \wedge (q \vee \neg q)) \equiv p$

Beweis:

1. Methode:

Wir ersetzen $\equiv$ durch $\Leftrightarrow$ und beweisen mit Wahrheitstafel, daß entstehende Aussageverbindung eine Tautologie ist.

Z.B. (5): $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$

p	q	$p \Rightarrow q$	$\neg q \Rightarrow \neg p$	$((p \Rightarrow q) \Longleftrightarrow (\neg q \Rightarrow \neg p))$
w	w	w	w	w
w	f	f	f	w
f	w	w	w	w
f	f	w	w	w

2. Methode:

Unter Ausnutzung bekannter Tautologien wird die linke Seite der Äquivalenz in die rechte Seite überführt.

z.B. Beweis von (7) unter Kenntnis von (1), (2), (3), (4), (6) und (10)

$$\begin{aligned}(p \Leftrightarrow q) &\overset{(6)}{\equiv} ((p \Rightarrow q) \wedge (q \Rightarrow p)) \\ &\overset{(4)}{\equiv} ((\neg p \vee q) \wedge (\neg q \vee p)) \\ &\overset{(2)}{\equiv} ((\neg p \wedge \neg q) \vee (\neg p \wedge p) \vee (q \wedge \neg q) \vee (q \wedge p) \\ &\overset{(1,10)}{\equiv} ((p \wedge q) \vee (\neg p \wedge \neg q))\end{aligned}$$

Wegen Transitivität von $\equiv$ gilt also

$$(p \Leftrightarrow q) \equiv ((p \wedge q) \vee (\neg p \wedge \neg q))$$

□

Abtrennungsregel (Modus ponens)

Ist p wahre Aussage und ist $p \Rightarrow q$ wahr, so ist auch q wahr.
Symbolisch:

$$\begin{array}{l} p \\ p \Rightarrow q \\ \hline \hookrightarrow q \end{array}$$

Allgemein gilt:

$$
\begin{array}{l}
p_0 \\
p_0 \Rightarrow p_1 \\
p_1 \Rightarrow p_2 \\
p_2 \Rightarrow p_3 \\
\vdots \\
p_{n-1} \Rightarrow p_n \\
\hline
\hookrightarrow p_n
\end{array}
$$

abkürzende Schreibweise anstelle von

$$p \Rightarrow p_1, p_1 \Rightarrow p_2, \cdots, p_{n-1} \Rightarrow p_n \quad \text{kurz} \quad p \Rightarrow p_1 \Rightarrow p_1 \Rightarrow \cdots \Rightarrow p_n$$

analog für

$$p \Leftrightarrow p_1, p_2 \Leftrightarrow p_2, \cdots, p_{n-1} \Leftrightarrow p_n \quad \text{kurz} \quad p \Leftrightarrow p_1 \Leftrightarrow p_2 \Leftrightarrow \cdots \Leftrightarrow p_n$$

1.4 Prädikate und Quantoren

Wir hatten Aussageformen wie

$$x > 3$$
$$x = y + 3$$
$$\vdots$$

betrachtet.

Aussageformen $P(x)$ sind weder wahr noch falsch, wenn die Variable x nicht spezifiziert wird. Man kann P als aussagelogische Funktion von x auffassen:

Sei $P(x) :=$ "$x > 3$", dann ist $P(4)$ wahr und $P(2)$ ist falsch.

Für alle x ergibt sich ein Wahrheitswert.

Man kann auch auf andere Weise aus einer Aussageform $P(x)$ Aussagen gewinnen:

a) Universelle Quantifizierung macht aus $P(x)$ die Aussage: "$P(x)$ ist wahr für alle x (des betrachteten Universums)".

Bezeichnung: $\forall x P x$

Beispiele:

(1) Sei $P(x) :=$ "$x+1 > x$", für $x \in \mathbb{R}$. $\forall x P(x)$ bedeutet "für alle $x \in \mathbb{R}$ gilt $x+1 > x$"
Dies ist eine wahre Aussage.

(2) $Q(x) :=$ "$x < 2$" für $x \in \mathbb{N}$. $\forall x Q(x)$ bedeutet "für alle $x \in \mathbb{N}$ gilt $x < 2$".
Dies ist eine falsche Aussage.

(3) $Q(x) :=$ "$x < 2$", für $x \in \mathbb{N}^-$. $\forall x Q(x)$ bedeutet "für alle $x \in \mathbb{N}^-$ gilt $x < 2$".
Dies ist eine wahre Aussage.

Ist das Universum endlich $\{x_1 \ldots x_t\}$, dann gilt:

$$\forall x P(x) \equiv P(x_1) \wedge \ldots \wedge P(x_t)$$

b) Existentielle Quantifizierung macht aus $P(x)$ die Aussage:

"Es existiert ein Element x (des Universums), für das $P(x)$ eine wahre Aussage ist."

Bezeichnung: $\exists x P(x)$

Beispiele:

(1) Sei $P(x)$: "$x + 1 > x$", für $x \in \mathbb{N}$.
$\exists x P(x)$ bedeutet "es ex. ein $x \in \mathbb{N}$, so daß $x + 1 > x$ gilt".
Dies ist eine wahre Aussage.

(2) Sei $Q(x) =$ "$x < 2$", für $x \in \mathbb{N}$.
$\exists x Q(x)$ bedeutet "es ex. ein $x \in \mathbb{N}$, so daß $x < 2$ ".
Dies ist eine wahre Aussage (z.B. $x = 1 \in \mathbb{N}$).

Ist Universum endlich $\{x_1, \ldots x_t\}$, dann gilt

$$\exists x P(x) \equiv P(x_1) \vee P(x_2) \vee \ldots \vee P(x_t).$$

Beispiel:

- $P(x) :=$ "$x^2 > 10$" , $x \in \{1, 2, 3, 4\}$
$\exists x P(x) \equiv$ "$1 > 10$" $\vee$ "$4 > 10$" $\vee$ "$9 > 10$" $\vee$ "$16 > 10$"
Dies ist eine wahre Aussage.

Zusammenfassung:

Aussage	wahr	falsch
$\forall x P(x)$	$P(x)$ ist wahr für alle x	Es ex. x, für das $P(x)$ falsch ist
$\exists x P(x)$	Es ex. x, für das $P(x)$ wahr ist	$P(x)$ ist falsch für alle x

Quantifizierung von Aussageformen mit mehreren Variablen
Wir können in Aussageformen auch über einzelne Variablen quantifizieren ("gebundene Variablen"), die nicht quantifizierten Variablen heißen "freie Variablen".

Beispiel:

- $P(x, y) : x^2 + y = 0$

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

Zusammenfassung

Aussage	wahr	falsch
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ ist wahr für alle x und alle y	Es gibt ein (x_1, y_1), so daß $P(x_1, y_1)$ falsch ist
$\forall x \exists y P(x, y)$	Für jedes x gibt es ein y, so daß $P(x, y)$ wahr ist	Es gibt ein x, so daß für jedes y $P(x, y)$ falsch ist
$\exists x \forall y P(x, y)$	Es gibt ein x, so daß $P(x, y)$ für jedes y wahr ist	Für alle x gibt es ein y, so daß $P(x, y)$ falsch ist
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	Es gibt ein Paar (x, y), so daß $P(x, y)$ wahr ist	Für jedes Paar (x, y) ist $P(x, y)$ falsch

Negierte Quantoren
Wollen quantifizierte Aussageformen negieren:

$$\neg(\forall x P(x))$$
$$\neg(\exists x P(x))$$

Lemma 1.9
Es gilt

(1) $\neg(\forall x P(x) \equiv \exists x(\neg P(x))$

(2) $\neg(\exists x P(x)) \equiv \forall x(\neg P(x))$

Beweis:
Wahrheitswertetabelle. □

Kapitel 2

Mengen und Mengenoperationen

Mengen: Zusammenfassungen von verschiedenen Einzelobjekten zu einheitlichem Ganzen.
Beispiele:

Schulklasse, Familie, ..., alle ganzen Zahlen

Die Objekte x einer Menge M heißen Elemente der Menge M.

Bezeichnung:
$x \in M$ (Elementrelation) "x ist Element von M".
Schreiben anstelle von $\neg(x \in M)$ kurz $x \notin M$ ("x ist kein Element von M").
Mengen mit endlich vielen Objekten heißen endliche Mengen, Mengen mit unendlich vielen Objekten heißen unendliche Mengen.

Gleichheit von Mengen

Definition:
M_1 und M_2 sind gleich (Bez. $M_1 = M_2$), wenn jedes Element von M_1 auch Element von M_2 und umgekehrt jedes Element von M_2 auch Element von M_1 ist.
Schreiben anstelle von $\neg(M_1 = M_2)$ kurz $M_1 \neq M_2$. damit sind Mengen durch ihre Elemente eindeutig bestimmt, ist M endlich, so kann M notiert werden durch Auflistung aller Elemente von M in beliebiger Reihenfolge.

$$M = \{x_1, x_2, \ldots, x_n\}$$

Beispiele:

(1) $\{a, b, c, d\} = \{c, b, d, a\} = \ldots$

(2) $\{1, 2, 2, 1\} = \{1, 2\}$

Sei M Menge und $E(x)$ Aussageformen über M. Es gibt eine Menge N, die die Elemente von M umfaßt, für die $E(x)$ eine wahre Aussage liefert.
Beispiel:

- $E(x) =$ "x ist durch 2 teilbar."

  $N =$ Menge aller geraden Zahlen.

  N ist durch M und $E(x)$ eindeutig bestimmt.

Bezeichnung:
$N = \{x \in M | E(x)\}$
"N ist Menge aller x aus M, für die $E(x)$ wahr ist."

Sprachlich verschiedene Aussageformen können die gleiche Menge N in M definieren:
Beispiel:

- $\{1, 2\}$ in $\mathbb{N}$ kann definiert werden als

$$\{x \in \mathbb{N} | x^2 - 3x + 2 = 0\}$$

oder

$$\{x \in \mathbb{N} | 0 < x \leq 2\}$$

da

$$(x^2 - 3x + 2 = 0) \Leftrightarrow (0 < x \leq 2)$$

Tatsächlich gilt:
Zwei über einer Menge M definierte Aussageformen $E_1(x), E_2(x)$ definieren genau dann die gleiche Menge N in M, wenn für jedes $x \in M$ gilt

$$E_1(x) \Leftrightarrow E_2(x).$$

Komplementäre Mengen:

Sei $N = \{x \in M | E(x)\}$.
Mit $E(x)$ ist auch $\neg E(x)$ Aussageform über Menge M; damit existiert eine eindeutig bestimmte Menge $\overline{N}$ die durch $\neg E(x)$ in M definiert wird.

$$\overline{N} = \{x \in M | \neg E(x)\}$$

Da $E(x)$ für jedes $x \in M$ entweder wahr oder falsch ist, gehört jedes Element von M entweder zu N oder zu $\overline{N}$ aber nie gemeinsam zu N und $\overline{N}$

Wegen $E(x) \equiv \neg(\neg E(x))$ gilt

$$\overline{(\overline{N})} = \{x \in M | \neg(\neg E(x))\} = \{x \in M | E(x)\} = N$$

Definition:
Sei M Menge, $E(x)$ Aussageform über M, dann heißen die Mengen

$$N = \{x \in M | E(x)\} \text{ und } \overline{N} = \{x \in M | \neg E(x)\}$$

in M komplementäre Mengen; $\overline{N}$ ist die Komplementärmenge von N in M und umgekehrt.

Beispiele:

(1) Menge der ungeraden Zahlen in $\mathbb{N}$ ist komplementär zur Menge der geraden Zahlen.

(2) Menge der Primzahlen in $\mathbb{N}^+ = \{x \in \mathbb{N} | x > 0\}$ ist komplementär zur Menge der zusammengesetzten Zahlen.

Leere Menge:

Betrachten für $E(x)$ eine Aussage über M, die für jedes $x \in M$ wahr ist, z.B. "$x = x$"

Dann gilt

$$\{x \in M | E(x)\} = M$$

also

$$\overline{M} = \{x \in M | \neg E(x)\} = \{x \in M) | x \neq x\}$$

$\overline{M}$ enthält kein Element. Trotzdem ist $\overline{M}$ eine Menge. $\overline{M}$ heißt leere Mengen.

Bezeichnung: $\emptyset_M$
$\emptyset_M$ ist abhängig von M, aber nur scheinbar:

Behauptung:
Für beliebige zwei Mengen M_1, M_2 gilt $\emptyset_{M_1} = \emptyset_{M_2}$, d.h. jedes Element von $\emptyset_{M_1}$ ist Element von $\emptyset_{M_2}$ und umgekehrt.

Beweis:
Sei $a \in M_1$ beliebig, dann ist Aussage "$a \in \emptyset_{M_1}$" falsch. Dann ist die Implikation "$a \in \emptyset_{M_1} \Rightarrow a \in \emptyset_{M_2}$" wahr.

Umgekehrt, sei $b \in M_2$ beliebig, dann ist Aussage "$b \in \emptyset_{M_2}$" falsch, also "$b \in \emptyset_{M_2} \Rightarrow b \in \emptyset_{M_1}$" wahr.

Insgesamt: $\emptyset_{M_1} = \emptyset_{M_2}$

Es gibt also nur eine leere Menge. □

Bezeichnung: $\emptyset$

Meistens umfaßt Menge $N = \{x \in M | E(x)\}$ nicht alle Elemente von M.

Teilmengen, Obermengen:

Definition:
Seien M und N Mengen. N heißt Teilmenge von M bzw. M heißt Obermenge von N, wenn jedes Element von N auch Element von M ist.

Bezeichnung:

$$N \subseteq M, M \supseteq N$$

Gilt speziell ($N \subseteq M$) und ($N \neq M$), dann heißt N echte Teilmenge von M bzw. M echte Obermenge von N.

Bezeichnung:

$$N \subset M, M \supset N$$

Bemerkung:
Schreiben $N \subset M$ nur, wenn explizit ausgedrückt werden soll, daß $N \neq M$ gilt.

Ist N Teilmenge von M, so läßt sich (bis auf logische Äquivalenz) eindeutig eine Aussageform $E(x)$ über M angeben, so daß gilt

$$N = \{x \in M | E(x)\}.$$

Wir können z.B. $E(x) =$ "$x \in N$" wählen.

Beispiele:

(1) für alle Aussageformen $E(x)$ über M gilt $N = \{x \in M | E(x)\} \subseteq M$
Damit gilt z.B. $\emptyset \subseteq M$, $M \subseteq M$.

(2) $\{a, b, c\} \subseteq \{a, b, c, d\}$

(3) $\mathbb{N} \leq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

(4) Seien $E_1(x), E_2(x)$ Aussageform über M. Gelte für jedes $x \in M$: ist $E_1(x)$ wahr, so ist auch $E_2(x)$ wahr. Dann gilt für $N_1 = \{x \in M | E_1(x)\}$ und $N_2 = \{x \in M | E_2(x)\}$ die Beziehung

$$N_1 \subseteq N_2.$$

("$E_2(x)$ ist notwendige Bedingung für $E_1(x)$", "$E_1(x)$ ist hinreichende Bedingung für $E_2(x)$".)

Ist $E(x)$ eine definierte Eigenschaft einer Teilmenge von M und sind $E_1(x)$ eine hinreichende, $E_2(x)$ eine notwendige Bedingung für $E(x)$, dann gilt

$$\{x \in M | E_1(x)\} \subseteq \{x \in M | E(x)\} \subseteq \{x \in M | E_2(x)\}.$$

Satz 2.1
Für beliebige Mengen M_1, M_2 gilt:

$$M_1 = M_2 \Leftrightarrow [(M_1 \subseteq M_2) \wedge (M_2 \subseteq M_1)].$$

Beweis:
($\Rightarrow$) ist $M_1 = M_2$, so ist jedes Element von M_1 in M_2, also $\Rightarrow M_1 \subseteq M_2$;
ebenso ist jedes Element von M_2 in M_1, also $\Rightarrow M_2 \subseteq M_1$.
($\Rightarrow$) gilt $M_1 \subseteq M_2$ und $M_2 \subseteq M_1$ gleichzeitig, so ist jedes Element von M_1 in M_2 und umgekehrt, jedes Element von M_2 in M_1 , $\Rightarrow M_1 = M_2$. □

Potenzmengen:

Zu jeder Menge M gibt es eine weitere Menge, die genau die Teilmengen von M als Elemente enthält.

Bezeichnung: $P(M), \mathcal{P}(M), 2^M$ "Potenzmenge von M"
Es gilt:

$$P(M) = \{N | N \subseteq M\}.$$

Es gilt stets

$$M \in P(M) \text{ und } \emptyset \in P(M).$$

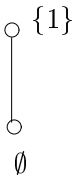
Ist M endlich, dann kann $P(M)$ in einem Diagramm aus Punkten und Linien dargestellt werden. Punkte stehen für die Teilmengen von M.

Teilmengen mit gleich vielen Elementen stehen auf gleichen Höhen; Teilmengen mit größerer Elementzahl stehen über Teilmengen mit niedrigerer Elementzahl; zwei Teilmengen N_1, N_2 werden durch Linien verbunden, wenn $N_1 \subset N_2$ gilt, aber kein N_3 existiert mit $N_1 \subset N_3$ und $N_3 \subset N_2$

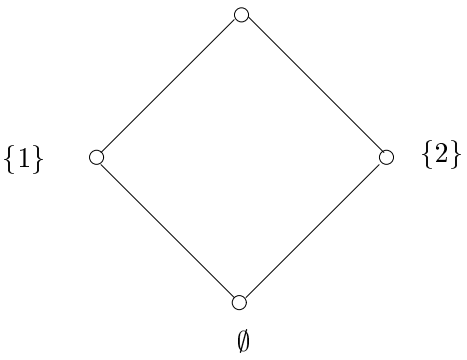
Beispiele:

$P(\emptyset)$:

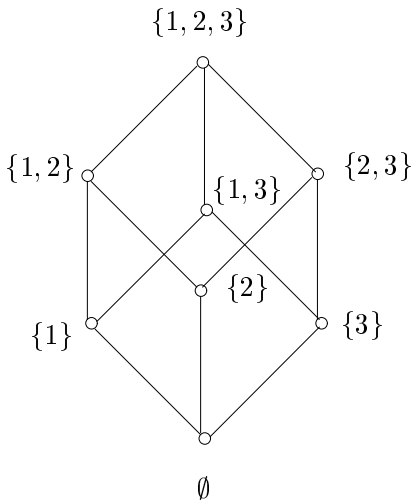
$P(\{1\})$:



$P(\{1,2\})$:



$P(\{1,2,3\})$:



$P(M)$ ist Menge, können also $P(P(M)), P(P(\ldots(P(M)\ldots)$ bilden:

$$P^m(M) = \underbrace{P(P(\ldots P}_{m \text{ mal}}(M)\ldots).$$

Besitzt M genau n Elemente, dann gilt

$$P(M) \text{ hat } \sum_{i=0}^{n} \binom{n}{i} = 2^n \text{ Elemente}$$

$$P^m(M) \text{ hat } \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2^n}}}}}}_{m \text{ Zweien}} \text{ viele Elemente.}$$

Wir können in Potenzmenge $P(M)$ Intervalle betrachten:

Sei $A, B \in P(M)$. Wir definieren:

$$(A,B) := \{X \in P(M) | A \subset X \subset B\}$$

$$\langle A,B) := \{X \in P(M) | A \subseteq X \subset B\}$$
$$(A,B\rangle := \{X \in P(M) | A \subset X \subseteq B\}$$
$$\langle A,B\rangle := \{X \in P(M) | A \subseteq X \subseteq B\}.$$

2.1 Vereinigung und Durchschnitt von Mengen

Führen nun "Mengenalgebra" ein, betrachte zunächst die Mengenoperation Vereinigung und Durchschnitt:

Wir können $\{1,2,3\}$ und $\{3,4,5\}$ die Mengen $\{1,2,3,4,5\}$ und $\{3\}$ zuordnen, die aus allen Elementen beider Mengen bzw. aus den gemeinsamen Elementen beider Mengen bestehen.

Definition:
Seien M_1, M_2 Mengen. Die Gesamtheit aller Elemente, die zu M_1 oder M_2 gehören, bildet wieder eine Menge M, die als Vereinigung von M_1 und M_2 bezeichnet wird.

Bezeichnung: $M = M_1 \cup M_2$
Es gilt: $M_1 \cup M_2 = \{x | x \in M_1 \vee x \in M_2\}$

Definition:
Seien M_1, M_2 Mengen. Die Gesamtheit aller Elemente, die sowohl zu M_1 als auch zu M_2 gehören bildet eine Menge M, die als Durchschnitt von M_1 und M_2 bezeichnet wird.

Bezeichnung: $M = M_1 \cap M_2$
Es gilt: $M_1 \cap M_2 = \{x | x \in M_1 \wedge x \in M_2\}$
Es gilt: $M_1 \cap M_2 = \{x \in M_1 \,|\, x \in M_2\} = \{x \in M_2 \,|\, x \in M_1\}$

$\Rightarrow M_1 \cap M_2 \subseteq M_1, M_1 \cap M_2 \subseteq M_2$

Beispiele:

(1) $\{a,b\} \cup \{a,b\} = \{a,b\}$

(2) $\mathbb{N}^- \cup \mathbb{N}^+ = \mathbb{N}$

(3) $\{x \in \mathbb{C} | x^2 + 1 = 0\} \cup \{x \in \mathbb{C} | x^2 - 1 = 0\} = \{x \in \mathbb{C} | x^4 - 1 = 0\}$

(4) Sei $A, B \in P(M)$, $(A,B) \cup \{A,B\} = \langle A,B \rangle$

(5) $\langle A,B) \cap (A,B\rangle = (A,B)$

(6) $\{(x,y) \in \mathbb{R}^2 | x^2 + y^2 = 4\} \cap \{(x,y) \in R^2 = 3x + 2\} = \{(0,2), (-\frac{6}{5}, -\frac{8}{5})\}$

Satz 2.2
Für beliebige Mengen M_1, M_2 gilt:

(1) $M_1 \cap M_2 \subseteq M_1 \subseteq M_1 \cup M_2$

(2) $M_1 \cap M_2 \subseteq M_2 \subseteq M_2 \cup M_2$.

Beweis:

(1) Sei $x \in M_1 \cap M_2$.

$\Rightarrow x \in M_1 \wedge x \in M_2 \qquad ((p \wedge q) \Rightarrow p)$

$\Rightarrow x \in M_1$

$\Rightarrow x \in M_1 \vee x \in M_2 \qquad (p \Rightarrow (p \vee q))$

$\Rightarrow x \in M_1 \cup M_2$.

(2) Analog.

□

Satz 2.3

Für jede Menge M gilt

$$M \cup M = M, M \cap M = M.$$

Beweis:

$x \in M \cup M \Longleftrightarrow x \in M \vee x \in M \Longleftrightarrow x \in M \qquad (p \vee p \equiv p)$

$x \in M \cap M \Longleftrightarrow x \in M \wedge x \in M \Longleftrightarrow x \in M \qquad (p \wedge p \equiv p)$ □

Satz 2.4

Für beliebige Mengen M_1, M_2 gilt:

(1) $M_1 \cup M_2 = M_2 \cup M_1$

(2) $M_1 \cap M_2 = M_2 \cap M_1$.

Beweis:

Z.B. (1):

$x \in M_1 \cup M_2 \Longleftrightarrow x \in M_1 \vee x \in M_2$

$\Longleftrightarrow x \in M_2 \vee x \in M_1$

$\Longleftrightarrow x \in M_2 \cup M_1$

(2) analog □

Satz 2.5

Für beliebige Mengen M_1, M_2, M_3 gilt

(1) $(M_1 \cup M_2) \cup M_3 = M_1 \cup (M_2 \cup M_3)$

(2) $(M_1 \cap M_2) \cap M_3 = M_1 \cap (M_2 \cap M_3)$.

Beweis: Analog zu Satz 2.4 □

Satz 2.6

Für beliebige Mengen M_1, M_2, M_3 gilt:

(1) $(M_1 \cup M_2) \cap M_3 = (M_1 \cap M_3) \cup (M_2 \cap M_3)$

(2) $(M_1 \cap M_2) \cup M_3 = (M_1 \cup M_3) \cap (M_2 \cup M_3)$.

Beweis:
Übungsaufgabe. □

Satz 2.7

Für beliebige Mengen M_1, M_2 gilt:

(1) $M_1 \cup (M_1 \cap M_2) = M_1$

(2) $M_1 \cap (M_1 \cup M_2) = M_1$.

Beweis: Es gilt $p \vee (p \wedge q) \equiv p$ und $p \wedge (p \vee q) \equiv p$. □
Wir können damit folgenden Satz beweisen.

Satz 2.8

Für beliebige Mengen M_1, M_2 gilt:

(1) $M_1 \subseteq M_2 \iff M_1 \cup M_2 = M_2$

(2) $M_1 \subseteq M_2 \iff M_1 \cap M_2 = M_1$.

Beweis:
(1) ($\Longrightarrow$)
Sei $M_1 \subseteq M_2$, d.h. es gelte $x \in M_1 \Rightarrow x \in M_2$.
Das ist logisch äquivalent zu

$$(\neg(x \in M_1) \vee (x \in M_2)).$$

Wegen $p \wedge p \equiv p$ und $(p \wedge q) \vee p \equiv p$ gilt:

$$(x \in (M_1 \cup M_2) \wedge (x \in M_1 \Longrightarrow x \in M_2)).$$

$\Longrightarrow (x \in M_1 \vee x \in M_2) \wedge (\neg(x \in M_1) \vee x \in M_2)$
$\Longrightarrow (x \in M_1 \wedge \neg(x \in M_1)) \vee (x \in M_1 \wedge x \in M_2) \vee (x \in M_2 \wedge \neg(x \in M_1)) \vee (x \in M_2 \wedge x \in M_2)$
$\Longrightarrow (x \in M_1 \wedge x \in M_2) \vee (x \in M_2 \wedge \neg(x \in M_1)) \vee x \in M_2$
$\Longrightarrow (x \in M_1 \wedge x \in M_2) \vee x \in M_2$.
$\Longrightarrow x \in M_2$.
Also ist $M_1 \cup M_2 \subseteq M_2$.
Wegen $M_2 \subseteq M_1 \cup M_2$, gilt $M_2 = M_1 \cup M_2$.
($\Longleftarrow$)
Sei $M_1 \cup M_2 = M_2$, dann gilt $x \in M_1 \vee x \in M_2 \Rightarrow x \in M_2$, also $x \in M_1 \Longrightarrow x \in M_2$, d.h. $M_1 \subseteq M_2$.
(2) analog. □

Definition:
Sei M Menge, $P(M)$ Potenzmenge, $T \subseteq P(M)$.
Die Menge

$$\bigcup_{N \in T} N = \{x \in M | \text{ es ex. } N \in T \text{ mit } x \in N\}$$

heißt Vereinigung aller Teilmengen N von M, die in T enthalten sind. Die Menge

$$\bigcap_{N \in T} N = \{x \in M | \text{ für alle } N \in T \text{ gilt } x \in N\}$$

heißt Durchschnitt aller Teilmengen N von M, die in T enthalten sind.

Beispiele:

(1) $M = \mathbb{N}^+$

(1a) $T = \{\{1,2,3\},\{3,4,5\},\{5,6,7\},\{7,8,9\}\}$

$$\bigcup_{N \in T} N = \{1,2,3,4,5,6,7,8,9\}, \bigcap_{N \in T} N = \emptyset$$

(1b) $T = \{\{1,2,3,4\},\{3,4,5,6\}\}$

$$\bigcup_{N \in T} N = \{1,2,3,4,5,6\}, \bigcap_{N \in T} N = \{3,4\}$$

(2) $M = \mathbb{N}$

$T = \{M_1, M_2, M_3, \ldots\}$ mit $M_i = \{x \in \mathbb{N} | 2^i \text{ teilt } x\}$

$$\bigcup_{N \in T} N = M, \bigcap_{N \in T} N = \{0\}$$

2.2 Produkte von Mengen

Die Produktmenge der Menge M_1 und M_2 soll aus geordneten Paaren (x, y) von Element $x \in M_1$ und $y \in M_2$ bestehen.

Achtung:
geordnetes Paar: zwei Elemente in bestimmter Reihenfolge
Zweiermenge: zwei Elemente in beliebiger Reihenfolge

Für Paare soll gelten:

$$(a,b) = (c,d) :\Longleftrightarrow a = c \wedge b = d.$$

Für Mengen gilt:

$$\{a,b\} = \{c,d\} \Longleftrightarrow (a = c \wedge b = d) \vee \ (a = d \wedge b = c).$$

Brauchen wir neuen Begriff?
$\{a, b\}$ ungeeignet zur Definition wegen $\{a, b\} = \{b, a\}$
$\{\{a\}, \{b\}\}$ ungeeignet wegen $\{\{a\}, \{b\}\} = \{\{b\}, \{a\}\}$
aber
$\{\{a\}, \{a, b\}\}$ ist geeignet!

Satz 2.9
Die Mengen $M_1 = \{\{a\}, \{a, b\}\}$ *und* $M_2 = \{\{c\}, \{c, d\}\}$ *sind gleich genau dann, wenn* $a = c$ *und* $b = d$.

Beweis:
($\Longleftarrow$): Aus $M_1 = M_2$ folgt nach Definition der Mengengleichheit
$(*)$ $\{a\} = \{c\}$ und $\{a, b\} = \{c, d\}$
oder
$(**)$ $\{a\} = \{c, d\}$ und $\{c\} = \{a, b\}$.
Gilt (*), dann folgt wegen $a = c$ auch $b = d$.
Gilt (**), dann ist $a = c = d$ bzw. $c = a = b$,
also $a = b = c = d$.
($\Longleftarrow$): Sei $a = c$ und $b = d$.
Dann folgt $\{a\} = \{c\}, \{b\} = \{d\}$ und $\{a, b\} = \{c, d\}$.
Folglich $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. □

Definition:
Eine Menge der Gestalt $\{\{a\}, \{a, b\}\}$ heißt geordnetes Paar.

Bezeichnung:
$(a, b) := \{\{a\}, \{ab\}\}$

Wir können Begriff des geordneten Paares rekursiv verallgemeinern zum geordneten n-Tupel $(n > 1)$:
$(a_1, \ldots, a_n) := \{\{(a_1, \ldots, a_{n-1})\}, \{(a_1, \ldots, a_{n-1}), a_n\}\}$.

Beispiel:

- Wir kennen geordnete Paare und n-Tupel aus der Geometrie:

  Punkte der Ebene $\stackrel{\wedge}{=}$ geordnete Paare
  Punkte des 3-dimensionalen Raumes $\stackrel{\wedge}{=}$ 3-Tupel

  Verfahren:
  Wir legen in jeder Dimension Maßstab fest (Einheit).
  Die $i$te Komponente des n-Tupels gibt die Entfernung (Vielfaches der Einheit)

der Punkte vom Ursprung des n-dimensionalen Euklidischen Raumes in der i-ten Dimension an.

$E^n = \{(x_1 \dots x_n) | x_1, \dots, x_n \in I\!R\}$

Definition:
Seien M_1, M_2 zwei Mengen

$M_1 \times M_2$ ist die Menge aller geordneten Paare (x_1, x_2) , wobei $x_1 \in M_1$ und $x_2 \in M_2$ gilt.

$M_1 \times M_2 := \{(x_1, x_2) | x_1 \in M_1 \wedge x_2 \in M_2\}$

Allgemein gilt:
$M_1 \times \dots \times M_n := \{(x_1, \dots, x_n) | x_1 \in M_1 \wedge \dots \wedge x_n \in M_n\}$

Offensichtlich gilt nach Definition:

$$M_1 \times \dots \times M_n = (M_1 \times \dots \times M_{n-1}) \times M_n.$$

Bezeichnung:
(1) Gilt $M_1 = \dots = M_n$ so wird M_1^n anstelle von $M_1 \times \dots \times M_1$ geschrieben ;
(2) $M \times \emptyset = \emptyset$ und $\emptyset \times M = \emptyset$

Beispiel:

- $M_1 = \{a, b\}, M_2 = \{\alpha, \beta, \gamma\}$
  $M_1 \times M_2 = \{(a.\alpha), (a, \beta), (a, \gamma), (b, \alpha), (b, \beta), (b, \gamma)\}$

Produkt- und Vereinigungsbildung sind wie folgt verknüpft:

Satz 2.10
Für beliebige M_1, M_2, M_3 gilt

$$M_1 \times (M_2 \cup M_3) = (M_1 \times M_2) \cup (M_1 \times M_3).$$

Beweis:
$(x, y) \in M_1 \times (M_2 \cup M_3)$
$\iff x \in M_1 \wedge (y \in M_2 \vee y \in M_3)$
$\iff (x \in M_1 \wedge y \in M_2) \vee (x \in M_1 \wedge y \in M_3)$
$\iff (x, y) \in M_1 \times M_2 \vee (x, y) \in M_1 \times M_3$
$\iff (x, y) \in M_1 \times M_2 \cup M_1 \times M_3$ □

Analog gilt:

Satz 2.11
Für beliebige M_1, M_2, M_3 gilt:

$$M_1 \times (M_2 \cap M_3) = (M_1 \times M_2) \cap (M_1 \times M_3).$$

□

Kapitel 3

Relationen

Teilmengen von Produktmengen haben in Mathematik und Informatik große Bedeutung.

Definition:
Seien $M_1, \dots M_n$ Mengen.
Eine n-stellige Relation zwischen den Mengen $M_1, \dots M_n$ ist eine Teilmenge R der Produktmenge $M_1 \times \dots \times M_n$,

$$R \subseteq M_1 \times \dots \times M_n$$

Bezeichnung:

(1) Gilt $M_1 = \dots = M_n = M$ so heißt R eine n-stellige Relation über M.

(2) Schreiben anstelle von $(x_1, \dots, x_n) \in R$ oft

$$R(x_1, \dots x_n)$$

(3) Gilt $n = 2$ so heißt R binäre Relation über M. Wir schreiben anstelle $(x_1, x_2) \in R$ oft $x_1 R x_2$.

Können Relationen durch Aussageformen beschreiben oder als Aussageform auffassen:

$$R \subseteq M^n \Longleftrightarrow E_R(x)$$

wobei $E_R(x)$ Aussageform über M^n ist mit

$$x \in R \Longleftrightarrow E(x).$$

Beispiele:

(1) $M_1 = M_2 = M_3 = \mathbb{R}$

$$R = \{(a, b, c) \in \mathbb{R}^3 | (a \leq b) \wedge (b \leq c)\}$$

"Zwischenrelation": "b liegt zwischen a und c."

(2) M_1 sei die Menge aller Geraden g und M_2 die Menge aller Ebenen e im euklidischen Raum.

$R = \{(g,e)|(g,e) \in M_1 \times M_2, g \text{ parallel zu } e\}$

"Parallelitätsrelation"

Schreiben anstelle von "gRe" kurz "$g \| e$.

(3) $M_1 = M_2 = \mathbb{Z} - \{0\}$,
$R = \{(a,b) \in \mathbb{Z} - \{0\} | a \text{ teilt } b\}$

"Teilbarkeitsrelation"

Bezeichnung: $a|b$

(4) $M_1 = M_2 = \mathbb{R}$

$R = \{(a,b) \in \mathbb{R}^2 | a \text{ kleiner als } b\}$

"Größenordnungsrelation"

Bezeichnung: $a < b$.

Betrachten im folgenden nur binäre Relationen.

Spezielle Relationen:

Betrachten Relationen über Menge M.

Nullrelation: $R = \emptyset$

Allrelation: $R = M \times M$

Gleichheitsrelation: $R = \Delta_M = \{(x,x)|x \in M\}$
(heißt auch "Diagonale in $M \times M$" oder "Identitätsrelation" id_M).

Mengenoperationen und Relationen:

R, S seien Relationen über M.

$R \subseteq S$:
$\iff (xRy \implies xSy \text{ für alle } x,y \in M)$

$R \cup S$:
$x(R \cup S)y :\iff (x,y) \in R \cup S$
$\iff (x,y) \in R \vee (x,y) \in S$
$\iff xRy \vee xSy \text{ für alle } x,y \in M$

$R \cap S$:
$x(R \cap S)y :\iff (x,y) \in R \cap S$

$\iff (x,y) \in R \wedge (x,y) \in S$
$\iff xRy \wedge xSy$ für alle $x, y \in M$

Definition:
(1) Sei R Relation zwischen M_1 und M_2, und sei S Relation zwischen M_2 und M_3.
Das Produkt von R und $S, R \circ S$, ist eine Relation zwischen M_1 und M_3, die wie folgt definiert ist:
für beliebige $x \in M_1$ und $z \in M_3$ gelte
$x(R \circ S)z \iff$ es existiert $y \in M_2$ mit xRy und ySz
(2) Ist R Relation zwischen M und M' und ist S Relation zwischen N und N', so ist die Relation $R \otimes S$ definiert als:
für beliebige $(x,y) \in M \times N$ gelte
$(x,y)(R \otimes S)(x',y') \iff xRx'$ und ySy'

Beispiele:

(1) In der Menge aller Dreiecke der euklidischen Ebene ist die Kongruenzrelation $\cong$ enthalten in der Ähnlichkeitsrelation $\sim$.

(2) Seien R und S auf $\mathbb{N}^+$ definiert wie folgt:

$$R = \{(x,y) \in (\mathbb{N}^+)^2 \mid x \neq y \wedge x|y\}$$

$$S = \{(x,y) \in (\mathbb{N}^+)^2 \mid 2|\,(x+y)\}$$

Dann ist:
$R \cup S = \{(x,y) \in (\mathbb{N}^+)^2 \mid x$ echter Teiler von y oder x und y haben gleiche Parität$\}$,
$R \cap S = \{(x,y) \in (\mathbb{N}^+)^2 \mid x$ echter Teiler von y und x und y haben gleiche Parität$\}$,
$R \circ S = \{x, y \in (\mathbb{N}^+)^2 \mid x$ ungerade oder y gerade $\}$.

Definition:
Seien M_1, M_2 Mengen, R Relation zwischen M_1 und M_2.
$\mathrm{Def}(R) = \{x \in M_1 |$ es existiert $y \in M_2$ mit $(x,y) \in R\}$ heißt <u>Definitionsbereich</u> oder <u>Vorbereich</u> von R
$W(R) = \{y \in M_2 |$ es existiert $x \in M_1$ mit $(x,y) \in R\}$, heißt <u>Wertebereich</u> oder <u>Nachbereich</u> von R.

Beispiel:

- Sei $M_1 = \{1,2,3\}, M_2 = \{a,b\}$ und $R = \{(1,a),(1,b),(3,b)\}$.
  Dann ist $\mathrm{Def}(R) = \{1,3\}$, $W(R) = \{a,b\}$.

Definition:
Seien M_1, M_2 Mengen und R Relation zwischen M_1 und M_2.
Die Relation zwischen M_2 und M_1

$$\{(y,x) \in M_2 \times M_1 | (x,y) \in R\}$$

heißt die zu R inverse bzw. duale Relation.

Bezeichnung: R^{-1}
Beispiel:

- Sei $R = \{(x,y) \in I\!R^2 | x \geq 0 \wedge y = x^2\}$. Dann ist

$$R^{-1} = \{(x,y) \in I\!R^2 | y \geq 0 \wedge y = \sqrt{x}\}.$$

Satz 3.1
Sei M eine Menge und R, S, T Relationen auf M. Dann gilt:

(1) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$,

(2) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$,

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

(4) $(R \cap S) \circ T \subseteq R \circ T \cap S \circ T$,

(5) $T \circ (R \cap S) \subseteq T \circ R \cap T \circ S$,

(6) $(R \cup S) \circ T = R \circ T \cup S \circ T$,

(7) $T \circ (R \cup S) = T \circ R \cup T \circ S$.

Beweis:

(1) $x(R \cup S)^{-1} y \iff y(R \cup S)x$
$\iff yRx \vee ySx$
$\iff xR^{-1}y \vee xS^{-1}y \iff x(R^{-1} \cup S^{-1})y$

(2) analog

(3) $x(R \circ S)^{-1} y \iff y(R \circ S)x$
$\iff (\exists z) : z \in M \wedge yRz \wedge zSx$
$\iff (\exists z) : z \in M : xS^{-1}z \wedge zR^{-1}y$
$\iff x(S^{-1} \circ R^{-1})y$

(4) $x((R \cap S) \circ T)y \implies (\exists z) : z \in M \wedge x(R \cap S)z \wedge zTy$
$\implies (\exists z) : z \in M \wedge xRz \wedge xSz \wedge zTy$
$\implies (\exists z) : z \in M \wedge (xRz \wedge zTy) \wedge (xSz \wedge zTy)$
$\implies x(R \circ T)y \wedge x(S \circ T)y$
$\implies x((R \circ T) \cap (S \circ T))y$

Rest analog. □

Übungsaufgabe:
Gib Beispiele, warum in (4), (5) nicht = stehen kann.

Definition:
Sei M Menge, R Relation auf M.
R heißt:
reflexiv, falls xRx für alle $x \in M$,
symmetrisch, falls $xRy \Longrightarrow yRx$ für alle $x, y \in M$,
antisymmetrisch, falls $xRy \wedge yRx \Longrightarrow x = y$ für alle $x, y \in M$,
transitiv, falls $xRy \wedge yRz \Longrightarrow xRz$ für alle $x, y, z \in M$,
nacheindeutig, falls $xRy \wedge xRy' \Longrightarrow y = y'$ für beliebige $x, y, y' \in M$.

Beispiele:

(1) $R = \{(1,2),(2,3),(1,3)\} \subseteq \mathbb{N}^2$
ist nicht reflexiv.
nicht symmetrisch.
nicht antisymmetrisch.
transitiv.
nicht nacheindeutig.

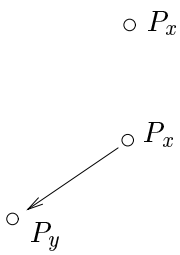
(2) $R = \{(x,y) \in R^2 : x^2 + y^2 = 1\}$
ist nicht reflexiv.
symmetrisch.
nicht antisymmetrisch.
nicht transitiv.
nicht nacheindeutig.

(3) $R_m = \{(a,b) \in Z^2 \mid m \mid (a-b)\}$
ist reflexiv.
symmetrisch.
transitiv : $m|(a-b) \wedge m|(b-c) \Longrightarrow m|(a-c)$

(4) $T = \{(a,b) \in (\mathbb{N}^+)^2 \mid a|b\}$
ist reflexiv.
antisymmetrisch.
transitiv.

(5) $R = \{(x,y) \in \mathbb{R}^2 | y = 3x\}$
ist nacheindeutig.

Wir können Relation R über endlichen Mengen M graphisch darstellen:
$x \in M$ entspricht Punkt und xRy entspricht gerichteter Kante .



Diese Darstellung von R heißt "Relationsgraph" oder Hasse-Diagramm.

Satz 3.2
Sei R Relation über M.

(1) R ist reflexiv genau dann wenn $\triangle_M \subseteq R$,

(2) R ist symmetrisch genau dann wenn $R^{-1} \subseteq R$ (d.h. $R^{-1} = R$),

(3) R ist transitiv genau dann wenn $R \circ R \subseteq R$,

(4) R ist antisymmetrisch genau dann wenn $R \cap R^{-1} \subseteq \triangle_M$.

Beweis:
zu (1) $(\longrightarrow)$ Sei R reflexiv
$\Longrightarrow xRx$ für alle $x \in M$
$\Longrightarrow (x,x) \in R$ für alle $x \in M$
$\Longrightarrow \triangle_M = \{(x,x) | x \in M\} \subseteq R$
$(\longleftarrow)$ Sei $\triangle_M = \{(x,x) | x \in M\} \subseteq R$
$\Longrightarrow xRx$ für alle $x \in M$
d.h. R ist reflexiv.

(2) – (4) analog. □

3.1 Äquivalenzrelationen

In der Mathematik und der Informatik tritt folgender Typ von Relationen sehr häufig auf:

Definition:
Eine binäre Relation R über M heißt Äquivalenzrelation $=_{\text{def}}$ R ist reflexiv, symmetrisch und transitiv.

Bezeichnung:
Anstelle von xRy wird oft $x \simeq y$ oder $x \sim y$ geschrieben.

Beispiele:

(1) Allrelation über M

(2) Gleichheitsrelation über M

(3) M Menge aller Waren W eines Ladens $W_1 \simeq W_2 :\Longleftrightarrow$ Preis $(W_1) =$ Preis (W_2)

(4) $R_m = \{(a,b) \in \mathbb{Z}^2 \mid m \mid (a-b)\}$

(5) Sei $x, y \in R$.
$x \sim y :\Longleftrightarrow x^2 = y^2$

(6) Sei $M = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}), (a,b), (c,d) \in M, (a,b) \sim (c,d) :\Longleftrightarrow ad = bc$. (Brüche!)

(7) $\mathcal{M}$ Menge aller endlichen Mengen.
$M_1 \sim M_2 :\Longleftrightarrow \#M_1 = \#M_2$ wobei $\#M$ die Anzahl der Elemente von M bezeichnet.

Definition:
Sei M eine nichtleere Menge.
Eine Zerlegung / Partition von M ist eine Teilmenge $Z \subseteq P(M)$ mit

(1) $\emptyset \notin Z$

(2) $M = \bigcup_{N \in Z} N$

(3) Gilt $N_1, N_2 \in Z$ und $N_1 \neq N_2$, so folgt $N_1 \bigcap N_2 = \emptyset$.

Bezeichnung:
Die Elemente N von Z heißen Klassen von M bei Zerlegung Z.
Eine Zerlegung wird auch Klasseneinteilung genannt.

Beispiel:

- $M = \{1, \ldots, 10\}$
  Zerlegung: $Z = \{\{1\}, \{2,3,5\}, \{4\}, \{6,7,8,9,10\}\}$
  keine Zerlegung: $Z = \{\{1,2,3\}, \{5,6\}\{3,10\}\}$

Es gibt einen fundamentalen Zusammenhang zwischen Äquivalenzrelation und Zerlegungen.

Satz 3.3

Sei M eine nichtleere Menge. Jede Äquivalenzrelation $\sim$ über M definiert eine Zerlegung Z von M und umgekehrt definiert jede Zerlegung Z von M eine Äquivalenzrelation über M.

Beweis: $(\longrightarrow)$
Sei $\sim$ Äquivalenzrelation über M.
Behauptung:
$Z = \{M_a = \{x \in M | x \sim a\} | a \in M\} \subseteq P(M)$ ist Zerlegung von M, dh.
(1) $M_a \neq \emptyset$ für alle $a \in M$
(2) Gilt $M_a \neq M_b$ so ist $M_a \cap M_b = \emptyset$
(3) $\bigcup_{a \in M_a} = M$

zu (1): $\sim$ ist reflexiv.
$\Longrightarrow a \sim a$ für alle $a \in M$
$\Longrightarrow a \in M_a$ für alle $a \in M$
$M_a \neq \emptyset$ für alle $a \in M$

zu (2): $M_a \neq M_b$

Annahme:
Es existiert $d \in M_a \bigcap M_b$

$\Rightarrow$ $d \sim a$ und $d \sim b$
$\overset{\text{sym.}}{\Rightarrow} \ldots$ $a \sim d$ und $d \sim b$
$\overset{\text{trans.}}{\Rightarrow} \ldots$ $a \sim d$ und $d \sim b$
$\Rightarrow$ $M_a = M_b$

zu (3):
Annahme:
Es existiert $d \in M$ mit $d \notin \bigcup_{a \in M} M_a$. Da $\sim$ reflexiv gilt $d \in M_d$. Widerspruch!

$(\longleftarrow)$
Sei Z Zerlegung von M und sei $M_x \in Z$ diejenige Menge mit $x \in M_x$. Wir definieren:
$a \sim b :\Longleftrightarrow M_a = M_b$ für alle $a, b \in M$.
Behauptung: $\sim$ ist Äquivalenzrelation, dh.
(1) $\sim$ ist reflexiv.
(2) $\sim$ ist symmetrisch.
(3) $\sim$ ist transitiv.

Zu (1):
$x \sim x$ wegen $M_x = M_x$ für jedes $x \in M$.

Zu (2):
$x \sim y$ impliziert $M_x = M_y$, also auch $y \sim x$ wegen Symmetrie von $=$.

Zu (3):
$x \sim y \wedge y \sim z$
$\Longrightarrow (M_x = M_y) \wedge (M_y = M_z)$
$\Longrightarrow M_x = M_z$

$\Longrightarrow x \sim z$

□

Bezeichnung:
M_x heißt Äquivalenzklasse von x bezüglich $\sim$ oder Äquivalenzklasse von x modulo $\sim$.

Bezeichnung:
"$[x]$" bzw. "x mod $\sim$", $[x]_\sim$, "$\overline{x}$"

Bemerkung: $[x] = [y] \Longleftrightarrow x \sim y$

Beispiele:
Äquivalenzklassen zu den Beispielen (1) bis (6) oben:

(1) Allrelation: $[x] = M$ für alle $x \in M$

(2) Gleichheitsrelation: $[x] = \{x\}$ für alle $x \in M$

(3) Preisrelation: $[W_i] = \{W \in M |\ \text{Preis}(W) = \text{Preis}(W_i)\}$
"Preisklassen von W_i"

- enthält alle Waren mit gleichem Preis wie W_i
- haben eine eindeutige Bezeichnung zwischen Preisklasse von W_i und Preis von W_i

(4) $R_m, m \in \mathbb{N}$

$$[a] = \{x \in \mathbb{Z} |\ \begin{array}{l} x \,|\, (x-a)\} \\ \Updownarrow \\ x \equiv a \text{mod } m \\ \Updownarrow \\ x = m \cdot q + a\,,\ q \in \mathbb{Z} \text{ beliebig} \end{array}$$

Division mit Rest ist in $\mathbb{Z}$ eindeutig ausführbar; für alle $a \in \mathbb{Z}$ und $m \in N$ existiert eindeutig bestimmte q, r mit $a = qm + r$ und $|r| < m$.

- Es gilt $[a] = [r]$
- Es gibt bei Division durch m genau m verschiedene Reste r :

$$0, 1, \ldots, m-1.$$

$\Longrightarrow$ es gibt genau m verschiedene Äquivalenzklasssen modulo m:

$$[0], [1], \ldots, [m-1]$$

Bezeichnung: "Restklassen modulo m"

Zuordnung $[a] \longleftrightarrow r$ mit $a \in \mathbb{Z}$ und $0 \leq r \leq m-1$

ist eineindeutig.

Zuordnung

$$a \longleftrightarrow r \text{ mit } a \in \mathbb{Z} \text{ und } 0 \leq r \leq m-1$$

ist eineindeutig.

(5) $x, y \in \mathbb{R}$, $x \sim y \Longleftrightarrow x^2 = y^2$

$$\begin{aligned}[2,5] &= \{r \in \mathbb{R} | r^2 = 6,25\} \\ &= \{2,5; -2,5\}\end{aligned}$$

(6) $(a,b) \sim (c,d) \Longleftrightarrow ad = bc$ (Brüche)

$[(3,5)] = \{(a,b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) : 5a = 3b\}$

Definition:
Sei $\sim$ Äquivalenzrelation in einer nichtleeren Menge M und Z sei die zugehörige Zerlegung. $Z \subseteq P(M)$ heißt Quotientenmenge oder Faktormenge von M modulo $\sim$.

Bezeichnung: $M/\sim$

Beispiel:

- $\mathbb{N}/R_m = \{[0], [1], \ldots, [m-1]\}$

Satz 3.4
Sind R und S Äquivalenzrelationen über M, so ist $R \bigcap S$ ebenfalls eine Äquivalenzrelation über M.

Beweis: $R \cap S$ ist
(1) reflexiv
(2) symmetrisch
(3) transitiv

Zu (1)
xRx und xSx impliziert $x(R \cap S)x$ für alle $x \in M$

Zu (2)
Sei $x(R \cap S)y$ für $x, y \in M$
$\Rightarrow xRy \wedge xSy$

$\Rightarrow yRx \wedge ySx$ da R, S Äquivalenzrelationen
$\Rightarrow y(R \cap S)x$

Zu (3)
Sei $x(R \cap S)y \wedge y(R \cap S)z$ für $x, y, z \in M$
$\Rightarrow (xRy \wedge xSy) \wedge (yRz \wedge ySz)$

$\wedge$ assoziativ, kommutativ
$\Rightarrow (xRy \wedge yRz) \wedge (xSy \wedge ySz)$

da R, S transitiv
$\Rightarrow xRz \wedge xSz$
$\Rightarrow x(R \cap S)z$ □

Satz 3.5

Seien R, S Äquivalenzrelationen über M.
$R \circ S$ ist Äquivalenzrelation über M genau dann, wenn $R \circ S = S \circ R$.

Beweis:
($\longrightarrow$) Sei $R \circ S$ Äquivalenzrelation in M. Wir benutzen die Sätze 3.1 und 3.2.

Es gilt
$\Rightarrow (R \circ S)^{-1} = R \circ S$. Andererseits ist $(R \circ S)^{-1} = S^{-1} \circ R^{-1} = S \circ R$ (da $S^{-1} = S$ und $R^{-1} = R$.
Also $S \circ R = R \circ S$.

($\longleftarrow$) Sei $R \circ S = S \circ R$.
Wegen $\Delta_M \subseteq R, \Delta_M \subseteq S$
folgt $\Delta_M = \Delta_M \circ \Delta_M \subseteq R \circ S$, das heißt $R \circ S$ ist reflexiv.
Wegen $(R \circ S)^{-1} = S^{-1} \circ R^{-1} = S \circ R = R \circ S$ ist $R \circ S$ symmetrisch.
Wegen $R \circ R \subseteq R, S \circ S \subseteq S$, gilt $(R \circ S) \circ (R \circ S) = R \circ (S \circ R) \circ S$
$= R \circ (R \circ S) \circ S$
$= (R \circ R) \circ (S \circ S)$
$\subseteq R \circ S$.
Das heißt $R \circ S$ ist transitiv. □

Satz 3.6

Seien R_1, R_2 Äquivalenzrelationen in M_1 bzw. M_2, dann ist $R_1 \otimes R_2$ eine Äquivalenzrelation in $M_1 \times M_2$.

Beweis:
(1)
Wegen $x_1 R_1 x_1$, $x_2 R_2 x_2$ für alle $x_1 \in M_2$, $x_2 \in M_2$ gilt $(x_1, x_2) R_1 \otimes R_2 (x_1, x_2)$ für alle $(x_1, x_2) \in M_1 \times M_2$

(2)
$(x_1, x_2) R_1 \otimes R_2 (y_1, y_2) \Rightarrow x_1 R_1 y_1$ und $x_2 R_2 y_2$
$\Rightarrow y_1 R_1 x_1$ und $y_2 R_2 x_2$
$\Rightarrow (y_1, y_2) R_1 \otimes R_2 (x_1, x_2)$

(3)
Sei $(x_1, x_2) R_1 \otimes R_2 (y_1, y_2) \wedge (y_1, y_2) R_1 \otimes R_2 (z_1, z_2)$
$\Rightarrow (x_1 R_1 y_1 \wedge y_1 R_1 z_1) \wedge (x_2 R_2 y_2 \wedge y_2 R_2 z_2)$
$\Rightarrow x_1 R_1 z_1 \wedge x_2 R_2 z_2$
$\Rightarrow (x_1, x_2) R_1 \otimes R_2 (z_1, z_2)$
für alle $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in M_1 \times M_2$. □

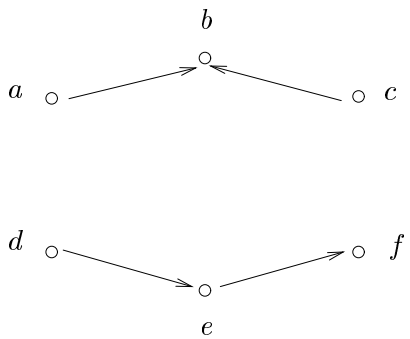
Wir zeigen nun, daß jede beliebige binäre Relation R auf einer nichtleeren Menge M eindeutig zu einer kleinsten, M umfassenden Äquivalenzrelation ausgebaut werden kann.

Beispiel:

$$M = \{a, b, c, d, e, f\}$$

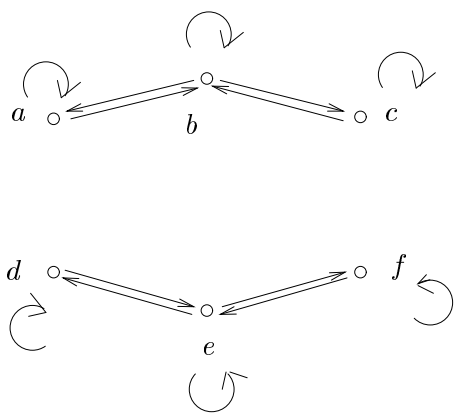
$$R = \{(a, b), (c, b), (d, e), (e, f)\}$$

Graphische Veranschaulichung:



R ist nicht reflexiv, symmetrisch oder transitiv.

Bauen R zu Äquivalenzrelation $\overline{R}$ aus:



Zu $\overline{R}$ gehörende Zerlegung z : $z = \{\{a, b, c\}, \{d, e, f\}\}$

Satz 3.7

Sei M eine nichtleere Menge und R eine beliebige binäre Relation auf M. Die nachfolgend definierte Relation $\overline{R}$ ist eine Äquivalenzrelation:
$x\overline{R}y :\Longleftrightarrow$ *es existieren in M endlich viele Elemente $x_1, \ldots, x_n$ mit*

$$x = x_1, y = x_n \text{ und}$$

$$x_1 = x_{i+1} \text{ oder } x_i R x_{i+1} \text{ oder } x_{i+1} R x_i.$$

Beweis:
(1) Wegen $x = x(x = x_1 = x_2 = x)$ gilt $x\overline{R}x$ für alle $x \in M$.
(2) $\overline{R}$ ist symmetrisch, da x_i und x_{i+1} vertauscht werden dürfen.
(3) Sei $x\overline{R}y$ und $y\overline{R}z$.
$\Rightarrow$ Es existieren Elemente $x_1, \ldots, x_n, y_1 \ldots y_m \in M$.
mit

$$x_1 = x, x_n = y = y_1, z = y_m$$

und

$$x_1 = x_{i+1} \text{ oder } x_i R x_{i+1} \text{ oder } x_{i+1} R x_i \text{ für } i = 1, \ldots, n$$

und

$$y_j = y_{j+1} \text{ oder } y_j R y_{j+1} \text{ oder } y_{j+1} R y_j \text{ für } j = 1, \ldots, m.$$

Setzen:

$$z_i := x_i \text{ für } i = 1, \ldots, n \text{ und}$$

$$z_{n+j} := y_j \text{ für } j = 1, \ldots, m$$

und erhalten

$$x = z_1, z = z_{n+m}$$

und

$$z_k = z_{k+1} \text{ oder } z_k R\, z_{k+1} \text{ oder } z_{k+1} R z_k$$

für alle $k_1, \ldots, n+m$. Also gilt $x\overline{R}z$. □

Definition:
Die Äquivalenzrelation $\overline{R}$ aus dem letzten Satz heißt die durch R auf M induzierte Äquivalenzrelation.

Beispiel:

- Sei M die Menge aller Menschen
  $R : xRy :\Longleftrightarrow x$ ist Elternteil von y.
  Dann ist $\overline{R}$ die Äquivalenzrelation
  $x\overline{R}y \Longleftrightarrow x = y$ oder x ist verwandt mit y.

3.2 Halbordnungsrelationen

Definition:
Eine binäre Relation R auf M heißt Halbordnungsrelation auf M, falls R reflexiv, antiysmmetrisch und transitiv ist.

Bezeichnung:
Anstelle von xRy wird oft $x \leq y$ geschrieben.

Definition:
Eine Halbordnungsrelation $\leq$ auf M heißt Ordnungsrelation auf M, falls für beliebige $x, y \in M$ gilt $x \leq y$ oder $y \leq x$.

Beispiel:

- Betrachten wir die Potenzmenge $P(M)$ einer Menge M.
  $\subseteq$ ist Halbordnungsrelation auf $P(M)$, denn für alle $M_1, M_2, M_3 \in P(M)$ gilt:

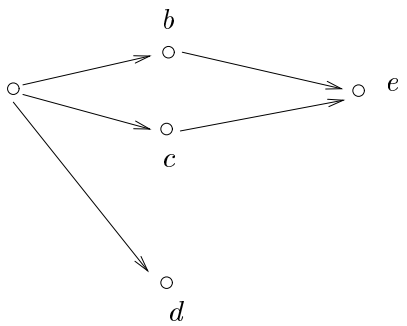
  (a) $M_1 \subseteq M_1$,
  (b) $M_1 \subseteq M_2 \wedge M_2 \subseteq M_1 \Rightarrow M_1 = M_2$,
  (c) $M_1 \subseteq M_2 \wedge M_2 \subseteq M_3 \Rightarrow M_1 \subseteq M_3$.

Wir können die Halbordnung auf endliche Mengen M durch Hasse-Diagramm veranschaulichen:

- stellen Elemente von M als Punkte dar
- verbinden zwei Punkte a, b durch Pfeil von a nach b falls $a \leq b$ und falls kein c existiert mit $a \leq c$ und $c \leq b$.

Beispiel:

- $M = \{a, b, c, d, e\}$
  $R = \{(a, a), \ldots (e, e), (a, b), (a, c), (a, d), (b, e), (c, e)\}$



Definition:
Zwei Elemente a, b heißen bzgl. $\leq$ vergleichbar, falls $a \leq b$ oder $b \leq c$ gilt.

(Bzgl. einer Ordnung sind alle Elemente vergleichbar.)
a heißt unmittelbarer Nachfolger von b, falls kein $c \in M$ existiert mit $a \leq c$ und $c \leq b$.

Definition:
Sei $\leq$ Halbordnung auf M.
$a \in M$ heißt minimales (maximales) Element von M bzgl. $\leq$, falls kein $x \in M$ existiert mit $x \leq a$ $(a \leq x)$

$a \in M$ heißt Minimum(Maximum) von M, falls für alle $x \in M$ gilt $a \leq x (x \leq a)$

Bemerkung:
Jede Teilmenge $N \subseteq M$ hat höchstens ein Minimum (Maximum), kann aber verschiedene minimale/maximale Elemente besitzen.

Definition:
Sei $\leq$ Halbordnung auf M. $N \leq M$ heißt <u>Kette</u> (bzgl. $\leq$), falls $\leq |_N$ eine Ordnung ist.

Wichtiges Axiom der Mengenlehre

Maximalkettenprinzip (Hausdorff-Birkhoff):
(1) In jeder halbgeordneten Menge gibt es bzgl. Mengeninklusion maximale Ketten.
(2) In jeder halbgeordneten Menge gibt es zu jeder Kette k eine k umfassende, bzgl. $\leq$ maximale Kette.

3.3 Funktionen und Abbildungen

Funktionen

Eine Menge von geordneten Paaren (gegeben z.B. durch Tabelle, Kurve, Relation) heißt Zuordnungsvorschrift.

Bezeichung: z.B. f
$(a, b) \in f$ bedeutet "f ordnet a das Element b zu" oder "a wird bei f dem Element b zugeordnet"
a heißt erste Projektion (Bez. $P_1((a, b))$), b heißt zweite Projektion (Bez. $P_2((a, b))$)

Beispiele:

(1)

x	y	
2	4	$f = \{(2,4),(1,2),(3,1),(5,2)\}$
1	2	
3	1	
5	2	

(2) $f = \{(x, y) | x^2 + y^2 = 1\}$ Einheitskreis

(3) $f = \{(x, y) | x \in R \wedge y \in N \wedge y \leq x \wedge y + 1 > x\}$ Gausklammer

Eine Zuordnungsvorschrift kann einem Element a verschiedene Elemente b und c zuordnen. Schränken dies ein:

Definition:
Eine Zuordnungsvorschrift f heißt funktional bzw. Funktion
falls gilt: $(x_1, y_1) \in f \wedge (x_1, y_2) \in f \Rightarrow y_1 = y_2$.
Der Definitionsbereich von f ist Menge der ersten Projektionen.

Bezeichnung: $\mathrm{D}(f), \mathrm{Def}(f), \mathrm{Dom}(f)$

Wertebereich von f ist Menge der zweiten Projektionen.

Bezeichnung: $W(f)$

Schreiben anstelle $(x, y) \in f$ kurz $y = f(x)$

Bemerkung:
Funktion f mit Definitionsbereich D und Wertebereich W ist eindeutige Relation zwischen D und W.

Wir können jede Funktion f mit $D, W \subseteq R$ graphisch darstellen:
Wir ordnen $(x, y) \in f$ den Punkt $P_{(x,y)}$ der euklidischen Ebene zu.
Menge aller Punkte $P_{(x,y)}$ heißt auch Kurve "$y = f(x)$".

Definition:
$f : D \to W'$ heißt umkehrbar eindeutig bzw. eineindeutig, falls für beliebige $(x_1, y), (x_2, y) \in f$ gilt:

$$(x_1, y) \in f \wedge (x_2, y) \in f \Rightarrow x_1 = x_2.$$

Eine eineindeutige Funktion f mit $D(f) = M$ und $W(f) = M'$ bestimmt eine eineindeutige Funktion g mit $D(g) = M'$ und $W(g) = M$ und

$$(y, x) \in g :\Longleftrightarrow (x, y) \in f$$

bzw.

$$x = g(y) \Longleftrightarrow y = f(x).$$

g heißt die zu f inverse Funktion.

Bezeichnung: f^{-1}
Es gilt $(f^{-1})^{-1} = f$.

Beispiele:

- $f_1(x) = 2x + 3$, $f_2(x) = e^x$ sind eineindeutige Funktionen.
  $f_1^{-1}(x) = \frac{y-3}{2}$, $f_2^{-1}(x) = \ln x$.

Abbildungen

Definition:
Eine Abbildung aus der Menge M in die Menge M' ist ein Tripel $F = (M, f, M')$, wobei f eine Funktion ist mit $D(f) \subseteq M, W(f) \subseteq M'$.

Zwei Abbildungen $(M_1, f_1, M_1'), (M_2, f_1, M_2')$ sind gleich, falls $M_1 = M_2, M_1' = M_2'$ und $f_1 = f_2$ im mengentheoretischen Sinne.

andere Schreibweise: $F : M \to M'$ bedeutet, daß F eine Abbildung (M, f, M') ist, mit $D(f) = M$.

Sei $F = (M, f, M')$ Abbildung.

Redeweisen:
F ist Abbildung aus ... bedeutet $D(f) \subseteq M$
F ist Abbildung auf ... bedeutet $W(f) = M'$
F ist Abbildung von ... bedeutet $D(f) = M$

Bemerkung:
Wenn nichts anderes vereinbart ist, betrachten wir stets "Abbildungen von" (andere werden auch partielle Abbildungen genannt).

Definition:
Sei $F = (M, f, M')$ eine Abbildung und $N \subseteq M$.

$\{f(x) | x \in N\}$ heißt Bild von N unter F.

Bezeichnung: $F(N)$.

Sei $N' \subseteq M'.\{x \in M \mid f(x) \in N'\}$ heißt Urbild von N' unter F.

Bezeichung: $F^{-1}(N')$

F ist surjektiv
$=_{\text{def}} F(M) = M'$
F ist injektiv.
$=_{\text{def}} F$ ist Abbildung von M und f ist eineindeutig.
F ist bijektiv.
$=_{\text{def}} F$ ist injektiv und surjektiv.

Folgen und Mengenfamilien

Wir können mit dem Abbildungsbegriff Begriff der Folge exakt fassen:

Definition:
Eine endliche Folge mit Gliedern aus einer Menge M ist eine Abbildung $F : [n] \to M$ von einer Teilmenge $[n] = \{k \in \mathbb{N} | k \leq n\}$ in M.

Bezeichnung: $a_i = F(i)$
Eine unendliche Folge ist eine Abbildung $F : \mathbb{N} \to M$.
Die Folgenglieder sind die Funktionswerte.

Definition:
Sei I eine nichtleere Menge und M beliebig.
Eine injektive Abbildung $F = (I, f, M)$ heißt Indexfunktion von I nach M.

Bezeichnung: I Indexmenge
Wir schreiben m_i anstelle von $f(i)$. i heißt Index von m_i.
(m_i) heißt Familie von Elementen aus M.

Beispiel:

- Π Menge der Primzahlen. Betrachten $P(\mathbb{N})$
  $M_p = \{p^n \,|\, n \in N\}$, $p \in \Pi$.
  $(M_p)_{p \in \Pi}$ Primzahlen sind Indizes.

Definition:
Sei $(M_i)_{i \in I}$ Familie von Teilmengen von M

$$\bigcap_{i \in I} M_i = \{m \,|\, m \in M_i \text{ für alle } i \in I\}$$

$$\bigcup_{i \in I} M_i = \{m \,|\, m \in M_i \text{ für ein } i \in I\}$$

Kardinalität

Definition:
Zwei Mengen M und M' heißen gleichmächtig.
$=_{\text{def}}$ existiert eine eineindeutige Abbildung von M auf M' (d.h. M und M' sind bijektiv).

Bemerkung:
Ist M endlich und sind M und M' gleichmächtig, dann ist M' endlich und hat die gleiche Zahl von Elementen.

Beweis: ÜA

Definition:
M heißt abzählbar unendlich.
$=_{\text{def}}$ M ist gleichmächtig zu $\mathbb{N}$.

Bemerkung:
Die Elemente von M lassen sich eindeutig mit Element aus $\mathbb{N}$ indizieren.

Beispiele:

- $\mathbb{Z}, \mathbb{N}, \mathbb{Q}, 7\mathbb{Z}, \ldots$

Definition:
M heißt nicht abzählbar
$=_{\text{def}}$ M ist weder endlich noch abzählbar unendlich.

Beispiele:

- $[-1, +1], \mathbb{R}, \ldots$

Satz 3.8
Seien $F = (M, f, M'), G = (M', g, M'')$ zwei Abbildungen, dann ist die Hintereinanderausführung von F und G eine Abbildung.
Es gilt

$$F \circ G : x \mapsto (f \circ g)(x) := g(f(x)) \text{ für alle } x \in M.$$

Beweis:
Es gilt $D(f) = M, W(f) \subseteq M'$.
Wegen $D(g) = M'$ gilt $D(f \circ g) = D(f) = M$.
Sei $z_1 = (f \circ g)(x), z_2 = (f \circ g)(x)$.
Dann existieren $y_1, y_2 \in M'$ mit $y_1 = f(x), z_1 = g(y_1)$ und $y_2 = f(x)$ und $z_2 = g(y_2)$.
Wegen $y_1 = f(x) = y_2$ folgt $z_1 = z_2$. □

Teil II

Techniken

Kapitel 4

Beweistechniken

4.1 Theoreme

Mathematische Aussagen werden in Form von Theoremen (Sätzen, Lemmata, Korollare) formuliert; gewöhnlich haben Theoreme die Gestalt

"wenn p so q" bzw. $p \to q$

wobei p und q Aussagen (bzw. Aussageformen) sind; zum Beweis muß q aus p abgeleitet werden unter Zuhilfenahme von Axiomen und logischen Ableitungsregeln (Inferenzregeln).

Inferenzregeln: Modus Ponens:

Wir haben Tautologie: $(p \wedge (p \to q)) \to q$

Schreibweise:

$$\begin{array}{l} p \\ p \to q \\ \hline \hookrightarrow q \end{array}$$

(Wenn p gilt und wenn q aus p folgt, dann gilt q.)

Zusammenstellung wichtiger Inferenzregeln:

Inferenzregel	Tautologie	Name
$\dfrac{p}{\hookrightarrow p \vee q}$	$p \to (p \vee q)$	Addition
$\dfrac{p \wedge q}{\hookrightarrow p}$	$(p \wedge q) \to q$	Vereinfachung
$\dfrac{p \quad p \to q}{\hookrightarrow q}$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\dfrac{\neg q \quad p \to q}{\hookrightarrow \neg p}$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$\dfrac{p \to q \quad q \to r}{\hookrightarrow p \to r}$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetischer Syllogismus
$\dfrac{p \vee q \quad \neg p}{\hookrightarrow q}$	$((p \vee q) \wedge \neg p) \to q$	Disjunktiver Syllogismus

4.2 Beweismethoden

Wir wollen Theorem der Form $p \to q$ beweisen.

(1) Inhaltsleerer Beweis:
Sei p falsch, dann ist $p \to q$ stets wahr, d.h. es kann bewiesen werden, daß p falsch ist, dann ist Beweis $p \to q$ erbracht, "inhaltsleerer Beweis".

Beispiel: $p(n)$: "$n > 1$" ; "$q(n) : n^3 > n$"

Theorem:
$p(0) \to q(0)$ durch inhaltsleeren Beweis.

(2) Trivialer Beweis:
Ist q wahr, dann ist $p \to q$ stets wahr. D.h. kann bewiesen werden, daß q wahr ist, dann

ist Beweis $p \to q$ erbracht. "Trivialer Beweis".

Beispiel: p : "a und b sind positive Zahlen mit $a \geq b$"
$q(n) : a^n \geq p^n$

Theorem:
$p \to q(0)$. Beweis trivial.

(3) direkter Beweis:
Beweisen $p \to q$ durch direkten Nachweis, daß aus Gültigkeit von p die von q folgt, "direkter Beweis".
Wir verwenden dabei Inferenzregeln, die auf die bereits abgeleitete Aussage in geeigneter Weise angewendet werden.

Beispiel:
$p(n)$: "n ist gerade."
$q(n)$: "n^2 ist gerade."

Theorem: $p(n) \to q(n)$

Beweis:
Ist n gerade, so kann n dargestellt werden als $n = 2k$ für ein $k \in \mathbb{Z}$; dann ist $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ eine gerade Zahl.

(4) indirekter Beweis:
$p \to q$ ist logisch äquivalent zu $\neg q \to \neg p$

Wir können $(p \to q)$ zeigen durch Nachweis von $(\neg q \to \neg p)$ "indirekter Beweis".

Beispiel:
$p(n)$:"$3n + 2$ ist ungerade"
$q(n)$:"n ist ungerade"

Beweis:
Annahme: n ist gerade $(\neg q(n))$, dann gilt $n = 2k$ für ein $k \in \mathbb{Z}$; dann ist

$$\begin{aligned} 3n + 2 &= 3(2k) + 2 \\ &= 6k + 2 \\ &= 2(3k + 1) \qquad \text{gerade.} \end{aligned}$$

(5) Beweis durch Widerspruch
Kann eine Kontradiktion q gefunden werden, so daß $\neg p \to q$ wahr ist, dann muß $\neg p$ falsch und demzufolge p wahr sein. "Beweis durch Widerspruch".

Wir können als Kontradiktion z.B. $q = (r \wedge \neg r)$ nehmen.

Beispiel: p : "$\sqrt{2}$ ist irrational."

Theorem: p ist wahr.

Beweis: Wir leiten aus $\neg p$ Widerspruch ab:

Annahme:
Es gilt $\neg p$, d.h. $\sqrt{2}$ ist rational.
Denn ex. teilerfremde $a, b \in \mathbb{Z}$, $b \neq 0$ mit $\sqrt{2} = \frac{a}{b}$.
Dann gilt $2 = (\frac{a}{b})^2 = \frac{a^2}{b^2}$, also $2b^2 = a^2$;
d.h. a^2 ist gerade, also auch a, d.h. es gilt $a = 2c$ für ein $c \in \mathbb{Z}$,
d.h. $2b^2 = (2c)^2 = 4c^2$, also $b^2 = 2c^2$,
woraus folgt, daß b^2 gerade ist und damit auch b.

Widerspruch:

a und b sind teilerfremd	$\stackrel{\triangle}{=} q$	
a und b sind nicht teilerfremd	$\stackrel{\triangle}{=} \neg q$	(ein gemeinsamer Teiler ist 2)

Wir können indirekte Beweise als Beweis durch Widerspruch schreiben:
im indirekten Beweis wird gezeigt, daß $p \to q$ wahr ist, indem $\neg q \to \neg p$ gezeigt wird.

D.h. es wird angenommen, daß $\neg q$ wahr ist und demzufolge $\neg p$ gelten muß. Wir erhalten Beweis durch Widerspruch, wenn angenommen wird, daß p und $\neg q$ wahr sind und gleichzeitig mit $\neg q \to \neg p$ gezeigt wird , daß $\neg p$ gilt; man erhält so Widerspruch $p \wedge \neg p$

Beispiel:
$p(n)$: "$3n + 2$ ist ungerade."
$q(n)$: "n ist ungerade."

Theorem: $p(n) \to q(n)$.

Beweis:
Annahme: $3n + 2$ ist ungerade und n ist nicht ungerade, also gerade.

Zeigen nun analog wie im Beispiel zu indirektem Beweis, daß dann $3n+2$ gerade ist; der erhaltene Widerspruch beweist das Theorem.

(6) Beweis durch Fallunterscheidung
Benutzen zum Beweis von Implikation
(*) $(p_1 \vee p_2 \vee ... \vee p_n) \to q$

die Tautologie

$$[(p_1 \vee p_2 \vee ... \vee p_n) \to q] \leftrightarrow [(p_1 \to q) \wedge ... \wedge (p_n \to q)]$$

als Inferenzregel; d.h. zum Beweis von (*) werden n Implikation $p_i \to q$ beweisen ("Beweis durch Fallunterscheidung").
Oft sinnvoll auch beim Beweis von Theorem der Art $p \to q$ durch "Zerlegung" von Hypothesen p in einfachen Hypothesen $p_1, ..., p_n$ mit $p = p_1 \vee ... \vee p_n$.

Beispiel:
$p(n)$: "$n \in \mathbb{Z}$ ist nicht durch 3 teilbar"
$q(n)$: "$n^2 \equiv 1(\text{mod}3)$"

Theorem: $p(n) \to q(n)$

Beweis: $p(n)$ ist äquivalent zu $p_1 \vee p_2$ mit
p_1 : "$n \equiv 1(\text{mod}3)$"
p_2 :" $n \equiv 2(\text{mod}3)$"

Zeigen $p_1 \to q$ und $p_2 \to q$

1. Fall:
Sei p_1 wahr, also $n \equiv 1(\text{mod}3)$, dann gilt $n = 3k+1$ für ein $k \in \mathbb{Z}$; also

$$\begin{aligned} n^2 = (3k+1)^2 &= 9k^2 + 6k + 1 \\ &= 3(3k^2 + 2k) + 1 \end{aligned}$$

also $n^2 \equiv 1(\text{mod}3)$.

2. Fall:
Sei p_2 wahr, also $n \equiv 2(\text{mod}3)$, dann gilt $n = 3k+2$ für ein $k \in \mathbb{Z}$; also

$$\begin{aligned} n^2 &= (3k+2)^2 = 9k^2 + 12k + 4 \\ &= 3(3k^2 + 4k + 1) + 1 \end{aligned}$$

also $n^2 \equiv 1(\text{mod}3)$.

(7) Äquivalenzbeweis:
Zum Beweis von Theorem der Form $p \leftrightarrow q$ wird die Tautologie

$$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$$

benutzt, wobei für $(p \rightarrow q)$ und $(q \rightarrow p)$ geeignete Beweismethode angewandt wird.

4.3 Theoreme und Quantoren

Viele Theoreme enthalten Quantoren.

(1) **Existenzbeweise:**
Oft haben Theoreme die Form $\exists x p(x)$. Beweise solcher Theoreme heißen "Existenzbeweise".

Methoden:

- Finde ein Element a, so daß $p(a)$ wahr ist ("Konstruktiver Existenzbeweis").
- Beweis, der nicht auf der Angabe eines die Aussageform erfüllenden Elementes beruht, heißt "nichtkonstruktiver Existenzbeweis", z.B. Beweis durch Widerspruch, angewandt auf Negation der Existenzaussage.

Beispiel: Konstruktiver Existenzbeweis:

Theorem:
Für jedes n existieren n aufeinanderfolgende zusammengesetzte Zahlen.

$(\forall n \, \exists k (k + i \text{ ist zusammengesetzt für alle } i = 1, ..., n))$

Beweis:
Sei $k = (n+1)! + 1$

Betrachten: $k+1, k+2, ..., k+n$.
Offenbar teilt $(i+1)$ die Zahl $(k+i) = (n+1)! + (i+1)$ für $i = 1, ..., n$.

Beispiel: Nichtkonstruktiver Existenzbeweis:

Theorem: Für alle $n \in I\!N$ gibt es eine Primzahl größer n. ($\forall n \, \exists x q(x)$ mit $q(x)$: "x ist Primzahl und $x > n$")

Beweis:
Betrachten: $n! + 1$

Da jede Zahl einen Primfaktor hat, hat auch $n! + 1$ wenigstens einen Primfaktor (z.B. $n! + 1$). Würde $n! + 1$ durch Zahl $\leq n$ geteilt werden, dann müßte der Rest 1 bleiben; d.h. jeder Primfaktor von $n! + 1$ muß $> n$ sein.

(2) **Beweis durch Gegenbeispiel:**
Wir wollen zeigen, daß die Aussage der Form $\forall x p(x)$ falsch ist;

es gilt $\neg \forall x p(x)$ ist logisch äquivalent zu $\exists x (\neg p(x))$. D.h. es genügt ein Element a zu finden, so daß $p(a)$ falsch ist ("Beweis durch Gegenbeispiel").

Bemerkung:
Ein einziges Gegenbeispiel genügt zum Nachweis von: $\forall x \, p(x)$ ist falsch.

Beispiel:
Die Aussage "alle Primzahlen sind ungerade" ist falsch.
($\forall x p(x)$ mit $p(x)$: "x ist ungerade und x ist Primzahl".)

Beweis:

Gegenbeispiel: $x = 2$.

4.4 Abschließende Bemerkungen

Wir haben verschiedene Beweismethoden vorgestellt, aber keinen Algorithmus zum Theorembeweisen angegeben; tatsächlich kann es keinen solchen Algorithmus geben ($\rightarrow$ Berechenbarkeitstheorie);

Theoreme zu beweisen, ist oft eine sehr anspruchsvolle Tätigkeit. Es gilt, die geeigneten Ableitungsschritte und Beweismethoden zu finden. Für viele Theoreme gibt es bis heute

keine Beweise, z.B. "Goldbach'sche Vermutung" - "jede ganze Zahl größer als 4 ist die Summe von zwei Primzahlen.

Kapitel 5

Mathematische Induktion

5.1 Einführung

Mathematische Induktion ist eine wichtige Beweistechnik. Zugrundeliegendes Axiom: Wohlordnungsprinzip - "jede nichtleere Menge nichtnegativer Zahlen hat ein kleinstes Element."

5.2 Idee der mathematischen Induktion

Sei $p(n)$ Aussageform, die von der mathematischen Zahl $n \in I\!N$ abhängt.

Mathematische Induktion ist Technik zum Beweis, daß Theorem: "$n \overset{\forall n}{\geq} 1 \;\; p(n)$" gilt
Der Beweis durch die mathematische Induktion besteht aus zwei Schritten.

Basisschritt:
Es wird gezeigt, daß $p(1)$ gilt.

Induktionsschritt:
Es wird gezeigt, daß die Implikation $p(n) \rightarrow p(n+1)$ für alle n gilt.

$p(n)$ heißt "Induktionsannahme"; beide Schritte zusammen ergeben, daß $n \overset{\forall n}{\geq} 1 \;\; p(n)$ gilt.
Zugrundeliegende Inferenzregel:

$$[p(1) \wedge \forall n(p(n) \rightarrow p(n+1))] \rightarrow \forall n \, p(n)$$

Bemerkung:
Induktionsannahme ist nicht, daß $p(n)$ für alle n gilt;

Induktionsannahme ist, daß $p(n)$ für ein n gilt.

Tatsächlich:
Zeigen $p(1)$ gilt (Basisschritt).
Zeige, aus $p(1)$ folgt $p(2)$, damit gilt $p(2)$.
Zeige, aus $p(2)$ folgt $p(3)$, damit gilt $p(3)$.
...

Mathematische Induktion liefert wahre Aussage, wegen Wohlordnungsaxiom:

Annahme:
$p(1)$ ist wahr und für alle n gilt $p(n) \rightarrow p(n+1)$

Behauptung:
$p(n)$ gilt für alle n

Annahme:
Es existiert n mit $p(n)$ ist falsch. Sei $S \subseteq I\!N$ Menge, für die $p(n)$ falsch ist. Nach Wohlordnungsaxiom hat S kleinstes Element n_0.
Wissen: $n_0 \neq 1$, da $p(1)$ gilt.
Wegen $n_0 - 1 < n_0$ gilt $p(n_0)$.
Dann ist $p(n_0 - 1) \rightarrow p(n_0)$ falsch. Widerspruch

5.3 Beispiele für Induktionsbeweise

1.) Behauptung: $p(n) : \Sigma_{i=1}^{n} (2i-1) = n^2$ gilt für alle n

Beweis:
Wir benutzen die Abkürzung $S(n) = \Sigma_{i=1}^{n}(2i-1)$.

Basis: $p(1) : S(1) = \Sigma_{i=1}^{1} (2i-1) = 2 \cdot i - 1 = 1 = 1^2$.

Induktion: Sei $p(n)$ bereits bewiesen

Zeigen $p(n) \rightarrow p(n+1)$ ist wahr, also gilt $p(n+1)$

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

$$
\begin{aligned}
&= \sum_{i=1}^{n}(2i-1) + 2(n+1) - 1 \\
&= n^2 + 2n + 1 \\
&= (n+1)^2
\end{aligned}
$$

2.) Behauptung: $p(n) : \Sigma_{i=0}^{n} 2^i = 2^{n+1} - 1$

Beweis:
Wir benutzen die Abkürzung $S(n) = \Sigma_{i=0}^{n} 2^i$.

Basis: $p(1) : \Sigma_{S(1)i=0}^{1} 2^i = 1 + 2 = 2^2 - 1$

Induktion:

$$
\begin{aligned}
S(n+1) &= \sum_{i=0}^{n+1} 2^i \\
&= \sum_{i=o}^{n} 2^i + 2^{n+1} \\
&= 2^{n+1} - 1 + 2^{n+1} \\
&= 2 \cdot 2^{n+1} - 1 \\
&= 2^{n+1} - 1 \\
&= 2^{(n+1)+1} - 1
\end{aligned}
$$

3.) Betrachte $H_k := 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{k}, \quad k = 1, 2, ...$ - "Harmonische Zahlen"

Behauptung $p(n) : H_{2^n} \geq 1 + \frac{n}{2}$ für alle $n \geq 1$.

Beweis durch mathematische Induktion:

Basis: $p(1) : H_{2^1} = 1 + \frac{1}{2} \geq 1 + \frac{1}{2}$.

Induktion:

$$
\begin{aligned}
H_{2^{n+1}} &= 1 + \tfrac{1}{2} + ... + \tfrac{1}{2^n} + \tfrac{1}{2^n+1} + ... + \tfrac{1}{2^{n+1}} \\
&= H_{2^n} + \tfrac{1}{2^n+1} + ... + \tfrac{1}{2^{n+1}} \\
&\geq (1 + \tfrac{n}{2}) + \tfrac{1}{2^n+1} + ... + \tfrac{1}{2^{n+1}} \text{ (nach Induktionsannahme)} \\
&\geq (1 + \tfrac{n}{2}) + 2^n \cdot \tfrac{1}{2^{n+1}} \; 2^n \text{ Terme} \geq \tfrac{1}{2^{n+1}} \\
&= (1 + \tfrac{n}{2}) + \tfrac{1}{2} \\
&= 1 + \tfrac{n+1}{2}.
\end{aligned}
$$

5.4 Vollständige Mathematische Induktion

Die sogenannte vollständige Induktion beruht auf folgendem Schema:

Basisschritt: Zeigen $p(1)$ ist wahr.

Induktionsschritt: Zeige

$$[p(1) \wedge ... \wedge p(n)] \rightarrow p(n+1)$$

ist wahr für alle n.

Beide Formen der Induktion sind äquivalent!

Beispiel:
Behauptung: $p(n)$: "n kann als Produkt von Primzahl geschrieben werden".

Beweis:
Basis: $p(2) = 2$ Produkt einer Primzahl.

Induktion:
Anmerkung: $p(n)$ ist wahr für alle $k \leq n$, zeige $p(n+1)$ ist wahr:

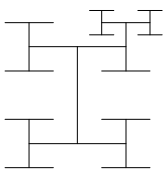
1. Fall:
$(n+1)$ ist Primzahl, dann gilt Behauptung.

2. Fall:
$(n+1)$ ist keine Primzahl, dann kann $(n+1)$ geschrieben werden als $(n+1) = k \cdot l$ mit $2 \leq k, l < n$.

Für k und l gilt Behauptung, also gilt Behauptung auch für $n+1$.

5.5 Rekursive Definitionen

Wir können Objekte mit sich selbst definieren; der Prozeß heißt "Rekursion".
Beispiel:



Wir können mathematische Objekte, wie z.B. Folgen, Funktionen, Mengen rekursiv definieren.

Rekursiv definierte Funktion
Funktionen über den natürlichen Zahlen können rekursiv definiert werden:

(1) spezifizieren Wert der Funktion in 0.

(2) geben Regeln an, um neue Werte der Funktion aus Werten für kleinere Argumente zu berechnen.

Beispiel: $f(0) = 3$.
$f(n+1) = 2f(n) + 3$.

Berechnen $f(1), f(2), f(3)$

$$\begin{array}{lll} f(1) = & 2f(0) + 3 = 2 \cdot 3 + 3 & = 9. \\ f(2) = & 2f(1) + 3 = 2 \cdot 9 + 3 & = 21. \\ f(3) = & & = 45. \\ f(4) = & & = 93. \end{array}$$

Beispiel: "Faktorial" $f(n) = n!$

Wir können Faktorial rekursiv definieren:

$f(0) = 1$.
$f(n+1) = (n+1) \cdot f(n)$.

Rekursiv definierte Funktionen sind wohldefiniert nach dem Prinzip der mathematischen Induktion.

Beispiel: Fibonacci–Zahlen

$$f_0 = 0\,,\ f_1 = 1$$

$$f_n = f_{n-1} + f_{n-2}$$

z.B.:

$$f_2 = f_1 + f_0 = 0 + 1 = 1.$$
$$f_3 = f_2 + f_1 = 1 + 1 = 2.$$
$$f_4 = f_3 + f_2 = 2 + 1 = 3.$$

$$f_5 = f_4 + f_3 = 3 + 2 = 5.$$

Wir können mit rekursiven Funktionen viele Eigenschaften beweisen.

Behauptung:
Für alle $n \geq 3$ gilt $f_n > \alpha^{n-2}$ für $\alpha = \frac{1+\sqrt{5}}{2}$.

Beweis: durch mathematische Induktion

$$p(n) \; : \; f_n > \alpha^{n-2}$$

Basisschritt:

$$\alpha^1 = \frac{1+\sqrt{5}}{2} \; < 2 = f_3$$

$$\alpha^2 = (\frac{1+\sqrt{5}}{2})^2 \; < 3 = f_4$$

Induktionsschritt:
Sei $p(k)$ wahr für alle $3 \leq k < n$, $n \geq 4$

Zu zeigen: Es gilt $p(n+1)$, also $\alpha^{n-1} < f_{n+1}$

α ist die Lösung von $x^2 - x - 1 = 0$

$$\begin{aligned}
\Rightarrow \alpha^2 \quad & = \alpha + 1 \\
\Rightarrow \alpha^{n-1} \quad & = \alpha^2 \, \alpha^{n-3} \\
& = (\alpha + 1) \, \alpha^{n-3} \\
& = \alpha^{n-2} \; + \alpha^{n-3} \\
& < f_n + f_{n-1} \\
& = f_{n+1}
\end{aligned}$$

Wir können interessante Theoreme beweisen mit Hilfe der Fibonacci Zahlen: **Theorem von Lamé**.

Sei $a, b \in I\!N$, $a \geq b$. Die Zahl der Divisionen beim Euklidischen Algorithmus zur Bestimmung von ggT(a, b) ist kleiner als das Fünffache der Dezimalstellen von b.

Beweis: Übung

Rekursiv definierte Mengen
Oft werden Mengen rekursiv definiert:
Ausgangspunkt: initiale Mengen von Elementen. Mit Hilfe von Regeln werden aus Element der Menge weitere Elemente berechnet.

Beispiel: $3 \in S$

$$x + y \in S \text{ falls } x \in S \text{ und } y \in S$$

Behauptung: $S = 3\mathbb{N} = \{3n \mid n \in \mathbb{N}\}$

Beweis: $\subseteq$: $3\mathbb{N} \subseteq S$

Wir beweisen induktiv: $p(n) : 3n \in S$

Basisschritt: $p(1) : 3 \in S$ ist klar.

Induktionsschritt: Sei $p(n)$ wahr.

$\Rightarrow 3n \in S$, wissen $3 \in S$

$\Rightarrow 3n + 3 = 3(n + 1) \in S.$

d.h. es gilt $p(n + 1)$.

$\supseteq$: $S \subseteq 3\mathbb{N}$

Beweis mittels rekursiver Definition:

Basisschritt: $3 \in S$ und $3 = 3 \cdot 1 \in 3\mathbb{N}$

Sei $x + y \in S$ mit $x \in S$ und $y \in S$ und $x, y \neq 3$.

Annahme: $x, y \in 3\mathbb{N}$

$\Rightarrow x = 3x'$, $y = 3y'$

$$\Rightarrow x + y = 3x' + 3y'$$
$$= 3(x' + y') \in 3\mathbb{N}$$

Wir können mittels rekursiver Definition wohlgeformte Ausdrücke in verschiedenen Systemen beschreiben.

Beispiel:
Wohlgeformte arithmetische Ausdrücke über Variablen, Zahlen und Operatoren aus $\{+, -, *, /, \uparrow\}$ können definiert werden durch:

(1) x ist wohlgeformte arithmetischer Ausdruck falls x eine Variable oder eine Zahl ist.

(2) $(f + g), (f - g), (f * g), (f/g), (f \uparrow g)$ sind wohlgeformte arithmetische Ausdrücke, falls f und g wohlgeformte artihmetische Ausdrücke sind.

Beispiel:
Wohlgeformte aussagenlogische Formeln über den Wahrheitswerten w, f , aussagenlogische Variablen und Operatoren aus $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ können definiert werden durch:

(1) w, f und p sind wohlgeformte, aussagenlogische Ausdrücke, wobei p eine aussagenlogische Variable ist.

(2) $(\neg p), (p \wedge q), (p \vee q), (p \rightarrow q), (p \leftrightarrow q)$ sind wohlgeformte aussagenlogische Formeln, falls p mit q wohlgeformte aussagenlogische Formeln sind.

Rekursive Definitionen werden oft zur Untersuchung von Strings (Buchstabenfolgen) benutzt:

Beispiel: Σ endliches Alphabet

Σ^* Menge aller Wörter über Σ

Wir können Σ^* rekursiv definieren mit Hilfe der "Konkatenation".
(Aneinanderhängen von Wörtern x und y, wobei das Wort xy entsteht).
$\lambda \in \Sigma^*$ λ ist das leere Wort, welches keine Symbole enthält.

$wx \in \Sigma^*$ falls $w \in \Sigma^*$ und $x \in \Sigma$

Beispiel:
Wir können die Länge von Strings rekursiv definieren:

$l(\lambda) = 0$

$l(wx) = l(w) + 1$ falls $w \in \Sigma^*$ und $x \in \Sigma$

Behauptung: $l(xy) = l(x) + l(y)$ für alle $x, y \in \Sigma^*$.

Beweis:
Sei $p(y) : l(xy) = l(x) + l(y)$ für $x \in \Sigma^*$

Basisschritt:
Zu zeigen: $p(\lambda)$ ist wahr.

Genügt zu zeigen: $l(x\lambda) = l(x) + l(\lambda)$ für alle $x \in \Sigma^*$.

Wegen

$$\begin{aligned} l(x\lambda) &= l(x) \\ &= l(x) + 0 \\ &= l(x) + l(\lambda) \text{ gilt: } p(\lambda) \text{ ist wahr.} \end{aligned}$$

Induktionsschritt:
Annahme: $p(y)$ ist wahr.
Zu zeigen: $p(ya)$ ist wahr für alle $a \in \Sigma$.

Genügt zu zeigen: $l(xya) = l(x) + l(ya)$ für alle $x \in \Sigma^*$, $a \in \Sigma$.

Wegen

$$l(xya) = l(xy) + 1, \quad l(ya) = l(y) + 1$$

und

$$l(xy) = l(x) + l(y)$$

folgt

$$\begin{aligned} l(xya) &= l(xy) + 1 \\ &= l(x) + l(y) + 1 \\ &= l(x) + l(ya). \end{aligned}$$

Kapitel 6

Zählen

Das Abzählproblem tritt in allen Gebieten der Mathematik und Infomatik auf.
Beispiele:

- Wie sicher sind Computercodes.
- Wie groß ist die Wahrscheinlichkeit eines Ereignisses.
- Welche Komplexität hat ein Algorithmus.
- ...

6.1 Grundlegende Zählprinzipien

(1) **Summenregel**
Für einen Versuch gebe es n_1 verschiedene Ausgänge vom Typ 1 und n_2 verschiedene Ausgänge vom Typ 2 (wobei kein Ausgang sowohl vom Typ 1 als auch vom Typ 2 sein kann) und keine weiteren.
Dann gibt es genau $n_1 + n_2$ verschiedene Verscuhsausgänge.

Beispiel:
Auswahl eines Repräsentanten aus zwei disjunkten Mengen der Größe 37 und 41:
Es gibt 37+41=78 Möglichkeiten.

Diese Regel kann auf mehr als zwei Klassen ausgedehnt werden.

Mathematische Formulierung:
Seien $A_1, ..., A_m$ disjunkte endliche Mengen.
Dann gilt:

$$\#\bigcup_{i=1}^{m} A_i = \sum_{i=1}^{m} \#A_i \text{ (Summenregel)}$$

Bemerkung:
$\#A := card\ A =$ Zahl der Elemente von A.

(2) **Produktregel**
Ein Versuch bestehe aus 2 Teilversuchen, von denen der erste n_1 verschiedene Ausgänge und der zweite n_2 verschiedene Ausgänge hat.
Dann gibt es genau $n_1 \cdot n_2$ verschiedene Versuchsausgänge.

Beispiel:
Nummerierung der Sessel eines Kinos mit einem Buchstaben und einer Zahl ≤ 100.
Dann gibt es $26 \cdot 100 = 2600$ verschiedene Platznummern.

Diese Regel kann verallgemeinert werden:

Mathematische Formulierung:
Seien $A_1, ..., A_m$ endliche Mengen.
Dann gilt:

$$\#(A_1 \times ... \times A_m) = \prod_{i=1}^{m} \#A_i.$$

(3) **Funktionsanzahl**
Seien A, B endliche Mengen
Dann gilt:

$$\#\{f : A \to B\} = \#B^{\#A}.$$

Beweis:
Jedem Element von A können $\#B$ Elemente zugeordnet werden.

$$\Rightarrow \text{Es gibt } \underbrace{\#B \cdots \#B}_{\#A\text{-mal}} = \#B^{\#A} \text{ verschiedene Funktionen } f : A \to B.$$

□

(4) **Anzahl eineindeutiger Abbildungen**
Sei A endliche Menge.

$$\#\{f : A \to A \text{ eineindeutig}\} = (\#A)!$$

Beweis:
Dem ersten Element von A können $\#A$ verschiedene Elemente zugeordnet werden.
Dem zweiten Element von A können $\#A - 1$ verschiede Elemente zugeordnet werden.
...

Dem letzten Element von A kann genau ein Element zugeordnet werden. □

Verallgemeinerung:
Anzahl der eineindeutigen Abbildungen von A in B.

$$\#\{f : A \to B \text{ eineindeutig}\} = \begin{cases} \#B \cdots (\#B - \#A + 1) & : \quad \#B \geq \#A. \\ 0 & : \quad \text{sonst.} \end{cases}$$

(5) **Anzahl der Untermengen einer endlichen Menge**
Sei A eine endliche Menge.
Dann gilt:

$$\#\{S : S \subseteq A\} = 2^{\#A}.$$

Beweis:
Aufschreiben der Elemente von A in beliebiger Ordnung.
Jeder Untermenge S der Menge A kann eindeutig ein Bitstring der Länge $\#A$ zugeordnet werden:
i-tes Bit ist $1 \Leftrightarrow$ i-tes Element von A gehört zu S.
Es gibt $2^{\#A}$ Bitstrings der Länge $\#A$.

□

6.2 Inklusions–Exklusionsprinzip

Seien A_1, A_2 endliche Mengen.
Dann gilt:

$$\#(A_1 \cup A_2) = \#A_1 + \#A_2 - \#A_1 \cap A_2 \text{ (Inklusions–Exklusionsprinzip)}$$

Beispiel:
Wieviele Binärwerte der Länge 8 gibt es, die mit 0 anfangen oder mit 11 enden?

Es gibt $2^7 = 128$ Binärwerte der Länge 8, die mit 0 anfangen.
Es gibt $2^6 = 64$ Binärwerte der Länge 8, die mit 11 enden.
Es gibt $2^5 = 32$ Binärwerte der Länge 8, die mit 0 anfangen und mit 11 enden.
$\Rightarrow$ Die gesuchte Anzahl ist $2^7 + 2^6 - 2^5 = 160$.

Verallgemeinerung auf mehr als zwei Mengen später.

6.3 Taubenschlagprinzip

Taubenschlagprinzip:
Werden $k + 1$ Objekte auf k Fächer verteilt, so gibt es ein Fach, das mindestens zwei

Objekte enthält.

Beispiel:
In jeder Gruppe von 8 Leuten haben mindestens zwei am gleichen Wochentag Geburtstag.

Verallgemeinertes Taubenschlagprinzip:
Werden n Objekte auf k Fächer verteilt, dann gibt es mindestens ein Fach, das $\lceil \frac{n}{k} \rceil$ Objekte enthält.

Beweis:
Annahme: Keins der Fächer enthält mehr als $\left\lceil \frac{n}{k} \right\rceil - 1$ Objekte.
Dann gilt für die Gesamtanzahl

$$k\left(\left\lceil \frac{n}{k} \right\rceil - 1\right) < k\left(\left(\frac{n}{k} + 1\right) - 1\right) = n. \text{ Widerspruch}$$

□

Beispiel:
Unter 100 Leuten sind mindestens $\left\lceil \frac{100}{12} \right\rceil = 9$ im gleichen Monat geboren.

Interessante Anwendungen

Satz 6.1
Jede Folge von n^2+1 verschiedenen reellen Zahlen enthält eine monoton fallende oder einen monoton wachsende Unterfolge der Länge $n+1$.

Beispiel: $(n=3)$
7,6,11,13,5,2,4,1,9,8.
Fallend: 7,6,2,1.

Beweis:
Sei $a_1, \ldots, a_{n^2+1}$ eine Folge verschiedener reeller Zahlen.
Ordne a_k den Term (i_k, d_k) zu mit

i_k	Länge der längsten monoton fallenden Unterfolge, die in a_k startet.
d_k	Länge der längsten monoton wachsenden Unterfolge, die in a_k startet.

Annahme: Es gibt weder mononton wachsende noch monoton fallende Unterfolgen der Länge $n+1$.
$\Rightarrow i_k, d_k \leq n$ für alle $k = 1, \ldots, n^2+1$.
$\Rightarrow$ Es gibt $\leq n^2$ verschiedene Paare unter den (i_k, d_k) $k = 1, \ldots, n^2+1$.
$\Rightarrow$ Mindestens zwei der n^2+1 Paare sind gleich.
$\Rightarrow$ Es gibt zwei Elemente a_t, a_s , $s < t$ mit $i_s = i_t$ und $d_s = d_t$.
Das ist unmöglich:
1.Fall: $a_s < a_t \Rightarrow$ Widerspruch zu $i_s = i_t$.
2.Fall: $a_s > a_t \Rightarrow$ Widerspruch zu $d_s = d_t$. □

6.4 Permutation und Kombination

Definition:
Eine *Permutation* ist ein geordnetes Arrangement von verschiedenen Objekten einer Menge S.

Beispiel:
$S = \{1, 2, 3\}$.
$\Rightarrow$ Mögliche Permutationen: 123,
132,
213,
231,
312,
321.

Definition:
Eine *r–Permutation* von n Objekten ist ein geordnetes Arrangement von r der n Objekte.

Beispiel:
$S = \{1, 2, 3\}$.
$\Rightarrow$ Mögliche 2–Permutationen: 12,
13,
21,
23,
31,
32.

Bezeichnung:
$P(n, r)$ entspricht der Anzahl der r–Permutationen von n Elementen.

Satz 6.2
Es gilt:

$$P(n, r) = n(n-1)\cdots(n-r+1).$$

Beweis:
Das erste Element einer Permutation kann auf n Weisen gewählt werden.
Das zweite Element einer Permutation kann auf $n-1$ Weisen gewählt werden.
...
$\Rightarrow P(n, r) = n(n-1)\cdots(n-r+1).$ □

Korollar

(1) $P(n, r) = \frac{n!}{(n-r)!}$.

(2) $P(n, n) = n!$.

Definition:
Eine *r–Kombination* von Elementen einer Menge ist eine umgeordnete Auswahl von r Elementen.
(D.h. r–Kombinationen sind Teilmengen mit r Elementen.)

Beispiel:
$S = \{1, 2, 3, 4\}$.
$\Rightarrow$ Alle 3–Kombinationen: {1,2,3},
{1,2,4},
{1,2,4},
{1,3,4},
{2,3,4}.
Sei $C(n, r)$ die Anzahl der r–Kombinationen einer Menge von n Elementen.

Satz 6.3
Sei $0 \leq r \leq n$.
Dann gilt:

$$C(n,r) = \frac{n!}{r!(n-r)!}.$$

Beweis:
Gewinnung der r–Kombinationen durch Festlegung der Anordnung der r–Permutationen.
Wegen

$$P(r,r) = r!$$

und

$$P(n,r) = C(n,r) \cdot P(r,r)$$

gilt

$$C(n,r) = \frac{P(n,r)}{P(r,r)} = \frac{n!}{(n-r)!\ r!}.$$

□

Korollar:

$$C(n,r) = C(n,n-r).$$

Beweis:

$$\begin{aligned} C(n,r) &= \frac{n!}{r!\ (n-r)!}. \\ C(n,n-r) &= \frac{n!}{(n-r)!\ (n-(n-r))!} \\ &= \frac{n!}{(n-r)!\ r!}. \end{aligned}$$

□

Definition:
Die Zahl der r–Kombinationen von n Elementen heißt *Binomialkoeffizient*.

$$\left(\begin{array}{c} n \\ r \end{array} \right) := \frac{n!}{r!\ (n-r)!}.$$

Satz: (Pascalsche Ungleichung)
Seien $n, k \in I\!N\ ,\ n \geq k$.
Dann gilt:

$$C(n+1,k) = C(n,k-1) + C(n,k).$$

Beweis:
Sei T eine Menge mit $n+1$ Elementen.
Sei $a \in T$, $S := T - \{a\}$
Es gilt:
$C(n+1,k)$ ist Teilmenge von T mit k Elementen.
Jede k–Teilmenge von T besteht aus k Elementen von S oder aus $k-1$ Elementen von S und zustzlich dem Element a.
$C(n,k-1)$ Zahl der $(k-1)$–Untermengen von S.
$C(n,k)$ Zahl der k–Untermengen S von T.
$\Rightarrow$

$$C(n+1,k) = C(n,k-1) + C(n,k).$$

bzw.

$$\left(\begin{array}{c} n+1 \\ k \end{array} \right) = \left(\begin{array}{c} n \\ k-1 \end{array} \right) + \left(\begin{array}{c} n \\ k \end{array} \right).$$

□

Pascalsches Dreieck:

$$\begin{array}{ccccccccccc}
 & & & & \left(\begin{array}{c} 0 \\ 0 \end{array} \right) & & & & & & \\
 & & & \left(\begin{array}{c} 1 \\ 0 \end{array} \right) & & \left(\begin{array}{c} 1 \\ 1 \end{array} \right) & & & & & \\
 & & \left(\begin{array}{c} 2 \\ 0 \end{array} \right) & & \left(\begin{array}{c} 2 \\ 1 \end{array} \right) & & \left(\begin{array}{c} 2 \\ 2 \end{array} \right) & & & & \\
 & \left(\begin{array}{c} 3 \\ 0 \end{array} \right) & & \left(\begin{array}{c} 3 \\ 1 \end{array} \right) & & \left(\begin{array}{c} 3 \\ 2 \end{array} \right) & & \left(\begin{array}{c} 3 \\ 3 \end{array} \right) & & & \\
\left(\begin{array}{c} 4 \\ 0 \end{array} \right) & & \left(\begin{array}{c} 4 \\ 1 \end{array} \right) & & \left(\begin{array}{c} 4 \\ 2 \end{array} \right) & & \left(\begin{array}{c} 4 \\ 3 \end{array} \right) & & \left(\begin{array}{c} 4 \\ 4 \end{array} \right) & & \\
\left(\begin{array}{c} 5 \\ 0 \end{array} \right) & & \left(\begin{array}{c} 5 \\ 1 \end{array} \right) & & \left(\begin{array}{c} 5 \\ 2 \end{array} \right) & & \left(\begin{array}{c} 5 \\ 3 \end{array} \right) & & \left(\begin{array}{c} 5 \\ 4 \end{array} \right) & & \left(\begin{array}{c} 5 \\ 5 \end{array} \right)
\end{array}$$

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Satz 6.4
Sei $n \in \mathbb{N}$.
Dann gilt:

$$\sum_{k=0}^{n} C(n,k) = 2^n.$$

Beweis:
Eine n–Menge hat 2^n Teilmengen.
Jede Teilmenge hat entweder 0 Elemente, 1 Element,..., n Elemente.
Es gilt:
$C(n,0)$ ist die Zahl der Teilmengen mit 0 Elementen.
$C(n,1)$ ist die Zahl der Teilmengen mit 1 Element.
...
$C(n,n)$ ist die Zahl der Teilmengen mit n Elementen.
$\Rightarrow$

$$\sum_{k=0}^{n} C(n,k) = 2^n.$$

□

Satz: (Vandermondsche Ungleichung)
Seien $m, n, r \in \mathbb{N}$, $r \leq m$ oder $n \leq m$.
Dann gilt:

$$C(m+n,r) = \sum_{k=0}^{r} C(m,r-k)\ C(n,k).$$

Beweis:
Seien M, N disjunkte Mengen mit $\#M = m, \#N = n$.
Dann gibt es $C(m+n,r)$ Möglichkeiten r Elemente aus der Vereinigung beider Mengen zu wählen.
Anstelle der r Elemente aus der Vereinigung werden k Elemente aus M und $(r-k)$ Elemente aus N ausgewählt. $(0 \leq k \leq r)$
Dies kann auf

$$C(m,k) \cdot C(n,r-k)$$

verschiedene Weisen geschehen.
$\Rightarrow$

$$C(m+n,r) = \sum_{k=0}^{r} C(m,r-k)\ C(n,k).$$

□

Theorem: (Binomischer Satz)
Seien x, y Variablen , $n \in \mathbb{N}$.
Dann gilt:

$$(x+y)^n = \sum_{j=0}^{n} C(n,j)\ x^{n-j}y^j.$$

Beweis: $(x+y)^n = \underbrace{(x+y)\cdots(x+y)}_{n\text{–mal}}$.
Beim Ausmultiplizieren entstehen Terme der Form $x^{n-j}y^j$, $j = 0, \ldots, n$.

Die Terme entstehen durch die Auswahl von $n-j$ vielen Symbolen x aus n möglichen.
$\Rightarrow$ Anzahl der Terme:

$$C(n, n-j) = C(n, j).$$

□

Beispiel:
$(x+y)^5 = 1x^5 \ + \ 5x^4y \ + \ 10x^3x^2 \ + \ 10x^2y^3 \ + \ 5xy^4 \ + \ 1y^5.$

Satz 6.5
Sei $n \in \mathbb{N}$.
Dann gilt:

$$\sum_{k=0}^{n} (-1)^k C(n,k) = 0.$$

Beweis:
Nach dem binomischen Satz gilt:

$$\begin{aligned} 0 = ((-1)+1)^n &= \sum_{k=0}^{n} C(n,k) \ (-1)^k 1^{n-k} \\ &= \sum_{k=0}^{n} C(n,k) \ (-1)^k. \end{aligned}$$

□

Kapitel 7

Diskrete Wahrscheinlichkeit

Kombinatorik und Wahrscheinlichkeitstheorie haben den gleichen Ursprung.

Sei S die Menge der möglichen, sich einander ausschließenden Ausgänge eines Versuchs *(Elementarereignisse)*.
$E \subseteq S$ heißt *Ereignis*.
(E tritt genau dann ein, wenn eines der Elementarereignisse aus E eintritt).
S heißt das *sichere Ereignis*.
$\emptyset$ heißt das *unmögliche Ereignis*.
Annahme: S endlich.

Definition:
Die Wahrscheinlichkeit $p(E)$ eines Ereignisses $E \subseteq S$ einer endlichen Menge von *gleichwahrscheinlichen Elementarereignissen* ist definiert durch

$$p(E) = \frac{\#E}{\#S}.$$

1. Beispiel:
Eine Urne enthält 3 blaue und 4 gelbe Kugeln.
Wie groß ist die Wahrscheinlichkeit, eine blaue Kugel zu ziehen?
Lösung:

$$\frac{3}{3+4} = \frac{3}{7}.$$

2.Beispiel:
Wie groß ist die Wahrscheinlichkeit für 6 Richtige beim Lotto "6 aus 49"?
Lösung:
$C(49,6) = 13983816$ ist Anzahl der Möglichkeiten 6 Zahlen aus 49 möglichen auszuwählen.
$\Rightarrow \frac{1}{C(49,6)} \approx 7.151123 * 10^{-8}$.

Satz 7.1

Sei E ein Ereignis aus der Menge S von gleichwahrscheinlichen Elementarereignissen. Die Wahrscheinlichkeit $p(\bar{E})$ des Komplementärereignisses berechnet sich durch

$$p(\bar{E}) = 1 - p(E).$$

Beweis:
Es gilt: $\bar{E} = S - E$.

$$\begin{aligned} \Rightarrow p(\bar{E}) = \frac{\#S - \#E}{\#S} &= 1 - \frac{\#E}{\#S} \\ &= 1 - p(E). \end{aligned}$$

□

Satz 7.2
Seien $E_1, E_2 \subseteq S$ Ereignisse aus einer Menge S von gleichwahrscheinlichen Elementarereignissen.
Dann gilt:

$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2).$$

Beweis:
Wegen

$$\#(E_1 \cup E_2) = \#(E_1) + \#(E_2) - \#(E_1 \cap E_2)$$

ergibt sich die Behauptung. □

Verlasse die Annahme, daß alle Elementarereignisse gleichwahrscheinlich sind:
Sei S eine Menge n von Elementarereignissen $x_1, \ldots x_n$.
Jedem Elementarereignis x_i sei die Wahrscheinlichkeit $p(x_i)$ mit folgenden Bedingungen zugeordnet:

(1) $0 \leq p(x_i) \leq 1$

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

Definition:
Die Wahrscheinlichkeit eines Ereignisses E ist die Summe der Wahrscheinlichkeiten aller Elementarereignisse $a_1, \ldots a_k$ in E:

$$p(E) = \sum_{i=1}^{k} p(a_i).$$

Beipiel:
Sei ein Würfel gegeben, der die sechs dreimal häufiger würfelt als die übrigen Zahlen.

Wie groß ist die Wahrscheinlichkeit eine durch drei teilbare Zahl zu würfeln?

Es gilt:

$$\begin{aligned} p(1) &= p(2) = p(3) = p(4) = p(5) = \frac{1}{8} \\ p(6) &= \frac{3}{8} \\ \Rightarrow p\{3,6\} &= \frac{1}{8} + \frac{3}{8} = \frac{1}{2}. \end{aligned}$$

Kombination von Ereignissen

Satz 7.3
Sei p eine Wahrscheinlichkeitsverteilung.

(1) $p(\bar{E}) = 1 - p(E)$.

(2) $p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$.

Beweis:

(1) $\sum_{i=1}^{n} p(x_i) = 1 = p(E) + p(\bar{E})$.
$\Rightarrow p(\bar{E}) = 1 - p(E)$.

(2) $P(E_1 \cup E_2)$ ist die Summe der Wahrscheinlichkeiten der Elementarereignisse $x \in E_1 \cup E_2$.
1.Fall: $x \in E_1 \cup E_2 \wedge x \notin E_1 \cap E_2$
$\Rightarrow p(x)$ wird auf der rechten Seite einmal gezählt.
2.Fall: $x \in E_1 \cup E_2 \wedge x \in E_1 \cap E_2$
$\Rightarrow p(x)$ wird in $p(E_1)$ und $p(E_2)$ zweimal gezählt und muß deshalb einmal abgezogen werden.

□

Bedingte Wahrscheinlichkeit

Definition:
Seien E, F Ereignisse mit $p(F) > 0$.
Die *bedingte Wahrscheinlichkeit von E unter F* ist definiert durch

$$p(E|F) = \frac{p(E \cap F)}{p(F)}.$$

$p(E|F)$ ist die Wahrscheinlichkeit dafür, daß E eintritt, falls F eingetreten ist.

Beispiel:
Wie groß ist die Wahrscheinlichkeit, daß ein zufällig erzeugtes 4–Bit Wort (alle 16 Worte seien gleich wahrscheinlich) mindestens zwei aufeinanderfolgende Nullen enthält, falls das erste Bit 0 ist.

Lösung:
E Ereignis, daß ein 4–Bit Wort mindestens zwei aufeinanderfolgende Nullen enthält.
F Ereignis, daß das erste Bit 0 ist.

$$\begin{aligned} p(E|F) &= \frac{p(E \cap F)}{p(F)} \\ E \cap F &= \{0000, 0001, 0011, 0010, 0100\} \\ p(E \cap F) &= \frac{5}{16} \\ p(F) &= \frac{8}{16} = \frac{1}{2} \\ \Rightarrow p(E|F) &= \frac{\frac{5}{16}}{\frac{1}{2}} = \frac{5}{8}. \end{aligned}$$

Unabhängigkeit

Definition:
Zwei Ereignisse E und F sind *unabhängig* genau dann, wenn

$$p(E \cap F) = p(E)\dot{p}(F).$$

Bemerkung:
E, F sind unabhängig $\Leftrightarrow p(E|F) = p(E)$.

Beispiel:
Seien alle vier Möglichkeiten der Geschlechtsverteilung der beiden Kinder einer vierköpfigen Familie gleichwahrscheinlich.
Sind die beiden folgenden Ereignisse unabhängig?

E Eine vierköpfige Familie hat zwei Jungen.
F Eine vierköpfige Familie hat mindestens einen Jungen.

Lösung:

$$\begin{aligned} p(E) &= \frac{1}{4}. \\ p(F) &= \frac{3}{4}. \end{aligned}$$

$$\begin{aligned} p(E \cap F) &= \frac{1}{4}. \\ \Rightarrow p(E \cap F) &= \frac{1}{4} \neq p(E)\dot{p}(F) = \frac{3}{16}. \end{aligned}$$

d.h. die Ereignisse sind nicht unabhägig.

Binomialverteilung

Betrachte:
Experimente mit zwei möglichen Ausgängen *(Erfolg, Fehler).*

Beispiel:
Münzwurf.

Sei p die Wahrscheinlichkeit für *Erfolg.*
Sei q die Wahrscheinlichkeit für *Fehler.*
$\Rightarrow 1 = p + q.$

Oft von Interesse:
Die Wahrscheinlichkeit des Erfolgs bei n unabhängigen Versuchen.

Beispiel:
Gegeben:
Eine Münze mit $\frac{2}{3}$ Wahrscheinlichkeit für Kopf und $\frac{1}{3}$ Wahrscheinlichkeit für Wappen.
Gesucht: Die Wahrscheinlichkeit dafür, daß bei sieben unabhängigen Würfen genau viermal Kopf erscheint.
Lösung:
Es gibt $2^7 = 128$ mögliche Ausgänge.
Davon sind genau $C(7,4)$ Kopf.
Da die Experimente unabhängig sind, ist die Wahrscheinlichkeit für solch einen Versuchsausgang

$$\left(\frac{2}{3}\right)^4 \left(\frac{1}{3}\right)^3.$$

$\Rightarrow$ Die Wahrscheinlichkeit ist

$$C(7,4)\left(\frac{2}{3}\right)^4 \left(\frac{1}{3}\right)^3 = \frac{560}{2187}.$$

Satz 7.4

Die Wahrscheinlichkeit dafür. bei n unabhängigen Versuchen mit Erfolgswahrscheinlichkeit p k Erfolge zu haben ist

$$C(n,k)p^k q^{n-k}.$$

Beweis:
Das Ergebnis der n Versuche ist der Vektor

$$(t_1, \ldots, t_n) \text{ mit } t_i = \begin{cases} E & \text{(Erfolg).} \\ F & \text{(Fehler).} \end{cases}$$

Die Wahrscheinlichkeit für einen Ergebnisvektor $(t_1, \ldots t_n)$ mit k mal E und $(n-k)$ mal F ist

$$p^k(1-p)^{n-k}.$$

Es gibt $C(n,k)$ Tupel mit $t_i = E$ für k verschiedene i.
$\Rightarrow$ Die gesuchte Wahrscheinlichkeit ist

$$C(n,k)\ p^k(1-p)^{n-k}.$$

□

Bezeichnung:

$b(k;n,p)$	Die Wahrscheinlichkeit dafür, von k Erfolgen bei n Versuchen mit Erfolgswahrscheinlichkeit p.
$b(k;n,p)$	$= C(n,k)\ p^k(1-p)^{n-k}$ (Binomialverteilung).

Bemerkung:

$$\sum_{k=0}^{n} C(n,k)\ p^k(1-p)^{n-k} = \quad 1 \quad = (p + (1-p))^n$$
$$= (p+q)^n$$

Zufallsvariable

Defintion:
Eine *Zufallsvariable* X ist eine reellwertige Funktion vom Raum der möglichen Ausgänge eines Experiments.

Beispiel:
Werfe Münze dreimal.
Sei X die Anzahl des Erscheinens von Kopf.
Losung:

$$\begin{aligned} X(KKK) &= 3, \\ X(KKW) = X(KWK) = X(WKK) &= 2, \\ X(KWW) = X(WKW) = X(WWK) &= 1, \\ X(WWW) &= 0. \end{aligned}$$

Erwartungswert

Definition:
Der *Erwartungswert* einer Zufallsvariable $X(S)$ auf dem Raum $S = \{s_1, \ldots s_n\}$ ist definiert durch

$$E(X) = \sum_{i=1}^{n} p(s_i) X(s_i).$$

Beipiel:
Der Erwartungswert der Erfolgszahlen bei n Experimenten mit zwei Ausgängen und Erfolgswahrscheinlichkeit p:
X sei die Zufallsvariable, die der Versuchsfolge die Zahl der Erfolge zuordnet.
Es gilt:

$$\begin{aligned} p(X = k) &= C(n,k)\, p^k (1-p)^{n-k} \\ E(X) &= \sum_{k=1}^{n} k\, p(X = k) \\ &= \sum_{k=1}^{n} k\, C(n,k)\, p^k (1-p)^{n-k} \\ &= \sum_{k=1}^{n} n\, C(n-1,k-1)\, p^k (1-p)^{n-k} \\ &= n \sum_{k=1}^{n} C(n-1,k-1)\, p^k (1-p)^{n-k} \\ &= n\, p \sum_{k=1}^{n} C(n-1,k-1)\, p^{k-1} (1-p)^{n-k} \end{aligned}$$

$$
\begin{aligned}
&= n\ p\ \sum_{j=0}^{n-1} C(n-1,j)\ p^j (1-p)^{n-1-j} \\
&= n\ p\ (p\ +\ (1-p))^{n-1} \\
&= n\ p.
\end{aligned}
$$

Average–Case Complexity

Die Berechnung der Average–case Komplexität eines Algorithmus kann als Berechnung der Erwartungswertes einer Zufallsvariable aufgefaßt werden:
Raum der Elementarereignisse : Menge der Inputs $a_j\ ,\ j = 1, \ldots, n$.
Die Zufallsvariable X ordnet a_j die Zahl der bei a_j auszuführenden Schritte zu.
Die Wahrscheinlichkeit $p(a_j)$ beschreibt die Wahrscheinlichkeit des Auftretens eines Inputs.
$\Rightarrow$

$$E(X) = \sum_{j=1}^{n} p(a_j)\ X(a_j)$$

ist die Average–Case Komplexität des Algorithmus.

Kapitel 8

Rekursionsrelationen

Beispiel:
Betrachte eine Kolonie von Bakterien:
Die Anzahl der Bakterien verdoppelt sich jede Stunde.
Wie viele Bakterien gibt es nach vier Stunden?

$$a_n = 2a_{n-1}.$$

Ausgangssituation: a_0
Z.B.: $a_5 = 7 \Rightarrow a_n$ eindeutig bestimmbar.

Definition:
Eine *Rekursionsrelation* für eine Folge $\{a_n\}$ ist eine Formel für a_n , $n \geq n_0$ in der die vorrausgegangenen Gliedern Folge: $a_0, \ldots a_{n-1}$ auftreten.
Die Folge heißt Lösung der Rekursionsrelation, falls alle Terme a_n , $n \geq n_0$ die Rekursionsrelation erfüllen.

Beipiel:
Sei $\{a_n\}$ eine Folge, die $a_n = a_{n-1} - a_{n-2}$ löst für $n = 2, 3$.
Sei $a_0 = 3$ und $a_1 = 5$.
$\Rightarrow \quad a_2 = a_1 - a_0 = 5 - 3 = 2,$
$\quad\quad a_3 = a_2 - a_1 = 2 - 5 = -3.$

Bemerkung:
Rekursionsrelation und Anfangsbedingung bestimmen die Folge eindeutig.
Rekursionsrelationen und Anfangsbedingung können somit zur rekursiven Definition von Folgen verwendet werden.

Beispiel:
Vermehrung von Kaninchen und Fibonacci–Zahlen:
Ein Kaninchenpaar wird nach der Geburt auf einer Insel ausgesetzt.
Wenn es zwei Monate alt ist erzeugt jedes Paar jeden Monat ein neues Pärchen.

Modellierung mit Rekursionsrelationen:
Sei f_n die Zahl der Kaninchenpärchen nach n Monaten.

$$\begin{aligned} f_1 &= 1 \\ f_2 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \end{aligned}$$

Die Folge f_n heißt *Fibonacci–Folge.*

Beispiel:
Gesucht wird die Rekursionsrelation und Anfangsbedingung für die Zahl der Bitstrings der Länge n ohne zwei aufeinanderfolgende Nullen.

Lösung:
Sei a_n die gesuchte Zahl der n–Bitstring.
a_{n-1} Zahl der $(n-1)$–Bitstrings, ohne zwei aufeinanderfolgende Nullen, die auf Null enden.
a_{n-2} Zahl der $(n-2)$–Bitstrings, ohne aufeinanderfolgende Nullen.
$\Rightarrow$

$$a_n = a_{n-1} + a_{n-2}. \quad (1)$$

Anfangsbedingungen:

$$\begin{aligned} a_1 &= 2, \\ a_2 &= 3. \end{aligned}$$

Bemerkung:
(1) stimmt mit der Rekursionsgleichung für Fibonacci–Zahlen überein und

$$\begin{aligned} a_1 &= f_3, \\ a_2 &= f_4, \end{aligned}$$

also

$$a_n = f_{n+2}.$$

Lösung von Rekursionsrelationen

Definition:
Eine lineare Rekursionsgleichung vom Grad k ist eine Relation der Form

$$a_n = c_1 a_{n-1} \ + \ c_2 a_{n-2} \ + \ \ldots \ + \ c_k a_{n-k}$$

wobei $c_1 \ldots c_k \in \mathbb{R}$, $c_k \neq 0$, $k = 1, \ldots, k$.

Bemerkung:
Eine lineare Rekursionsgleichung vom Grad k definiert eindeutig eine Folge $\{a_n\}$, falls k Anfangsbedingungen

$$\begin{aligned} a_0 &= c_0, \\ a_1 &= c_1, \\ &\vdots \\ a_{k-1} &= c_{k-1}. \end{aligned}$$

gegeben sind.

Beispiel:

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2}, \\ a_n &= a_{n-5}. \end{aligned}$$

Beispiel für eine nichtlineare Rekursionsgleichung:

$$a_n = a_{n-1} - a_{n-2}^2.$$

ist nicht linear!

Satz 8.1
Seien $c_1, c_2 \in \mathbb{R}$ und habe $r^2 - c_1 r - c_2 = 0$ zwei verschiedene Lösungen r_1, r_2.
Dann gilt:
$\{a_n\}$ ist genau dann Lösung der Rekursionsrelation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ (*), wenn für geeignete $\alpha_1, \alpha_2 \in \mathbb{R}$ gilt:

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n \text{ für alle } n.$$

Beweis:
$(\leftarrow)$:
Sei $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$
Da r_i Lösung von $r^2 - c_1 r - c_2 = 0$ ist, gilt:

$$\begin{aligned} r_1^2 &= c_1 r_1 + c_2 \\ r_2^2 &= c_1 r_2 + c_2 \end{aligned}$$

$$\Rightarrow c_1 a_{n-1} + c_2 a_{n-2} = c_1(\alpha_1 r_1^{n-1} + \alpha_2 r_2^{n-1}) + c_2(\alpha_1 r_1^{n-2} + \alpha_2 r_2^{n-2})$$

$$
\begin{aligned}
&= \alpha_1 r_1^{n-2}(c_1 r_1 + c_2) + \alpha_2 r_2^{n-2}(c_1 r_2 + c_2) \\
&= \alpha_1 r_1^{n-2} r_1^2 + \alpha_2 r_2^{n-2} r_2^2 \\
&= \alpha_1 r_1^n + \alpha_2 r_2^n \\
&= a_n.
\end{aligned}
$$

d.h. $\{a_n\}$ ist Lösung von (*).

$(\rightarrow)$:
Sei $\{a_n\}$ die Lösung von (*) mit den Anfangsbedingungen:

$$
\begin{aligned}
a_0 &= c_0, \\
a_1 &= c_1.
\end{aligned}
$$

Sei

$$
\begin{aligned}
\alpha_1 &= \frac{c_1 - c_0 r_2}{r_1 - r_2}, \\
\alpha_2 &= \frac{c_0 r_1 - c_1}{r_1 - r_2}.
\end{aligned}
$$

Wir zeigen durch vollständige Induktion, dass damit

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

gilt.
$n = 0$:

$$a_0 = c_0 = \frac{c_1 - c_0 r_2}{r_1 - r_2} + \frac{c_0 r_1 - c_1}{r_1 - r_2} = \alpha_1 r_1^0 + \alpha_2 r_2^0.$$

$n = 1$:

$$a_1 = c_1 = \frac{c_1 r_1 - c_0 r_1 r_2}{r_1 - r_2} + \frac{c_0 r_1 r_2 - c_1 r_2}{r_1 - r_2} = \alpha_1 r_1^1 + \alpha_2 r_2^1.$$

$\{n-2, n-1\} \rightarrow n$:

$$
\begin{aligned}
& a_n \\
= \; & c_1 a_{n-1} + c_2 a_{n-2} && \text{(da } (a_n) \text{ die Rekursionsgleichung erfüllt)} \\
= \; & c_1(\alpha_1 r_1^{n-1} + \alpha_2 r_2^{n-1}) + c_2(\alpha_1 r_1^{n-2} + \alpha_2 r_2^{n-2}) && \text{(nach Induktionsvorraussetzung)} \\
= \; & \alpha_1 r_1^{n-2}(c_1 r_1 + c_2) + \alpha_2 r_2^{n-2}(c_1 r_2 + c_2) \\
= \; & \alpha_1 r_1^{n-2} r_1^2 + \alpha_2 r_2^{n-2} r_2^2 && \text{(da } r_i^2 = c_1 r_i + c_2 \text{ ist)} \\
= \; & \alpha_1 r_1^n + \alpha_2 r_2^n.
\end{aligned}
$$

□

Beispiel:

$$a_n = a_{n-1} + 2a_{n-2}$$

mit

$$\begin{aligned} a_0 &= 2, \\ a_1 &= 7. \end{aligned}$$

Lösung:
Betrachte die charakteristische Gleichung der Rekursionsrelation:

$$r^2 - r - 2 = 0.$$

$$\begin{aligned} \Rightarrow r_1 &= 2, \\ r_2 &= -1. \end{aligned}$$

$$\Rightarrow a_n = \alpha_1 2^n + \alpha_2 (-1)^n.$$

Wegen

$$\begin{aligned} a_0 &= 2 = \alpha_1 + \alpha_2, \\ a_1 &= 7 = \alpha_1 2 + \alpha_2 (-1) \end{aligned}$$

folgt

$$\alpha_1 = 3, \alpha_2 = -1,$$

also

$$a_n = 3 \cdot 2^n - (-1)^n.$$

Beispiel:
Fibonacci $\rightarrow$ Übung.

Satz 8.2
Seien $c_1, c_2 \in \mathbb{R}$ und habe $r^2 - c_1 r - c_2 = 0$ nur eine Wurzel r_0.
$\{a_n\}$ ist genau dann Lösung von $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, wenn für geeignete $\alpha_1, \alpha_2 \in \mathbb{R}$ gilt:

$$a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n \text{ für alle } n.$$

Beweis:
Übung. □

Teile- und Herrsche–Relationen

Satz 8.3
Sei $f(n) = af(\frac{n}{b}) + c$, *wobei* $b|n$, $a \geq 1$, $c \in \mathbb{R}^+$.
Dann gilt:

$$f(n) = \begin{cases} O(n^{\log_b a}) & : \quad a > 1. \\ O(\log n) & : \quad a = 1. \end{cases}$$

Beweis:
Übung. □

Satz 8.4
Sei $f(n) = a\ f(\frac{n}{b}) + cn^d$, *wobei* $n = b^k$, $a \geq 1$, $b \in \mathbb{N}$, $b \geq 1$, $c, d \in \mathbb{R}^+$.
Dann gilt:

$$f(n) = \begin{cases} O(n^d) & : \quad a < b^d. \\ O(n^d \log n) & : \quad a = b^d. \\ O(n^{\log_b a}) & : \quad a > b^d. \end{cases}$$

Beweis:
Vorlesung Info II. □

Teil III

Strukturen

Kapitel 9

Boolesche Algebren

Ziel: Rechnen mit Bits. (Datendarstellung in Computern, digitale SK)

George Boole: The Laws of Thought (1854).

9.1 Boolesche Funktionen und Ausdrücke

n–stellige Boolesche Funktion: Funktion der Gestalt

$$f : \{0,1\}^n \to \{0,1\}.$$

Einfache Fälle:
$(n = 1)$
Beispiel:

- $f(b) = \bar{b}$ Boolesches Komplement,
  $\bar{0} = 1$, $\bar{1} = 0$.

$(n = 2)$
Beispiel:

- $f(b_1, b_2) = b_1 \cdot b_2$ Boolesches Produkt,
  $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$
- $f(b_1, b_2) = b_1 + b_2$ Boolesche Summe,
  $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1 + 1 = 1$.

Unbestimmte, die Werte aus B annehmen können, heißen Boolesche Variable.

Seien $x_1, \ldots x_n$ Boolesche Variable.
Definiere Booleschen Ausdruck:

- $0, 1, x_1, \ldots, x_n$ sind Boolesche Ausdrücke.

– sind E_1, E_2 Boolesche Ausdrücke, so sind auch $\bar{E}_1, (E_1 E_2), (E_1 + E_2)$ Boolesche Ausdrücke.

Beispiel:
$E_1 = x_1 \cdot x_2 + \overline{(x_2 + 1)}$.

Jeder Boolesche Ausdruck repräsentiert eine Boolesche Funktion:
$f(b_1, \ldots, b_n) =$ Wert von E nach Substitution $x_i \to b_i$,
für alle in E vorhandenen Variablen.

Beispiel: (s.o.)
$f(1,0) = 1 \cdot 0 + \overline{(0+1)} = 0 + \bar{1} = 0 + 0 = 0$.

Wertetafel von f:

b_1	b_2	$f(b_1, b_2)$
0	0	0
0	1	0
1	0	0
1	1	1

auch geschrieben als $f(x_1, x_2) = x_1 \cdot x_2 + \overline{(x_2 + 1)}$.

Beobachtung:
Werden F_1, F_2 durch E_1, E_2 repräsentiert, so wird nach Definition

$$\begin{aligned} \bar{F}_1 : (b_1, \ldots b_n) &\to \overline{F_1(b_1, \ldots, b_n)} \quad \text{durch} \quad \bar{E}_1, \\ F_1 \cdot F_2 : (b_1, \ldots, b_n) &\to F_1(b_1, \ldots, b_n) \cdot F_2(b_1, \ldots, b_n) \quad \text{durch} \quad (E_1 \cdot E_2), \\ \text{und } F_1 + F_2 : (b_1, \ldots, b_n) &\to F_1(b_1, \ldots, b_n) + F_2(b_1, \ldots, b_n) \quad \text{durch} \quad (E_1 + E_2) \end{aligned}$$

repräsentiert.

9.2 Boolesche Äquivalenzen

Definition:
E_1, E_2 heißen äquivalent, falls sie die gleiche Boolesche Formel repräsentieren.

Beispiel:
E_1 ist äquivalent zu $E_2 = x_1 \cdot x_2$.

Schreibweise:
$E_1 = E_2$.

Wichtige Beispiele:

$\bar{\bar{x}} = x$	Doppelte Komplementierung
$x + x = x \ , \ x \cdot x = x$	Idempotenz
$x + 0 = x \ , \ x \cdot 1 = x$	Identitätsgesetze
$x + 1 = 1 \ , \ x \cdot 0 = 0$	Dominanz
$x + y = y + x \ , \ x \cdot y = y \cdot x$	Kommutativität
$x + (y + z) = (x + y) + z \ , \ x \cdot (y \cdot z) = (x \cdot y) \cdot z$	Assoziativität
$x + yz = (x + y)(x + z) \ , \ x(y + z) = xy + xz$	Distrbutivität
$\overline{(x \cdot y)} = \bar{x} + \bar{y} \ , \ \overline{(x + y)} = \bar{x} \cdot \bar{y}$	DeMorgansche Regeln
$x \cdot \bar{x} = 0 \ , \ x + \bar{x} = 1$	Komplementgesetze

Beweis:
Z.B.: über Wertetafel.
Beispiel:

$\overline{(x \cdot y)} = \bar{x} + \bar{y}$

x	y	$x \cdot y$	$\overline{(x \cdot y)}$	$\bar{x}$	$\bar{y}$	$\bar{x} + \bar{y}$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Beweis der anderen: Übungsaufgabe. □

Ableitung weitere Äquivalenzen wie in der Ausagenlogik möglich.

Beispiel:
Absorbtionsgesetz:

$$x(x + y) = x.$$

Beweis:

$$\begin{array}{lcll} x(x+y) & = & (x+0)(x+y) & \text{Identität} \\ & = & x + 0 \cdot y & \text{Distributivität} \\ & = & x + y \cdot 0 & \text{Dominanz} \\ & = & x. & \text{Identität} \end{array}$$

□

Boolesche Äquivalenzen haben eine große Bedeutung beim Schaltungsentwurf. Ein weiteres Hilfsmittel zur Ableitung von Booleschen Äquivalenzen:

Dualität

Definition:
Der *duale Ausdruck* E^D zu einem Booleschen Ausdruck E entsteht aus E durch Vertauschen von 0 und 1, sowie $\cdot$ und $+$ an allen Stellen in E.

Beispiel: $E = ((x + (y \cdot z)) + 0) \rightarrow E^D = ((x \cdot (y + z)) \cdot 1)$

Definition:
Die duale Funktion F^D zur Booleschen Funktion F ist definiert durch

$$F^D(b_1, \ldots b_n) = \overline{F(\bar{b_1}, \ldots, \bar{b_n})}.$$

Beispiel:
$F(b_1, b_2) = b_1 + b_2$, $F^D(b_1, b_2) = \bar{b_1} \cdot \bar{b_2}$.

Satz 9.1
Werde die Boolesche Funktion F durch den Booleschen Ausdruck E repräsentiert. Dann wird F^D durch E^D repräsentiert.

Beweis:
IA:

- $E = b \in \{0, 1\}$
  $\Rightarrow F$ konstant b
  $\Rightarrow F^D$ konstant $\bar{b} = E^D$.

- $E = x_i$
  $\Rightarrow E^D = x_i$
  $\Rightarrow F(b_1, \ldots, b_n) = b_i$
  $\Rightarrow F^D(b_1, \ldots, b_n) = \overline{F(\bar{b_1}, \ldots, \bar{b_n})} = \bar{\bar{b_i}}$
  $\Rightarrow F = F^D$ (selbstdual).

IV:
Gelte die Aussage für Boolesche Ausdrücke E_1, E_2 und die durch sie repräsentierten Funktionen F_1, F_2.

IS:
Aussage gilt auch für

- $\bar{E_1} : \bar{F_1}^D$ wir durch $\bar{E_1}^D$ repräsentiert (Übungsaufgabe).

– $(E_1 \cdot E_2) : (E_1 \cdot E_2)^D = (E_1^D + E_2^D)$ repräsentiert nach Vorraussetzung
$F_1^D + F_2^D : (b_1, \ldots, b_n) \to \overline{F_1^D(b_1, \ldots, b_n)} + F_2^D(b_1, \ldots, b_n)$
$= \overline{F_1(\bar{b_1}, \ldots, \bar{b_n}) + F_2(\bar{b_1}, \ldots, \bar{b_n})}$
$= \overline{F_1(\bar{b_1}, \ldots, \bar{b_n})} \cdot \overline{F_2(\bar{b_1}, \ldots, \bar{b_n})}$
$= (F_1 \cdot F_2)^D$.

– $(E_1 + E_2)$: analog.

□

Folgerung: (Dualitätsprinzip)
Sind die Booleschen Ausdrücke E_1 und E_2 äquivalent, dann sind auch E_1^D, E_2^D äquivalent.

Beispiel:
$x(x + y)x$ Absorbtionsgesetz
$\Rightarrow x + (x \cdot y) = x$ Absorbtionsgesetz.

9.3 Boolesche Algebren

Sei $\mathcal{B}$ eine nichtleere Menge und $\sqcup, \sqcap : \mathcal{B} \times \mathcal{B} \to \mathcal{B}$ eine *zweistellige Operation auf* $\mathcal{B}$ und $' : \mathcal{B} \to \mathcal{B}$ *einstellige Operation auf* $\mathcal{B}$.

Schreibweise:
z.B.:

$$\begin{aligned} \sqcup(a, b) &=: a \sqcup b, \\ '(a) &=: a'. \end{aligned}$$

Definition:
Die Struktur $(\mathcal{B}; 0, 1; \sqcup, \sqcap, ')$ heißt *Boolesche Algebra*, falls für alle $a, b, c \in \mathcal{B}$ gilt:

(1) $0, 1 \in \mathcal{B}, 0 \neq 1$.

(2) $\sqcap$ und $\sqcup$ sind kommutativ und assoziativ.

(3) $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$,
$a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$.

(4) $a \sqcap (a \sqcup b) = a$,
$a \sqcup (a \sqcap b) = a$.

(5) $(a')' = a$.

(6) $a \sqcap 0 = 0$,
$a \sqcup 0 = a$,
$a \sqcap 1 = a$,
$a \sqcup 1 = 1$.

(7) $a \sqcap a' = 0$,
$a \sqcup a' = 1$.

Satz 9.2
Die folgenden Strukturen sind Boolesche Algebren:

(1) $B = (\{0,1\}; 0, 1; \cdot, +, \bar{})$.

(2) $L = (\{F, W\}; F, W; \wedge, \vee, \neg)$.

(3) $n \in \mathbb{N}_+$, $B^n = (\{0,1\}^n; 0, 1; \cdot, +, \bar{})$.
(Operationen komponentenweise definiert)

(4) $A \neq \emptyset$, $\mathcal{P}(A) = (2^A; \emptyset, A; \cap, \cup, \bar{})$.

(5) $\mathbb{B}_n = (B_n; 0, 1; \cdot, +, \bar{})$,
wobei $B_n = \{f | f : \{0,1\}^n \to \{0,1\}\}$.
(Operationen punktweise definiert)

Beweis:
Übungsaufgabe. □

Satz: (ohne Beweis)
Zwei endliche Boolesche Algebren sind *isomorph* (d.h. im wesentlichen gleich), wenn sie die gleiche Kardinalität haben.
⇒ Die Aussagenlogik kann auf der Mengenlehre aufgebaut werden und umgekehrt.

Darstellung Boolescher Funktionen
Normalformen

Beispiel:
Gesucht: Ein Boolescher Ausdruck, der die Funktion f mit

x_1	x_2	f
0	0	1
0	1	0
1	0	0
1	1	1

repräsentiert.

f nimmt den Wert 1 nur auf $(0,0)$ und $(1,1)$ an.
⇒ f wird repräsentiert durch $\bar{x_1}\bar{x_2} + x_1 x_2$.

Definition:
Sei $b = (b_1, \ldots, b_n) \in \{0,1\}$.

Der Ausdruck $x_1^{b_1} \cdots x_n^{b_n}$
mit $x_i^{b_i} = \begin{cases} x_i & \text{, falls } b_i = 1 \\ \bar{x}_i & \text{, sonst} \end{cases}$ heißt Minterm von b.
(Kurzschreibweise: x^b , falls $x = (x_1, \ldots, x_n)$ fixiert.

Für die durch den Minterm x^b repräsentierte Funktion $f : \{0,1\}^n \to \{0,1\}$ gilt

$$f(a) = \begin{cases} 1 & \text{, falls } a = (a_1, \ldots a_n) = b \\ 0 & \text{, sonst.} \end{cases}$$

(durch Einsetzen)

Sei $f : \{0,1\}^n \to \{0,1\}$ beliebig und seien $a^1, \ldots, a^t \in \{0,1\}^n$ die Binärtupel, auf denen f den Wert 1 annimmt.
Dann wird f durch den Booleschen Ausdruck $x^{a^1} + \ldots + x^{a^t}$ repräsentiert.

Beweis:
Durch Einsetzen. □

Der obige Ausdruck heißt kanonische Disjunktive Normalform von f (kDNF).

Allgemein wird eine Boolesche Summe von Booleschen Produkten von Literalen Disjunktive Normalform genannt.

⇒

Satz 9.3

Jede Boolesche Formel wir durch einen Booleschen Ausdruck (sogar in DNF) repräsentiert.

Boolesche Produkte von Booleschen Summen von Literalen werden konjunktive Normalform (KNF) genannt.

Satz 9.4

Jede Boolesche Formel wird durch eine KNF repräsentiert.

Beweis:
Übungsaufgabe. □

Funktionale Vollständigkeit
Wie gezeigt, läßt sich jede Boolesche Formel durch Variablen und Boolesche Operationen $\cdot, +$ und $^-$ darstellen (z.B. durch DNF).

$\Rightarrow$ Wir sagen, die Menge $\{\cdot, +, \bar{}\}$ ist funktional vollständig.

Gibt es kleinere funktional vollständige Mengen?
Ja! Wir können z.B. $\cdot$ eliminieren: $E_1 \cdot E_2 = \overline{(\bar{E}_1 + \bar{E}_2)}$

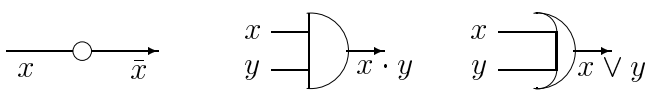
Die Menge $(+, \bar{})$ ist funktional vollständig.
Die Menge $(\cdot, +)$ ist nicht funktional vollständig!
Zum Beispiel kann die Funktion $f(b_1) = \bar{b_1}$ nicht allein durch Variablen, $\cdot$ und $+$ dargestellt werden.
(Übungsaufgabe)

Beispiel für einelementige funktional vollständige Mengen:
$x_1|x_2 = \mathrm{NAND}(x_1, x_2) := \overline{x_1 x_2}$. (analog NOR)
$\{|\}$ ist funktional vollständig.
Es genügt zu zeigen, daß $\bar{}$ und $+$ durch NAND "*simuliert* werden können.

$$\bar{E}_1 = E_1|E_1 \ , \ E_1 + E_2 = (E_1|E_1)|(E_2|E_2).$$

Kombinatorische Schaltkreise

Boolesche Operationen lassen sich technisch durch *Gatter* (Schaltglieder) realisieren, die z.B. auf Transistoren aufgebaut sind.
Kreisfreie Zusammenschaltungen solcher Gatter heißen kombinatorische Schaltkreise.
Symbole:

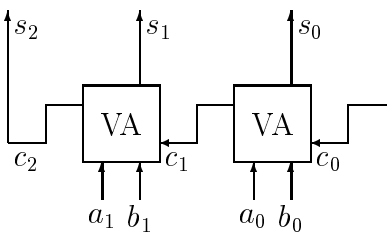


Inverter AND–Gatter OR–Gatter

Entwurf eines einfachen Additionsschaltkreises für 2–Bit–Zahlen:
Prinzip:

$$\begin{aligned} (a_1, a_0) &= a = 2a_1 + a_0. \\ (b_1, b_0) &= b = 2b_1 + b_0. \\ a : b = s \ : \ (s_2, s_1, s_0) &= s = 4s_2 + 2s_1 + s_0. \end{aligned}$$

Blockschaltbild der Schulmethode:



Verallgemeinerung:
n Volladdierer ergeben einen Additionschaltkreis für n–Bit–Zahlen. (Ripple–Carry–Adder)

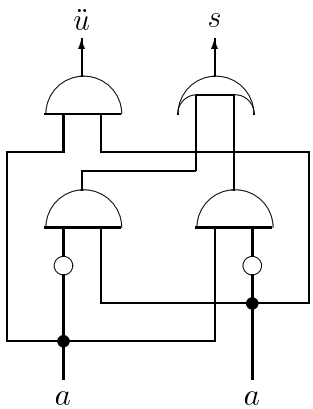
Volladdierer:
3 Eingänge $i_1, i_0, c \in B$.
2 Ausgänge $o_1, o_0 \in B$.
Spezifikation: $i_1 + i_0 + c = 2o_1 + o_0$.

Entwerfen zunächst Halbaddierer:

Halbaddierer

2 Eingabe:	a, b.
2 Ausgänge:	$s, \ddot{u}$.
Spezifikation:	$\ddot{u} = a + b$
	$s = \bar{a} \cdot b + a \cdot \bar{b} = a + b \ mod\ 2$.

$\Rightarrow$ Realisierungsmöglichkeit für HA:

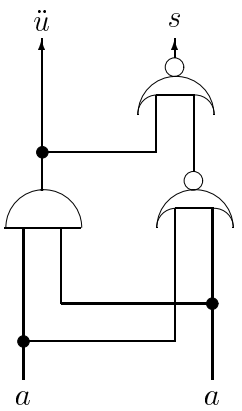


Vereinfachung mittels Boolescher Äquivalenzen:

$$s = \bar{a}b + a\bar{b} \quad = \quad (\bar{a}b + a)(\bar{a}b + \bar{b}$$

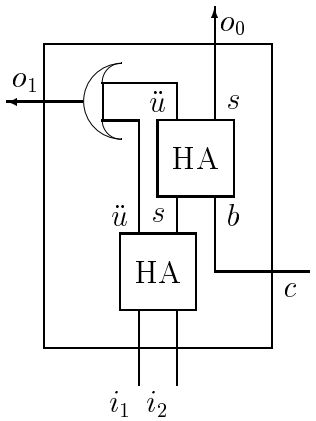
$$
\begin{aligned}
&= (a+b)(\bar{a}+\bar{b} \\
&= \overline{\overline{(a+b)}+ab} = NOR(NOR(a,b), \underbrace{ab}_{\ddot{u}})
\end{aligned}
$$

$\Rightarrow$ Realisierung mit weniger Gattern:



NOR–Gatter sind technisch einfach zu realisieren.

Aufbau des Volladdieres auf dem Halbaddierer:
Blockschaltbild:



Übertrag o_0 entsteht, wenn $a = b = 1$ oder $a + b = 1$ und $c = 1$.

Kapitel 10

Aussagenlogik

Seien $A_1, A_2, \ldots$ die atomaren Sprachgebilde (Formeln).

Definition: (Syntax der Aussagenlogik)
Eine *atomare Formel* hat die Form A_i , $(i = 1, 2, \ldots)$.
Formeln sind induktiv definiert durch:

(1) Alle atomaren Formeln sind Formeln.

(2) Sind F, G Formeln, so auch $(F \wedge G)$ und $(F \vee G)$.

(3) Ist F Formel, so auch $\neg F$.

Bezeichnung:

$\neg F$	*Negation* von F.
$(F \wedge G)$	*Konjunktion* von F und G.
$(F \vee G)$	*Disjuktion* von F und G.

Eine Formel F, die als Teil der Formel G auftriit heißt *Teilformel* von G.

Beispiel:
$F = ((A_1 \wedge A_7) \vee (A_6 \vee \neg A_2))$.
Teilformeln:
$F, (A_1 \wedge A_7), A_1, A_7, (A_6 \vee \neg A_2), \neg A_2, A_2, A_6$.

Abkürzende Schreibweise:

A, B, C	anstelle von	A_1, A_2, A_3.
$(F_1 \to F_2)$	anstelle von	$(\neg F_1 \vee F_2)$.
$(F_1 \leftrightarrow F_2)$	anstelle von	$(F_1 \wedge F_2) \vee (\neg F_1 \wedge \neg F_2)$.
$(\bigvee_{i=1}^{n} F_i)$	anstelle von	$(\ldots((F_1 \vee F_2) \vee F_3) \vee \ldots) \vee F_n)$.
$(\bigwedge_{i=1}^{n} F_i)$	anstelle von	$(\ldots((F_1 \wedge F_2) \wedge F_3) \wedge \ldots) \wedge F_n)$.

Bisher haben Formeln keine Bedeutung (Inhalt).
Sie sind lediglich Zeichenreihen (*syntaktische* Objekte).

Definition: (Semantik der Aussagenlogik)
Die Elemente aus $\{0,1\}$ heißen *Wahrheitswerte*.
Sei $D \subseteq \{A_1, A_2 \ldots : A_i \text{ atomare Formel }\}$.
$\mathcal{A} : D \to \{0,1\}$ heißt *Belegung*.
Sei $[D]$ die Menge aller Formeln, die nur aus den atomaren Formeln aus D aufgebaut sind.
Erweiterung von $\mathcal{A}$ zur Funktion $\tilde{\mathcal{A}} : [D] \to \{0,1\}$, wobei $\tilde{\mathcal{A}}(A)$ für ein $A \in [D]$ definiert ist, als

(1) Fall: $A \in D$.
$\tilde{\mathcal{A}}(A) := \mathcal{A}(A)$.

(2) Fall: $A = F \wedge G$.

$$\tilde{\mathcal{A}}(A) = \begin{cases} 1 & \text{falls } \tilde{\mathcal{A}}(F) = 1 \text{ und } \tilde{\mathcal{A}}(G) = 1. \\ 0 & \text{sonst.} \end{cases}$$

(3) Fall: $A = F \vee G$.

$$\tilde{\mathcal{A}}(A) = \begin{cases} 1 & \text{falls } \tilde{\mathcal{A}}(F) = 1 \text{ oder } \tilde{\mathcal{A}}(G) = 1. \\ 0 & \text{sonst.} \end{cases}$$

(4) Fall: $A \notin D$, $A \neq F \wedge G$, $A \neq F \vee G$.
$\Rightarrow A = \neg F$.

$$\tilde{\mathcal{A}}(A) = \begin{cases} 1 & \text{falls } \tilde{\mathcal{A}}(F) = 0. \\ 0 & \text{sonst} \end{cases}$$

Definition:
Belegte Formeln heißen *Aussagen*.

Bezeichnung:

(1) Schreiben anstelle von $\tilde{\mathcal{A}}$ wieder A.

(2) Die Definition von $\mathcal{A}(F \wedge G)$, $\mathcal{A}(F \vee G)$, $\mathcal{A}(\neg F)$ macht deutlich, daß $\wedge$ "und", $\vee$ "oder", $\neg$ "nicht" bedeutet.
$\rightarrow$ beutet "impliziert" , $\Leftrightarrow$ bedeutet "genau dann, wenn.".

Beispiel:
$\mathcal{A}(A) = 1$, $\mathcal{A}(B) = 1$, $\mathcal{A}(C) = 0$.
Dann gilt:

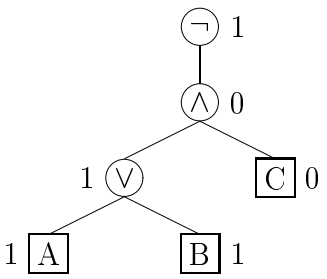
$$\begin{aligned} \mathcal{A}(\neg((A \wedge B) \vee C)) &= \begin{cases} 1 & \text{falls } \mathcal{A}((A \wedge B) \vee C) = 0 \\ 0 & \text{sonst} \end{cases} \\ &= \begin{cases} 0 & \text{falls } \mathcal{A}((A \wedge B) \vee C) = 1 \\ 1 & \text{sonst} \end{cases} \end{aligned}$$

$$
\begin{aligned}
&= \begin{cases} 0 & \text{falls } \mathcal{A}(A \wedge B) = 1 \text{ oder } \mathcal{A}(C) = 1 \\ 1 & \text{sonst} \end{cases} \\
&= \begin{cases} 0 & \text{falls } \mathcal{A}(A \wedge B) = 1 \text{ (da } \mathcal{A}(C) = 1) \\ 1 & \text{sonst} \end{cases} \\
&= \begin{cases} 0 & \text{falls } \mathcal{A}(A) = 1 \text{ und } \mathcal{A}(B) = 1 \\ 1 & \text{sonst} \end{cases} \\
&= 0
\end{aligned}
$$

Die Wirkung der Operatoren $\wedge, \vee, \neg$ kann durch "Wahrheitstafeln" deutlich gemacht werden:

$\mathcal{A}(F)$	$\mathcal{A}(G)$	$\mathcal{A}(F \wedge G)$
0	0	0
0	1	0
1	0	0
1	1	1

Graphische Darstellung von Formeln:
Beispiel: $\neg((A \vee B) \wedge C)$.
$\mathcal{A}(A) = 1$, $\mathcal{A}(B) = 1$, $\mathcal{A}(C) = 0$



Die induktive Definition von $\mathcal{A}(F)$ orientiert sich an der üblichen Definition einer Formel. Die Induktionprinzip kann auch bei Beweisen verwendet mwerden.

Man zeigt, daß eine Behauptung $B(F)$ für jede Formel F gilt, indem man

(1) zeigt, daß $B(F)$ für alle atomaren Formeln A_i gilt.

(2) zeigt, daß die Richtigkeit von
$B(F)$ und $B(G)$ die Richtigkeit von $B(\neg F)$, $B(F \wedge G)$, $B(F \vee G)$ impliziert.

Definition: (Zu F passende Belegung, Modell)
Sei F eine Formel.
Eine Belegung $\mathcal{A}$ heißt *zu F passend*, falls $\mathcal{A}$ für alle in F vorkommenden atomaren

Formeln definiert ist.
Eine Belegung $\mathcal{A}$ heißt *Modell* für F (F *gilt unter der Belegung* $\mathcal{A}$), falls $\mathcal{A}$ zu F passend ist und $\mathcal{A}(F) = 1$.

Bezeichnung:
$A \models F$.

Definition:
Eine Belegung $\mathcal{A}$ ist kein *Modell* für F (F *gilt nicht unter der Belegung* $\mathcal{A}$), falls $\mathcal{A}$ zu F passend ist und $\mathcal{A}(F) = 0$.

Bezeichnung:
$A \not\models F$.

Beispiel:
$F = ((A \vee B) \to C)$.
Sei $\mathcal{A}_1(A) = 0$, $\mathcal{A}_1(B) = 1$, $\mathcal{A}_1(C) = 0$

$$\begin{aligned} \Rightarrow \mathcal{A}_1(F) &= \begin{cases} 1 & \text{falls } \mathcal{A}_1(\neg(A \vee B)) = 1 \text{ oder } \mathcal{A}_1(C) = 1 \\ 0 & \text{sonst} \end{cases} \\ &= \begin{cases} 1 & \text{falls } \mathcal{A}_1((A \vee B)) = 0 \text{ oder } \mathcal{A}_1(C) = 1 \\ 0 & \text{sonst} \end{cases} \\ &= 0 \end{aligned}$$

(d.h. $\mathcal{A}_1$ ist kein Modell für F.)

Sei $\mathcal{A}_2(A) = 0$, $\mathcal{A}_2(B) = 0$, $\mathcal{A}_2(C) = 1$.
$\Rightarrow \mathcal{A}_2(F) = 1$.
(d.h $\mathcal{A}_2$ ist ein Modell für F.)

Definition:
Eine Formel F heißt *erfüllbar*, falls es (mindestens) ein Modell für F gibt.

Beispiel:
Die Formel aus dem letzten Beispiel war erfüllbar.

Definition:
Eine Menge M von Formeln heißt erfüllbar, falls es eine Belegung $\mathcal{A}$ gibt mit $\mathcal{A} \models F$ für alle $F \in M$.

Satz 10.1
Sei $M = \{F_1, \ldots F_k\}$ *eine Menge von Formeln.*
M *heißt genau dann erfüllbar, wenn* $(\bigwedge_{i=1}^{k} F_i)$ *erfüllbar ist.*

Beweis:
($\rightarrow$):
M ist erfüllbar.
$\Rightarrow$ Es gibt ein Modell $\mathcal{A}$ mit $\mathcal{A}(F_i) = 1$ für alle $i = 1, \ldots, k$.
$\Rightarrow \mathcal{A}(\bigwedge_{i=1}^{k} F_i) = 1$.
$\Rightarrow (\bigwedge_{i=1}^{k} F_i)$ ist erfüllbar. □

Definition:
Eine Formel F heißt *gültig*, falls jede zu F passende Belegung ein Modell für F ist.

Bezeichnung:
$\models F$.

Beispiel:

(1) $F = (A \vee \neg A)$.
Sei $\mathcal{A}$ eine zu F passende Belegung.
$\Rightarrow \mathcal{A}(A)$ ist definiert.
Sei $\mathcal{A}(A) = \delta$, $\delta \in \{0, 1\}$
$\Rightarrow \mathcal{A}(\neg A) = \bar{\delta}$ mit $\bar{\delta} = \begin{cases} 1 & \text{falls} \quad \delta = 0. \\ 0 & \text{sonst.} \end{cases}$
$\Rightarrow \mathcal{A}(A \vee \neg A) = \begin{cases} 1 & \text{falls} \quad \mathcal{A}(A) = 1 \text{ oder } \mathcal{A}(\neg A) = 1. \\ 0 & \text{sonst.} \end{cases}$

(2) $((A \wedge (A \rightarrow B)) \rightarrow B)$ (Wahrheitstafel !)

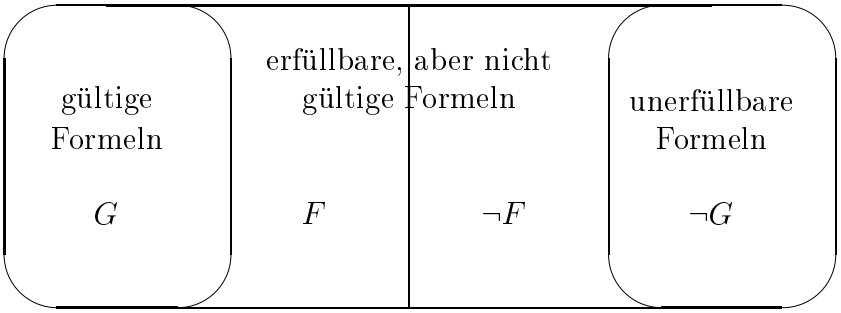
Definition:
F heißt unerfüllbar (oder F ist Kontradiktion), falls F in keinem zu F passenden Modell erfüllbar ist.

Beispiel:
$F = (A \wedge \neg A)$. (Übungsaufgabe)

Satz 10.2
Eine Formel F ist genau dann gültig, wenn $\neg F$ unerfüllbar ist.

Beweis:
Es gilt: F ist Tautologie.
$\Leftrightarrow$ jede zu F passenden Belegung ist Modell für F.
$\Leftrightarrow$ jede zu F und damit auch zu $\neg F$ passende Belegung kein Modell für $\neg F$ ist.
$\Leftrightarrow \neg F$ besitzt kein Modell.
$\Leftrightarrow \neg F$ ist unerfüllbar. □

Die aussagenlogischen Formeln:



Definition:
Eine Formel G heißt Folgerung der Formeln $F_1, \ldots, F_k$, falls für jede zu $F_1, \ldots, F_k$ und G passende Belegung $\mathcal{A}$ gilt:
Ist $\mathcal{A}$ Modell von $\{F_1, \ldots, F_k\}$ so auch für G.

Satz 10.3
Die folgenden drei Aussagen sind äquivalent.

(1) G *ist Folgerung von* $F_1, \ldots, F_k$.

(2) $((\bigwedge_{i=1}^{k} F_i) \to G)$ *ist eine Tautologie.*

(3) $((\bigwedge_{i=1}^{k} F_i) \wedge \neg G)$ *ist unerfüllbar.*

Beweis:
Übungsaufgabe. □

Der Wahrheitswert einer Formel F hängt nur vom Wahrheitswert der in F vorkommenden atomaren Formeln ab.

Satz 10.4
Sei F *eine Formel und seien* $\mathcal{A}, \mathcal{A}'$ *zwei zu* F *passende Belegungen, die in den atomaren Formeln von* F *übereinstimmen.*
Dann gilt:

$$\mathcal{A}(F) = \mathcal{A}'(F).$$

Beweis: (Induktion über den Formelaufbau)

(1) Sei F atomare Formel $\Rightarrow \mathcal{A}(F) = \mathcal{A}'(F)$ nach Vorraussetzung.

(2) Sei die Behauptung für die Formeln G und H bereits bewiesen und gelte:

(2a) $F = (G \wedge H)$.

$$\begin{aligned} \Rightarrow \mathcal{A}(F) = \mathcal{A}(G \wedge H) &= \begin{cases} 1 & \text{falls} \quad \mathcal{A}(G) = 1 \text{ und } \mathcal{A}(H) = 1 \\ 0 & \text{sonst} \end{cases} \\ &= \begin{cases} 1 & \text{falls} \quad \mathcal{A}'(G) = 1 \text{ und } \mathcal{A}'(H) = 1 \\ 0 & \text{sonst} \end{cases} \\ &= \mathcal{A}'(G \wedge H) = \mathcal{A}'(F). \end{aligned}$$

(2b) $F = (G \vee H)$.
(analog)

(2c) $F = \neg G$.

$$\begin{aligned} \Rightarrow \mathcal{A}(F) &= \begin{cases} 1 & \text{falls} \quad \mathcal{A}(G) = 0 \\ 0 & \text{sonst} \end{cases} \\ &= \begin{cases} 1 & \text{falls} \quad \mathcal{A}'(G) = 0 \\ 0 & \text{sonst} \end{cases} \\ &= \mathcal{A}'(\neg G) = \mathcal{A}'(F). \end{aligned}$$

□

Es genügt zur Feststellung der Erfüllbarkeit/Gültigkeit von F die endlich vielen Belegungen, die genau auf den atomren Formeln Teilformeln von F definiert sind zu testen. Besitzt F n atomare Teilformeln, dann sind genau 2^n viele Belegungen zu untersuchen.

Wahrheitswertetafeln / Wahrheitstafeln:

	A_1	...	A_{n-1}	A_n	F
$\mathcal{A}_1$	0	...	0	0	$\mathcal{A}_1(F)$
$\mathcal{A}_2$	0	...	0	1	$\mathcal{A}_2(F)$
$\vdots$					
$\mathcal{A}_{2^n}$	1	...	1	1	$\mathcal{A}_{2^n}(F)$

F ist genau dann unerfüllbar, wenn in der letzten Spalte keine 1 vorkommt.
F ist genau dann gültig, wenn die letzte Spalte nur aus 1en besteht.
F ist genau dann unerfüllbar, wenn in der letzten Spalte nur aus 0en besteht.
F ist genau dann gültig, wenn in der letzten Spalte keine 0 vorkommt.

Beispiel:
$F = ((A \to (\neg A \vee B)) \wedge B)$.

A	B	$\neg A$	$(\neg A \vee B)$	$A \to (\neg A \vee B)$	F
0	0	1	1	1	0
0	1	1	1	1	1
1	0	0	0	0	0
1	1	0	1	1	1

$\Rightarrow F$ ist keine Tautologie.

Problem:
Hat eine Formel zum Beispiel 100 atomare Formeln, so ist selbst der schnellste Rechner tausende von Jahre mit der Berechnung der Wahrheitstafel befaßt.
(Annahme: $1\mu s$ zur Berechnung einer Zeile.)

Theoretischer Hintergrund:
Das Erfüllbarkeitsproblem ist "NP–vollständig."

10.1 Äquivalenz und Normalformen

Definition:
Zwei Formeln F und G heißen (semantisch) äquivalent, falls für alle Belegungen $\mathcal{A}$, die

sowohl für F als auch für G passend sind, gilt

$$\mathcal{A}(F) = \mathcal{A}(G).$$

Bezeichnung:
$F \equiv G$.

Beispiel:

(1) $(F \wedge G) \equiv (G \wedge F)$.

(2) $\neg(F \wedge G) \equiv (\neg F \vee \neg G)$. (de Morgansche Regel)

(3) Alle Tautologien sind (semantisch) äquivalent zu 1.

(4) Alle unerfüllbaren Formeln (Kontradiktionen) sind (semantisch) äquivalent zu 0.

Satz: (Ersetzbarkeitstheorem)
Sei $F \equiv G$. Ist H eine Formel, in der F als Teilformel vorkommt, dann gilt:

$$H \equiv H'$$

wobei H' aus H durch die Ersetztung eines Vorkommens der Teilformel F durch die Teilformel G hervorgeht.

Beweis: (Induktion über den Formelaufbau)
IA:
Ist H eine atomare Formel,dann gilt $H = F$.
$\Rightarrow H' \equiv G$ und folglich $H \equiv H'$.

IS:
Gilt $F = H$, dann kann wie beim IA geschlossen werden.
Gelte also $F \neq H$.

(1) Fall: $H = \neg H_1$.
Nach IV gilt $H_1 \equiv H_1'$, wobei H_1' aus H_1 durch Ersetzung von F durch G hervorgeht.
Für $H' = \neg H_1'$ folgt aus $H_1 \equiv H_1'$ auch $H \equiv H'$.

(2) Fall: $H = (H_1 \vee H_2)$.
F kommt in H_1 oder H_2 vor.
OBdA komme F in H_1 vor.
Nach IV gilt $H_1 \equiv H_1'$, wobei H_1' aus H_1 durch Erstzung von F durch G hervorgeht.
Nach Definition gilt:

$$H' \equiv (H_1' \vee H_2) \equiv (H_1 \vee H_2) \equiv H.$$

(3) Fall: $H = (H_1 \wedge H_2)$.
(Analog zu Fall 2)

□

Formeln können stets in Normalform überführt werden.

Definition: (Normalform)
Ein *Literal* ist eine atomare Formel ("positives Literal") oder die Negation einer atomaren Formel ("negatives Literal").
Eine Formel F ist in konjunktiver Normalform (KNF), falls

$$F = (\bigwedge_{i=1}^{n} (\bigvee_{j=1}^{m_i} L_{ij}))$$

und L_{ij} Literale für alle i, j.
Eine Formel F ist in disjunktiver Normalform (DNF), falls

$$F = (\bigvee_{i=1}^{n} (\bigwedge_{j=1}^{m_i} L_{ij}))$$

und L_{ij} Literale für alle i, j.

Satz 10.5

Zu jeder Formel gibt es eine äquivalente Formel in KNF und eine äquivalente Formel in DNF.

Beweis: (Vollständige Induktion über den Formelaufbau)
IA:
Trivial, da F als atomare Formel KNF und DNF ist.

IS:

(1) Fall: $F = \neg G$.
Nach IV gibt es eine KNF $G_1 = (\bigwedge_{i=1}^{n} (\bigvee_{j=1}^{m_i} L_{ij}))$ und eine DNF $G_2 = (\bigvee_{i=1}^{n} (\bigwedge_{j=1}^{m_i} L_{ij}))$ mit $G \equiv G_1$ und $G \equiv G_2$.
Mehrfache Anwendung der DeMorganchen Regeln liefert:

$$\begin{aligned} F = \neg G &\equiv \neg G_1 \\ &\equiv \neg(\bigwedge_{i=1}^{n} (\bigvee_{j=1}^{m_i} L_{ij})) \\ &\equiv (\bigvee_{i=1}^{n} \neg(\bigvee_{j=1}^{m_i} L_{ij})) \\ &\equiv (\bigvee_{i=1}^{n} (\bigwedge_{j=1}^{m_i} \neg L_{ij})) \end{aligned}$$

ist DNF, da $\neg L_{ij}$ wieder Literal.
Analog für

$$\begin{aligned} F = \neg G &\equiv \neg G_2 \\ &\equiv (\bigwedge_{i=1}^{n} (\bigvee_{j=1}^{m_i} L_{ij})). \end{aligned}$$

(2) Fall: $F = (G \vee H)$.
Nach IV gibt es für G und H äquivalente DNF und KNF.

DNF–Darstellung Für F:
$G \equiv (\bigvee_{i=1}^{n} G_i)$, $H \equiv (\bigvee_{l=1}^{k} H_l)$, wobei die G_i und H_l Konjunktion von Literalen.
$\Rightarrow F = (G \vee H) \equiv ((\bigvee_{i=1}^{n} G_i) \vee (\bigvee_{l=1}^{k} H_l))$.
liefert mit den Assoziativgesetzen eine äquivalente DNF.

KNF–Darstellung für F:
$G \equiv (\bigwedge_{i=1}^{n} G_i)$, $H \equiv (\bigwedge_{l=1}^{k} H_l)$, wobei
$G_i = (\bigvee_{j=1}^{m_l} L_{ij})$ und $H_l = (\bigvee_{r=1}^{s_l} L'_{lr})$.

$$\begin{aligned} \Rightarrow F &= (G \vee H) \\ &\equiv ((\bigwedge_{i=1}^{n} G_i) \vee (\bigwedge_{l=1}^{k} H_l)) \\ &\equiv (\bigwedge_{i=1}^{n} (\bigwedge_{l=1}^{k} (G_i \vee H_l))) \\ &\equiv \bigwedge_{i=1}^{nk} F_i \end{aligned}$$

mit $F_i = (\ldots(L_1 \vee L_2) \vee \ldots) \vee L'_1) \vee \ldots \vee L'_{sl})$,
wobei eventuell moch Tautologieregeln, Idempotenz,... angenwedet werden können.

(3) Fall: $F = (G \wedge H)$.
(Analog zu 2.Fall.)

□

Achtung:

- Die entstehenden DNF / KNF sind nicht notwendigerweise die kürzesten DNF / KNF Darstellungen.
  → Logikminimierung (zweistufige Logikminimierung)
  Schaltkreisentwurf (effektiver Chipentwurf)

- Der Umformungsprozeß einer Formel in KNF bzw. DNF kann zu einer exponentiellen Aufblähung der Formel führen.
  Schlimmstenfalls kann aus einer Formel der Länge n eine Formel der Länge 2^n entstehen. (Das Distributivgesetz verdoppelt in etwa die Formellänge!)
- Eine Formel mit kurzer DNF hat im allgemeinen eine lange KNF und umgekehrt.

Hornformeln

Definition:
Eine Formel F ist eine *Hornformel* (Alfred Horn), falls F in KNF ist und jedes Disjunktionsglied höchstens ein positives Literal enthält.

Beispiel:
$F = (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B) \wedge D \wedge \neg A$ ist Hornformel.
$F' = (A \vee B \vee C) \wedge (\neg A \vee B)$ ist keine Hornformel.

Anschaulichere Darstellung: (von F)
$\tilde{F} = ((B \wedge C) \to A) \wedge (A \to B) \wedge (1 \to D) \wedge (A \to 0))$.

Offenbar gilt: $F \equiv \tilde{F}$.
(0 steht für unerfüllbare Formel.)
(1 steht für Tautologie.)

Grundproblem:
Gesucht:
Allgemeiner Test für die $\left\{ \begin{array}{c} \text{Gültigkeit} \\ \text{Erfüllbarkeit} \\ \text{Unerfüllbarkeit} \end{array} \right\}$ einer Formel.
Es genügt dabei $\left\{ \begin{array}{c} \text{Erfüllbarkeit} \\ \text{Unerfüllbarkeit} \end{array} \right\}$ zu betrachten.

(F ist gültig $\Leftrightarrow \neg F$ unerfüllbar.)

$\left\{ \begin{array}{c} \text{Erfüllbarkeit} \\ \text{Unerfüllbarkeit} \end{array} \right\}$ kann stets getestet werden. (Wahrheitstafel.)

Aufwand:
Exponentiell in der Zahl der atomaren Formeln!

Für Hornformeln gibt es effizientere Erfüllbarkeitstests.

Eingabe:
Hornformel F.

Algorithmus:

(1) Markiere alle Vorkommen einer atomaren Formel A in F mit "1", falls es in F die Teilformel $(1 \to A)$ gibt.

(2) while

es in F eine Teilformel G der Form $(A_1 \wedge \ldots \wedge A_n \to B)$ oder $(A_1 \wedge \ldots \wedge A_n \to 0)$, $n \geq 1$, wobei $A_1 \ldots A_n$ bereits mit "1" markiert sind (und B noch nicht markiert ist).

do

if G hat die erste Form then markiere jedes Vorkommen von B.
else gib "unerfüllbar" aus und stoppe.

(3) Gib "erfüllbar" aus und stoppe.

Bemerkung:
Die Markierung liefert die erfüllende Belegung:
$\mathcal{A}(A_i) = \begin{cases} 1 & \text{falls } A_i \text{ ist markiert.} \\ 0 & \text{sonst.} \end{cases}$

Satz 10.6

Der obige Algorithmus ist für Hornklauseln als Eingabe korrekt und stoppt nach höchstens n Markierungsschritten, wobei n die Anzahl der atomaren Formeln in F ist.

Beweis:

- In jedem Schritt wird mindestens eine atomare Formel markiert.
  $\Rightarrow$ Der Algorithmus bricht nach höchstens n Schritten ab.
- Die Korrektheit des Algorithmus wird gezeigt durch:
  (1) Angabe eines Modells $\mathcal{A}$ für F, falls der Algorithmus "erfüllbar" ausgibt.
  (2) Nachweis der Unerfüllbarkeit von F, falls der Algorithmus "unerfüllbar" ausgibt.

Zu 1:
Setze $\mathcal{A}(A_i) = \left\{ \begin{array}{ll} 1 & \text{falls } A_i \text{ ist markiert.} \\ 0 & \text{sonst.} \end{array} \right\}$ für alle atomaren Formeln A_i in F.

Behauptung:
$\mathcal{A}(F) = 1$.

Es genügt zu zeigen:
$\mathcal{A}(G) = 1$ für alle Disjunktionsglieder G von F.

(1) Fall: $G = A_i$ atomare Formel.
$\Rightarrow_{1.\text{ Schritt}} G$ ist markiert
$\Rightarrow \mathcal{A}(G) = 1.$

(2) Fall: $G = (A_1 \wedge \ldots \wedge A_n \rightarrow 0)$.
$\Rightarrow$ Es gibt ein unmarkiertes A_i (Sonst gibt der Algorithmus "unerfüllbar" aus.)
$\Rightarrow \mathcal{A}(A_1 \wedge \ldots \wedge A_n) = 0.$
$\Rightarrow \mathcal{A}(G) = 1.$

(3) Fall: $G = (A_1 \wedge \ldots \wedge A_n \rightarrow B)$.

- Alle A_i sind markiert.
  $\Rightarrow_{2.\text{Schritt}} B$ ist markiert.
  $\Rightarrow \mathcal{A}(G) = 1.$
- Es gibt ein unmarkiertes A_i.
  $\Rightarrow \mathcal{A}(A_i) = 0.$
  $\Rightarrow \mathcal{A}(A_1 \wedge \ldots \wedge A_n) = 0.$
  $\Rightarrow \mathcal{A}(G) = 1.$

Zu 2:
Der Algorithmus gibt "unerfüllbar' aus.
$\Leftrightarrow$ Ein Disjunktionsglied $G = (A_1 \wedge \ldots \wedge A_n \rightarrow 0)$ gibt in dem alle A_i markiert sind.
Annahme: Es gibt ein Modell $\mathcal{A}$ für F.
$\Rightarrow \mathcal{A}(A_i) = 1$ für alle in F markierten atomaren Formeln.

- klar für atomare Formeln (Nach Schritt 1).
- klar für $(A_1 \wedge \ldots \wedge A_n \rightarrow B)$.

$\Rightarrow \mathcal{A}(G) = 0.$
$\Rightarrow \mathcal{A}(F) = 0.$ (Widerspruch)

□

Korollar 1:
Das im Korrektheitsbeweis konstruierte Modell $\mathcal{A}$ für F ist das kleinste Modell für F.
D.h. ist $\mathcal{A}'$ ein weiteres Modell für F, dann gilt:

$$\mathcal{A}(A_i) \leq \mathcal{A}'(A_i).$$

für alle atomaren Teilformeln A_i von F.

Korollar 2:
Enthält eine Hornformel F keine Teilformel der Bauart $(A_1 \wedge \ldots \wedge A_n \rightarrow 0)$, so ist F erfüllbar.

Beweis:
Die einzige Möglichkeit für den Algorithmus "unerfüllbar" auszugeben, ist auf einem

Disjunktionsglied der Gestalt $(A_1 \wedge \ldots \wedge A_n \to 0)$ zu stoppen. □

Bezeichnung:
Disjunktionsglieder der Gestalt $(A_1 \wedge \ldots \wedge A \to 0)$ heißen *Zielklausel*.

Korollar 3:
Enthält eine Hornformel F keine Teilformel der Bauart $(1 \to A)$, so ist F erfüllbar.

Beweis:
In diesem Fall wird die While–Schleife nicht betreten! □

Endlichkeitssatz

Satz (Endlichkeitssatz, compactness theorem)
Für eine Menge M von Formeln gilt

$$M \text{ ist erfüllbar} \iff \text{jede endliche Teilmenge von } M \text{ ist erfüllbar.}$$

Beweis:
$(\to)$:
Jedes Modell für M ist ein Modell für eine beliebige Teilmenge von M, insbesondere für endliche Teilmengen.

$(\leftarrow)$:
Konstruktion eines Modells der Gesamtmenge aus der Vielzahl existierender Modell für die endlichen Teilmengen.

$$M_n = \{\text{Formeln, die nur aus den atomaren Formeln } A_1, \ldots A_n \text{ bestehen}\}.$$

In M_n gibt es höchstens $k \leq 2^{2^n}$ paarweise nicht äquivalente Formeln $F_1, \ldots F_k$,da es genau 2^{2^n} verschiedene Wahrheitstafeln mit den atomaren Formeln $A_1, \ldots A_n$ gibt.
$\Rightarrow$ Jedes Modell Für $\{F_1, \ldots, F_k\}$ ist Modell für M_n.
(Für alle $F \in M_n$ gibt es ein F_i mit $F \equiv F_i$.)
Sei $\mathcal{A}_n$ Modell für $\{F_1, \ldots F_n\}$. (Existiert nach Vorraussetzung!)
Wegen $M_1 \subseteq \ldots \subseteq M_n$ ist $\mathcal{A}_n$ auch Modell für $M_1, \ldots, M_{n-1}$.

Stufenweise Konstruktion eines Modells für $\mathcal{A}$ mit Hilfe der $\mathcal{A}_i$.

Konstruktion:
Stufe 0:

$$\begin{array}{rrl} \text{Definiere: } \mathcal{A} & := & \emptyset. \\ I & := & \{1, 2, 3, \ldots\}. \end{array}$$

Stufe $n > 0$:

if es gibt unendlich viele Indizes $i \in I$ mit $\mathcal{A}_i(A_n) = 1$
then
begin

$$\begin{aligned} \text{Definiere: } \mathcal{A} &:= \mathcal{A} \cup \{A_n\}, \\ \mathcal{A}(A_n) &:= 1, \\ I &:= I - \{i : \mathcal{A}_i(A_n) \neq 1\}. \end{aligned}$$

end

else

begin

$$\begin{aligned} \text{Definiere: } \mathcal{A} &:= \mathcal{A} \cup \{A_n\}, \\ \mathcal{A}(A_n) &:= 0, \\ I &:= I - \{i : \mathcal{A}_i(A_n) \neq 0\}. \end{aligned}$$

end

$\mathcal{A}$ ist wohldefiniert.
Es gilt entweder $\mathcal{A}(A_n) = 1$ oder $\mathcal{A}(A_n) = 0$. □

Behauptung:
$\mathcal{A}$ ist Modell für M.

Beweis:
Sei $F \in M$.
In F kommen nur atomare Teilformeln A_i , $i \leq l$ vor.
$\Rightarrow F \in M_l \subseteq M_{l+1} \subseteq \ldots$
und
$\mathcal{A}_l, \mathcal{A}_{l+1}, \ldots$ sind Modelle für F.
Nach Konstruktion von $\mathcal{A}$ simmt $\mathcal{A}$ mit unendlichen vielen der $\mathcal{A}_i$ überein.
$\Rightarrow \mathcal{A}$ ist Modell für F. □

Achtung:
Der Beweis ist nicht konstruktiv!
Die Existenz wird bewiesen, ohne daß die Konstruktion algorithmisch ausführbar wäre.
D.h. es ist kein Algorithmus, der tatsächlich konstruiert.

Korollar
Die Formelmenge M ist unerfüllbar
$\Leftrightarrow$ Eine unerfüllbare endliche Teilmenge $M' \subseteq M$ existiert.

Definition:
Eine Formelmenge M_0 heißt *Axiomensystem* für die Formelmenge M, falls
$\{\mathcal{A} : \mathcal{A} \text{ ist Modell für } M_0\} = \{\mathcal{A} : \mathcal{A} \text{ ist Modell für } M\}$.
M heißt *endlich axiomisierbar*, falls M ein endliches Axiomensystem besitzt.

10.2 Resolution

Resolution ist ein einfach anwendbarer *syntaktischer* Umformungsprozeß.
Aus zwei Formeln wird durch bestimmt Ersetzungsregeln eine dritte Formel generiert.

Kalkül:
Menge syntaktischer Umformungsregeln.
Rein mechanisch anwendbar.
Gut geeignet zur algorithmischen Implementierung am Computer.

Resolutionskalkül:
Besteht nur aus einer Umformungsregel

Anforderungen:
Vollständig und korrekt (im Bezug auf die betrachtete Aufgabenstellung).

Aufgabenstellung:
Nachweis der Unerfüllbarkeit.

Korrektheit:
Keine erfüllbare Formelmenge wird durch das Kalkül als unerfüllbar ausgewiesen.

Vollständigkeit:
Jede unerfüllbare Formelmenge wird durch das Kalkül als unerfüllbar ausgewiesen.

Vorraussetzung für die Anwendung des Resolutionskalküls:
Formeln sind in KNF.
$F = (L_{1,1} \vee \ldots \vee L_{1,n_1}) \wedge \ldots \wedge (L_{k,1} \vee \ldots \vee L_{k,n_k})$, $L_{i,j} \in \{A_k\} \cup \{\neg A_k\}$ (Literal) wird als Menge von "Klauseln" $F = \{\{L_{1,1}, \ldots, L_{1,n_1}\}, \ldots, \{L_{k,1}, \ldots, L_{k,n_k}\}\}$ geschrieben.

Vorteil: Die Elemente der Klauseln haben keine Rangordnung.
$\Rightarrow$ Die Vereinfachungen durch Assoziativ- und Kommutativgesetze ergeben sich unmittelbar.
Kein Element kommt mehrfach vor.
$\Rightarrow$ Die Vereinfachung durch das Idempotenz ergibt sich unmittelbar.

Beispiel:

- $((A_1 \vee \neg A_2) \wedge (\neg A_3 \vee \neg A_3))$
- $(\neg A_3 \wedge (\neg A_2 \vee A_1))$
- $(\neg A_3 \wedge ((\neg A_2 \vee \neg A_2) \vee A_1))$

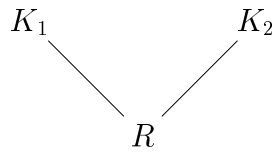
haben die gleiche Mengendarstellung:

$$\{\{A_1, \neg A_2\}, \{\neg A_3\}\}.$$

Definition:
Seien K_1, K_2, R Klauseln.
R heißt *Resolvent von* K_1 *und* K_2, falls es ein Literal L mit $L \in K_1, \neg L \in K_2$ gibt und R hat die Gestalt:

$$R = (K_1 - \{L\}) \cup (K_2 - \{\neg L\}).$$

Darstellung:

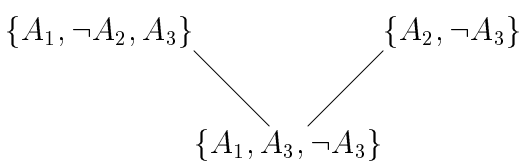


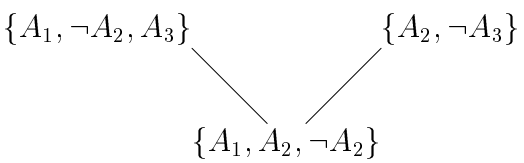
R wird aus K_1 und K_2 resolviert.

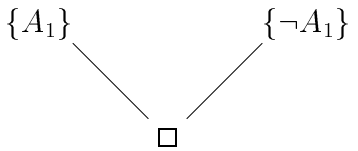
Vereinbarung:
Bezeichnung der als Resolvent auftretenden leeren Menge durch $\square$.
$\square$ bezeichnet die unerfüllbare Formel.

Beispiel:
$K_1 = \{L\}, K_2 = \{\neg L\} \Rightarrow R = \square$ unerfüllbar.
$\rightarrow$ Eine Klauselmenge, die $\square$ enthält ist per Definition unerfüllbar.

Beispiel:







Resolutionslemma:
Sei F in KNF in Mengendarstellung.
R sei Resolvent zweier Klauseln $K_1, K_2 \in F$.
Dann gilt:

$$F \equiv F \cup \{R\}.$$

Beweis:
Sei $\mathcal{A}$ zu F passend $\Rightarrow \mathcal{A}$ ist auch zu $F \cup \{R\}$ passend.

Noch zu zeigen:
$\mathcal{A} \models F \Leftrightarrow \mathcal{A} \models F \cup \{R\}$.

Beweis:
($\leftarrow$): (trivial)
($\rightarrow$):
Sei $\mathcal{A} \models F$.
$\Rightarrow \mathcal{A} \models K$ für alle $K \in F$.
Sei $R = ((K_1 - \{L\}) \cup (K_2 - \{\neg L\})$ mit $K_1, K_2 \in R$, $L \in K_1$, $\neg L \in K_2$.

(1) Fall: $\mathcal{A} \models L$.
Aus $\mathcal{A} \models K_2$ und $\mathcal{A} \not\models \neg L$ folgt $\mathcal{A} \models K_2 - \{\neg L\}$.
$\Rightarrow \mathcal{A} \models R$.

(2) Fall:$\mathcal{A} \not\models L$.
Aus $\mathcal{A} \models K_1$ folgt $\mathcal{A} \models K_1 - \{L\}$.
$\Rightarrow \mathcal{A} \models R$.

$\square$

Definition:
Sei F eine Klauselmenge.
Dann ist $Res(F)$ definiert als

$$Res(F) = F \cup \{R : R \text{ ist Resolvent zweier Klauseln aus } F\}.$$

$Res^0(F) = F$.
$Res^{n+1}(F) = Res(Res^n(F))$ für $n > 0$.
$Res^*(F) = \bigcup_{n \geq 0} Res^n(F)$.

Für jede endliche Klauselmenge F gibt es ein $k \geq 0$ mit

$$Res^k(F) = Res^{k+1}(F) = \ldots = Res^*(F).$$

Resolutionstheorem: (Für Aussagenlogik)
Eine Klauselmenge F ist unerfüllbar
$\Leftrightarrow \square \in Res^*(F)$.

Beweis:
($\leftarrow$): (Korrektheit)
Sei $\square \in Res^*(F)$.
$\square$ entsteht nur aus Klauseln K_1, K_2 mit $K_1 = \{L\}$, $K_2 = \{\neg L\}$.
$\Rightarrow_{\text{Resolutionslemma}} F \equiv Res^1(F) \equiv \ldots \equiv Res^n(F) \equiv \ldots$.
Wegen $\square \in Res^*(F)$ gibt es ein $n > 0$ mit $\square \in Res^n(F)$.
$\Rightarrow K_1, K_2 \in Res^n(F)$.
Da es kein Modell gibt, in dem sowohl K_1 als auch K_2 erfüllt ist, ist $Res^n(F)$ unerfüllbar.
Wegen $Res^n(F) \equiv F$ ist F unerfüllbar.

($\rightarrow$) : (Vollständigkeit)
Annahme: F ist unerfüllbar.
Ist F unendlich, so können wir uns nach dem Endlichkeitssatz auf endliche unerfüllbare Teilmengen von F beschränken.
Zeigen von $\square \in Res^*(F)$ durch Induktion über die Anzahl n der in F vorkommenden atomaren Formeln.

IA: n=0:
$\Rightarrow F = \{\square\} \Rightarrow \square \in F \subseteq Res^*(F)$.

IS: $n \rightarrow n + 1$:
Sei F eine Klauselmenge mit den atomaren Formeln $A_1, \ldots, A_{n+1}$.
Betrachte die Klauselmengen F_0 und F_1:
F_0 entsteht aus F durch:

- streichen jedes Vorkommens von A_{n+1} in den Klauseln von F.

– streichen der Klauseln von F, in denen $\neg A_{n+1}$ vorkommt.

(D.h. F_0 entsteht aus F durch Belegung von A_{n+1} mit 0.)

F_1 wird analog mit vertauschter Rolle von A_{n+1} und $\neg A_{n+1}$ definiert.
(D.h. F_1 entsteht aus F durch Belegung von A_{n+1} mit 1.)

Zeige:
F_0 und F_1 sind unerfüllbar.

Annahme: Es gibt eine Modell $\mathcal{A} : \{A_1, \ldots, A_n\} \to \{0, 1\}$ für F_0.
$\Rightarrow$ Belegung $\mathcal{A}'$ mit

$$\mathcal{A}'(B) = \begin{cases} \mathcal{A}(B) & \text{falls } B \in \{A_1, \ldots, A_n\}. \\ 0 & \text{falls } B = A_{n+1}. \end{cases}$$

ist Modell für F. (Widerspruch zur Unerfüllbarkeit von F)

Analog ergibt sich die Unerfüllbarkeit von F_1.
$\Rightarrow_{\text{IV}} \square \in Res^*(F_0)$ und $\square \in Res^*(F_1)$.
$\Rightarrow$ Es gibt Klauseln $K_1, \ldots, K_m$ mit
$K_m = \square$ und
$K_i \in F_0$ oder K_i ist Resolvent zweier Klauseln K_r, K_s mit $r, s < i$.

Betrachte:

$$\tilde{K_i} = \begin{cases} K_i \cup \{A_{n+1}\} & \text{falls } K_i \text{ durch Streichung von } A_{n+1} \\ & \text{aus einer Klausel von } F \text{ entstanden ist.} \\ K_i & \text{sonst.} \end{cases}$$

A_{n+1} wird bei den Resolutionsschritten mitgeführt.
$\Rightarrow$ Es entsteht eine Folge $\tilde{K_1}, \ldots, \tilde{K_m}$ mit $\{A_{n+1}\} \in Res^*(F)$ oder
$\square \in Res^*(F)$.
Tritt letzteres ein, dann sind wir fertig.
Für F_1 können analog Folgen $K'_1, \ldots K'_l$ aufgebaut werden mit $\square \in Res^*(F_1)$

Betrachte:

$$\tilde{K'_i} = \begin{cases} K'_i \cup \{\neg A_{n+1}\} & \text{falls } K'_i \text{ durch Streichung von } \neg A_{n+1} \\ & \text{aus einer Klausel von } F \text{ entstanden ist.} \\ K'_i & \text{sonst.} \end{cases}$$

$\tilde{K'_1}, \ldots, \tilde{K'_l}$ zeigt $\{A_{n+1}\} \in Res^*(F)$ oder
$\square \in Res^*(F)$.
Gilt $\{\{A_{n+1}\}, \{\neg A_{n+1}\}\} \in Res^*(F) \Rightarrow$
$\Rightarrow \square \in Res^*(F)$. $\square$

Algorithmus:

Eingabe:
Formel F in KNF.

Ausgabe:
Entscheidung über Unerfüllbarkeit von F.

Algorithmus:

(1) Bilde aus F Klauselmenge.

(2) $n := 0$, $R[n] := F$.

(3) repeat
$n := n + 1$
$R[n] := Res(R[n-1])$
until ($\square \in R[n]$ oder $R[n] = R[n-1]$)

(4) if $\square \in R[n]$ then "F ist unerfüllbar"
else "F ist erfüllbar".

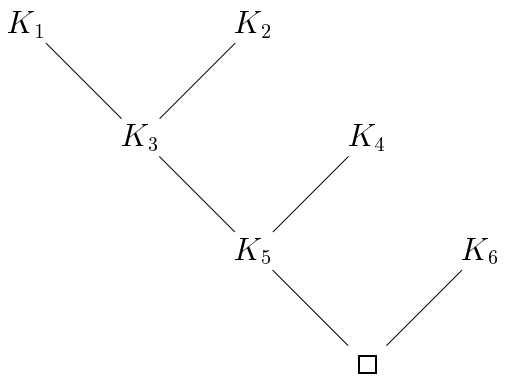
Analyse:
Manchmal sehr schlecht, oft auch exponentiell.

Betrachte lediglich die Klauseln, die für die Erzeugung von $\square$ wichtig sind:

Definition:
Eine *Deduktion* der leeren Klausel aus einer Klauselmenge F ist eine Folge $K_1, \ldots K_m$ von Klauseln mit: $K_m = \square$ und
$K_i \in F$ oder K_i ist Resolvent zweier Klauseln K_r, K_s mit $r, s < i$.

Zum Beweis der Unerfüllbarkeit genügt die Angabe einer Deduktion der leeren Klausel aus F.
Es werden nicht alle Klauseln aus $Res^*(F)$ gebraucht.

Beispiel:
$K_1 = \{A_1, A_2, \neg A_3\}$,
$K_2 = \{A_1, A_2, A_3\}$,
$K_4 = \{A_1, \neg A_2\}$,
$K_6 = \{\neg A_1\}$,
$K_1, K_2, K_4, K_6 \in F$.



Bemerkung:
Das Resolutionskalkül kann auf Hornformeln eingeschränkt werden:
Es genügt dazu, die folgend eingeschränkte Resolution (Einheitsrelation) zu betrachten:

$$\#K_1 = 1 \text{ oder } \#K_2 = 1.$$

Deratiege Resolutionen verkürzen die Klauseln mit Sicherheit.
$\Rightarrow$ Angabe eines effektiven Algorithmus zur Entscheidung von $\square \in Res^*(F)$.

Kapitel 11

Graphen

11.1 Wegprobleme in Graphen

Viele praktische Anwendungen verlangen die Bestimmung des kürzesten Weges zwischen zwei Orten, der kostengünstigsten Transportverbindung zwischen zwei Städten oder der minimalen Leitungslänge zur Verkabelung zweier Stationen. Graphentheoretisch betrachtet, führen alle diese Probleme auf die Frage nach kürzesten Wegen, bzw. allgemeiner nach kostengünstigen Wegen zwischen zwei Knoten $v, w \in V$ in einem gerichteten Graphen $G = (V, E)$. Das Problem der Bestimmung des kürzesten Weges, kurz auch *kürzester–Weg* Problem genannt, ist ein Spezialfall des *allgemeinen Wegproblems*, das im *Auffinden aller Wege zwischen zwei Knoten von* G besteht. Wegprobleme sind als Kernstück zur Lösung verschiedenster Graphprobleme von zentraler Bedeutung für die Anwendung der Graphentheorie.
Die Lösung des *Wegproblems* steht in engem Zusammenhang mit der Bestimmung des *transitiven Abschlusses* $G^* = (V, E^*)$ eines Graphen $G = (V, E)$, der alle Paare $(u, v) \in E^*$, als Kanten enthält die in G durch Wege verbunden sind.
Eine einheitliche und darum sehr effektive Beschreibung der verschiedenen Wegprobleme ist in der algebrischen Struktur der *abgeschlossenen Halbringe* möglich.
Ein *Halbring* ist eine Menge H, in der zwei Elemente 0 und 1 ausgezeichnet sind, und auf der zwei 2–stellige Operationen $\oplus$ (Addition) und $\odot$ (Multiplikation) mit den folgenden Eigenschaften definiert sind:

(1) $(H, \oplus, 0)$ ist ein kommutatives Monoid, d.h. für alle $u, v \in H$ gilt:

(1a) $(u \oplus v) \oplus w = u \oplus (v \oplus w)$,

(1b) $u \oplus 0 = u$,

(1c) $u \oplus v = v \oplus u$.

(2) $(H, \odot, 1)$ ist ein Monoid, d.h. für alle $u, v \in H$ gilt:

(2a) $(u \odot v) \odot w = u \odot (v \odot w)$,

(2b) $u \odot 1 = u$.

(3) Die Operation $\odot$ distributiert über die Operation $\oplus$, d.h. für alle $u, v, w \in H$ gilt:
$u \odot (v \oplus w) = u \odot v \oplus u \odot w$ und
$(u \oplus v) \odot w = u \odot w \oplus v \odot w$.

(4) Es gilt für alle $u \in H$:
$u \odot 0 = 0$.

Ein Halbring heißt abgeschlossen, wenn unendliche Summen existieren, d.h. wenn zu jeder abzählbar unendlichen Menge I und jeder Menge $\{u_i : i \in I, u_i \in H\}$ ein Element $\sum_{i \in I} u_i$, die (unendliche) Summe der u_i , $i \in I$, existiert. Für diese unendlichen Summen gelte:
Für jede endliche Teilmenge $I' = \{i_i, \ldots, i_k\} \subseteq I$ gilt:

$$\sum_{j \in I'} u_j = u_{i_1} \oplus \ldots \oplus u_{i_k}.$$

Für $I' = \emptyset$ gilt:

$$\sum_{j \in \emptyset} u_j = 0.$$

Die Operation $\odot$ distributiert über unendliche Summen,
d.h.

$$\left(\sum_{i \in I} u_i\right) \odot \left(\sum_{j \in J} v_j\right) = \sum_{i \in I} \left(\sum_{j \in J} u_i \odot v_j\right).$$

Beispiel:
Einige bekannte abgeschlossene Halbringe.

(1) Der einfachste abgeschlossene Halbring ist der Boolesche Halbring $\mathcal{B} = (\{0,1\}, \vee, \wedge, 0, 1)$ wobei $\vee$ (OR) bzw. $\wedge$ (AND) wie üblich die Boolesche Addition bzw. die Boolesche Multiplikation bezeichne. Unendliche Summen sind definiert durch

$$\sum_{i \in I} a_i = \begin{cases} 1 & \text{falls ein } \imath \in I \text{ existiert mit } A_i = 1. \\ 0 & \text{sonst.} \end{cases}$$

Mit Hilfe Boolescher Halbringe ist die *Existenz von Verbindungswegen zwischen zwei Knoten eines Graphen entscheidbar.*

(2) Auch die Menge der nichtnegativen reellen Zahlen $\mathbb{R}^+$ bildet unter Hinzunahme von ∞ (Nullelement) mit den Operationen inf (Addition) und $+$ (Multiplikation) einen abgeschlossenen Halbring $\mathcal{R}^+ = \{\mathbb{R}^+ \cup \{\infty\}, inf, +, \infty, 0\}$, im Rahmen dessen wir *kostengünstige Wege* berechnen können.

(3) Bezeichnet $\circ$ die Konkatenation zweier Worte eines freien Monoids A^* über einem endlichen Alphabet A, und λ das leere Wort, dann bildet die Potenzmenge $\mathcal{P}(A^*)$ von A^* bezüglich $\cup$ (Addition) und $\circ$ (Multiplikation) zusammen mit $\emptyset$ (Nullelement) und $\{\lambda\}$ (Einselement) einen abgeschlossenen Halbring $\mathcal{P}(A^*) = (\mathcal{P}(A^*), \cup, \circ, \emptyset, \{\lambda\})$.

In einem abgeschlossenen Halbring gibt es zu jedem Element u ein Element u^*, das definiert ist durch

$$u^* = 1 \oplus u \oplus u^2 \oplus \ldots = \sum_{0 \leq j \leq \infty} u^j,$$

wobei $u^0 = 1$ und $u^{i+1} = u \circ u^i$ gesetzt wird.
Die damit definierte 1–stellige Operation * heißt *Abschluß* und ist bei der Arbeit in abgeschlossenen Halbringen von großer Bedeutung.
Stets gilt: $0^* = 1$.

Beispiel:
Wirkung der Abschlußoperationen in den abgeschlossenen Halbringen aus dem vorangegangenen Beispiel.

(1) Im Booleschen Halbring gilt stets $a^* = 1$.

(2) In $\mathcal{R}^+$ gilt stets $a^* = 0$ für alle $a \in I\!R^+$.

(3) In $\mathcal{P}(A^*)$ gilt:

$$M^* = \{\lambda\} \cup \{a_1 \circ \ldots \circ a_k : k \geq 1 \text{ und } a_i \in M\}.$$

Kommen wir zurück zur Betrachtung *gerichteter Graphen* $G = (V, E)$. Ist $c : E \to H$, eine Kantenbewertung von G mit Werten in einem abgeschlossenen Halbring $H = (H, \oplus, \odot, 0, 1)$, dann kann diese leicht zu einer, wieder durch c bezeichneten *Bewertung der Wege* $p = (v_1, \ldots, v_k)$, $v_i \in V$, $k \geq 1$, von G erweitert werden (λ bezeichne einen nur aus einem Knoten bestehenden trivialen Weg):

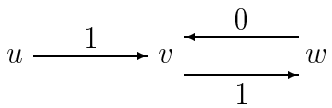
$$\begin{aligned} c(\lambda) &= 1 \\ c(p) &= \prod_{1 \leq i \leq k-1} c(v_i, v_{i+1}). \end{aligned}$$

Ist P eine Menge von Wegen, dann definieren wir

$$c(P) = \sum_{p \in P} c(p) \text{ bzw. } c(\emptyset) = 0.$$

Im folgenden bezeichnen wir durch $[u, v]$ die Menge alle Wege in G von u nach v.

Beispiel:
Ein gerichteter Graph mit einer Bewertung im Booleschen Halbring $\mathcal{B}$.



Offenbar gilt:

$$\begin{aligned} c[u,u] = c[v,u] = c[w,u] = c[v,v] = c[w,w] = c[w,v] &= 0 \\ c[u,v] = c[u,w] = c[v,w] &= 1 \end{aligned}$$

11.2 Allgemeines Wegproblem

Mit den eingeführten Bezeichnungen kann das *allgemeine Wegproblem* nun leicht charakterisiert werden als die Bestimmung von $c[u,v]$ für alle Paare von Knoten $u, v \in V = \{v_1, \ldots, v_n\}$ eines gerichteten Graphen $G = (V, E, c)$ mit einer Kantenbewertung $c : E \to H$ in einem abgeschlossenen Halbring H.
Das allgemeine Wegproblem läßt sich mit Hilfe des folgenden Algorithmus, der als *Algorithmus von Kleene* bekannt ist, lösen. Als *elementarer Schritt* gilt dabei die Ausführung einer der Operationen $\oplus, \odot$ und * aus H.

Methode:
Bezeichne P_{ij}^k die Menge aller Wege in G von v_i nach v_j, die, abgesehen von den Endpunkten, nur Knoten mit einem Index $\leq k$ enthalten. Ist $i = j$, dann sei der triviale Weg (v_i) der Länge 0 nur im Falle $k \geq i$ in P_{ii}^k enthalten.
Beispielsweise gilt $v_9v_3v_8 \in P_{98}^3, P_{98}^5$, $v_9v_3v_8 \notin P_{98}^2$ und $(v_i) \notin P_{ii}^{i-1}$.
Offenbar gilt für $c_{ij}^k := c(P_{ij}^k)$:

$$c_{ij}^n = c[v_i, v_j].$$

Zur Ermittlung der c_{ij}^n , $1 \leq i, j \leq n$, berechnen wir iterativ unter Verwendung der Technik der iterativen Programmierung die c_{ij}^k für alle $1 \leq i, j \leq n$, $0 \leq k \leq n$. Das ist möglich mit Hilfe der folgenden, leicht einzusehehnden Rekursion:

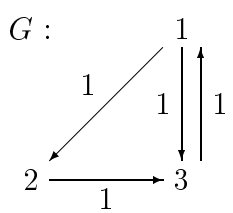
$$c_{ij}^0 = \begin{cases} c(v_i, v_j) & \text{falls } (v_i, v_j) \in E. \\ 0 & \text{sonst.} \end{cases}$$

und für $k \geq 1$

$$c_{ij}^k = \begin{cases} c_{ij}^{k-1} \oplus c_{ik}^{k-1} \odot (c_{kk}^{k-1})^* \odot c_{kj}^{k-1} \oplus 1 & \text{falls } i = j = k. \\ c_{ij}^{k-1} \oplus c_{ik}^{k-1} \odot (c_{kk}^{k-1})^* \odot c_{kj}^{k-1} \oplus & \text{sonst.} \end{cases}$$

Dabei enthält der erste Summand von c_{ij}^k die Kosten aller Wege von v_i nach v_j, die v_k nicht als Zwischenknoten enthalten. Der zweite Summand gibt die Kosten aller Wege wieder, die v_k als Zwischenknoten enthalten, wobei durch $(c_{ij}^{k-1})^*$ die Kosten aller Wege zwischen dem ersten und dem letzten Auftreten von v_k erfaßt werden.

Beispiel:
Lösung des allgemeinen Wegproblems in G nach der angegebenen Methode.



Bestimmung der Mengen P_{ij} , $1 \leq i,j \leq 3$, $0 \leq k \leq 3$:
$k = 0$:

$$P_{11}^0 = P_{22}^0 = P_{33}^0 = P_{12}^0 = P_{21}^0 = P_{13}^0 = P_{31}^0 = P_{23}^0 = P_{32}^0 = \emptyset.$$

$k = 1$:

$$\begin{array}{lll} P_{11}^1 = \{(1)\}, & P_{22}^1 = \emptyset, & P_{33}^1 = \{(3,1,3)\}, \\ P_{12}^1 = \{(1,2)\}, & P_{21}^1 = \emptyset, & P_{13}^1 = \{(1,3)\}, \\ P_{31}^1 = \{(3,1)\}, & P_{23}^1 = \{(2,3)\}, & P_{32}^1 = \{(3,1,2)\}. \end{array}$$

$k = 2$:

$$\begin{array}{lll} P_{11}^2 = \{(1)\}, & P_{22}^2 = \{(2)\}, & P_{33}^2 = \{(3,1,2,3),(3,1,3)\}, \\ P_{12}^2 = \{(1,2)\}, & P_{21}^2 = \emptyset, & P_{13}^2 = \{(1,3),(1,2,3)\}, \\ P_{31}^2 = \{(3,1)\}, & P_{23}^2 = \{(2,3)\}, & P_{32}^2 = \{(3,1,2)\}. \end{array}$$

$k = 3$:

$$\begin{array}{l} P_{11}^3 = \{(1,3,1),(1,2,3,1)\}^*, \\ P_{22}^3 = \{(2,3)\{(3,1,3)\}^*(3,1,2)\}^*, \\ P_{33}^3 = \{(3,1,3),(3,1,2,3)\}^*, \\ P_{13}^3 = \{(1,3,1),(1,2,3,1)\}^*(1,3)\{(3,1,3),(3,1,2,3)\}^*, \\ P_{31}^3 = \{(3,1,3)\}^*(3,1)\{(1,3,1)\}^*, \\ P_{23}^3 = \{(2,3,1,2)\}^*(2,3)\{(3,1,3),(3,1,2,3)\}^*, \\ P_{32}^3 = \{(3,1,2,3)\}^*(3,1,2)\{(2,3,1,2)\}^* = P. \end{array}$$

Arbeitet man im *Booleschen Halbring* $\mathcal{B}$, dann erhält man $c[i,j] = 1$ genau dann, wenn es in G einen Weg von i nach j gibt.
Arbeitet man dagegen im *Halbring* $\mathcal{R}^+$, dann gibt $c[i,j]$ die Kosten der *billigsten Verbindung* von i nach j in G an.

ALGORITHMUS von Kleene:

Eingabe:

> Ein gerichteter, kantenbewerteter Graph $G = (V,E,c)$ mit $V = \{v_1,\ldots,v_n\}$.
> Die Kantenbwertung $c : E \to H$ in den abgeschlossenen Halbring $H = (H,\oplus,\odot,0,1)$ ist gegeben durch die Matrix $c[1:n,1:n]$ mit $c[i,j] = (v_i,v_j)$.

Ausgabe:

> $c[i,j] = c([v_i,v_j])$ für beliebige $v_i, v_j \in V$.

Prozedur:

PROZEDURE Comp($c[1:n, 1:n]$);
(* In den Elementen $c'[i,j,k]$ der Matrix $c'[1:n, 1:n, 0:n]$ werden die c_{ij}^k gespeichert. *)
BEGIN

FOR $1 \leq, i, j \leq n$ DO $c'[i,j,0] \leftarrow 0$;
FOR $1 \leq i, j \leq n$ und $(v_i, v_j) \in E$ DO

$c'[i,j,0] \leftarrow c[i,j]$;

FOR $k \leftarrow 1$ to n DO

FOR $1 \leq i, j \leq n$ DO
BEGIN

$c'[i,j,k] \leftarrow c'[i,j,k-1] \oplus c'[i,k,k-1] \odot (c'[k,k,k-1])^* \odot c'[k,j,k-1]$;
IF $i = j = k$ THEN $c'[i,j,k] \leftarrow c'[i,j,k] \oplus 1$;

END;

FOR $1 \leq i, j \leq n$ DO $c[i,j] \leftarrow c'[i,j,n]$;

END

Analyse:

Die aufwendigste Berechnung ist die in der vorletzten FOR–Anweisung. Die dort enthaltenen 4 Operationen sind jeweils n^3 mal auszuführen, während alle übrigen Anweisungen jeweils nur n^2 bzw. n mal auszuführen sind.

Insgesamt gilt also:

Satz 11.1
Bei der Lösung des allgemeinen Wegproblems in $G = (V, E, c)$, d.h. zur Bestimmung der $c([v_i, v_j])$, $1 \leq i, j \leq n$, führt der Algorithmus von Kleene $O(n^3)$ Operationen im zugrundeliegenden abgeschlossenen Halbring H aus.

11.3 Transitiver Abschluß

Mit Hilfe des im letzten Abschnitt vorgestellten Algorithmus von Kleene kann der *transitive Abschluß* $G^* = (V, E^*)$ eines gerichteten Graphen $G = (V, E)$, $n = \#V$ und $e = \#E$, leicht bestimmt werden. Wir arbeiten dazu im *Booleschen Halbring* $\mathcal{B}$, und wählen als Kantenbewertung die charakteristische Funktion $\mathcal{X}_E$ der Kantenmenge E von G.

$$\begin{aligned} \mathcal{X}_E &: V^2 \to \{0,1\} \\ \mathcal{X}_E(u,v) &= \begin{cases} 1 & \text{falls } (u,v) \in E \\ 0 & \text{sonst} \end{cases} \end{aligned}$$

Es ist unmittelbar klar, daß unter diesen Vorraussetzungen (in den Bezeichnungen des letzten Abschnitts) gilt:

Lemma:
Es gilt $c([u,v]) = 1\ ,\ u,v \in V$, genau dann, wenn es in G einen Weg von u nach v gibt, also $(u,v) \in E^*$ gilt.

Folglich ist die Bestimmung des transitiven Abschlusses G^* von G (in Form der Adjazenzmatrix) mit der Prozedur Comp durch die Ausführung von $O(n^3)$ Booleschen Operationen $\vee$ und $\wedge$ möglich. Man beachte, daß dabei die Berechnung in der vorletzten FOR–Anweisung von Comp wegen $0^* = 1^* = 1$ in B stark vereinfacht werden kann zu

$$c'[i,j,k] \leftarrow c'[i,j,k-1] \vee c'[i,k,k-1] \wedge c'[k,j,k-1].$$

11.4 Kürzeste und kostengünstigste Wege

Auch die Bestimmung eines kürzesten bzw. eines kostengünstigsten Weges zwischen zwei Knoten $u,v \in V$ eines gerichteten Graphen $G = (V,E)$ ist mit dem Algorithmus von Kleene leicht möglich.
Ist nämlich $c : E \to \mathbb{R}^+$ eine Kantenbewertung von G im *abgeschlossenen Halbring* $(\mathbb{R}^+ \cup \{\infty\}, inf, +, \infty, 0)$ mit

$$c(u,v) = \infty \text{ falls } (u,v) \notin E,$$

dann liefert $c([u,v])$ offenbar die Kosten eines billigsten Weges von u nach v in G.

Lemma:
$c([u,v])\ ,\ u,v \in V$, beinhaltet die Kosten eines kostengünstigsten Weges von u nach v in G.

Bewertet man jede Kante von G mit 1,

$$\begin{aligned} c &: V^2 \to \mathbb{R}^+ \\ c(u,v) &= \begin{cases} 1 & \text{falls } (u,v) \in E. \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

dann liefert $c([u,v])$ die *Länge eines kürzesten Weges* von u nach v in G.
Folglich können sowohl *kürzeste* als auch *kostengünstigste* Wege in einem gerichteten Graphen $G = (V,E)$ mit der Prozedur Comp berechnet werden, die dazu $O(n^3)$ Infimumbildungen und Additionen auszuführen hat. Man beachte, daß sich auch in diesem Fall die arithmetische Anweisung in der vorletzten FOR–Anweisung wegen $a^* = 0$ für alle $a \in \mathbb{R}^+$ einfach schreibt als

$$c'[i,j,k] \leftarrow min\{c'[i,j,k-1], c'[i,k,k-1] + c'[k,j,k-1]\}.$$

11.5 Wegprobleme und Matrizenmultiplikation

Im fogenden wollen wir den bereits mehrfach zutage getretenen Zusammenhang zwischen der Behandlung von Wegproblemen in gerichteten Graphen und der Multiplikation von Matrizen über abgeschlossenen Halbringen deutlicher herausarbeiten.
Wir bemerken zunächst die einfach zu beweisende Tatsache, daß die Menge $\mathbb{M}_{H,n}$ aller $n \times n$ Matrizen über einem abgeschlossenen Halbring $H = (H, \oplus, \odot, 0, 1)$ einen abgeschlossenen Halbring

$$\mathbb{M}_{H,n} = (\mathbb{M}_{H,n}, \oplus, \odot, (m_{ij})_{1 \leq i,j \leq n}, E_n),$$

bildet, wobei $\oplus$ und $\odot$ für zwei Matrizen $M = (m_{ij})_{1 \leq i,j \leq n}$, $M' = (m'_{ij})_{1 \leq i,j \leq n} \in \mathbb{M}_{H,n}$ definiert sind durch

$$\begin{aligned} M \oplus M' &= (m_{ij} \oplus m'_{ij})_{1 \leq i,j \leq n}, \\ M \odot M' &= (\sum_{1 \leq k \leq n} m_{ik} \odot m'_{kj})_{1 \leq i,j \leq n}, \end{aligned}$$

und

$$E_n = (\delta_{ij})_{1 \leq i,j \leq n}$$

mit

$$\delta_{ij} = \begin{cases} 1 & \text{falls } i = j. \\ 0 & \text{sonst.} \end{cases}$$

Beispiel:
Summe und Produkt Boolescher Matrizen.
Die Summe $M \vee M'$ und das Produkt $M \wedge M'$ zweier Boolescher Matrizen $M, M' \in \mathbb{M}_{B,3}$

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \ , \ M' = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

haben die Gestalt

$$M \vee M' = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \ , \ M \wedge M' = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Betrachtet man M und M' als Matrizen über dem abgeschlossenen Halbring $\mathcal{R}^+$, dann ergeben sich Summe und Produkt als

$$min(M, M') = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \ , \ M + M' = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Im abgeschlossenen Halbring $\mathbb{M}_{H,n}$ aller $n \times n$ Matrizen M sind die Potenzen M^i , $i \in \mathbb{N}$, und der transitive Abschluß M^* (wie üblich) definierbar.
Es gilt:

$$M^0 = E_n \ , \ M^{i+1} = M \odot M^i$$

und

$$M^* = \sum_{0 \leq i \leq \infty} M^i = E \oplus M \oplus M^2 \oplus \ldots .$$

Beispiel:
Der transitive Abschluß M^* der im vorigen Beispiel definierten Booleschen Matrix M hat die Gestalt

$$M^* = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Betrachtet man M dagegen M als Matrix über dem abgeschlossenen Halbring $\mathcal{R}^+$, dann gilt:

$$M^* = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Wir sind nun in der Lage, den Zusammenhang zwischen den Brechnungen zum Wegproblem und der Matrizenmultiplikation formal zu fassen. Sei also $G = (V, E, c)$ ein gerichteter Graph mit der Knotenmenge $V = \{v_1, \ldots v_n\}$ und einer Kantenbewertung $c : V^2 \to H$ im abgeschlossenen Halbring $H = (H, \oplus, \odot, 0, 1)$, für die $c(u, v) = 0$ gilt, falls $(u, v) \notin E$. $[u, v]_l$, $l \in \mathbb{N}$ bezeichne die *Menge aller Wege* in G von u nach v der Länge l. Dann gilt:

Satz 11.2
Ist $C_G = (c_{ij}) \in \mathbb{M}_{H,n}$ *definiert durch* $c_{ij} = c(v_i, v_j)$, $1 \leq i, j \leq n$, *dann gilt für alle* $l \in \mathbb{N}$

$$C_G^l = (c([v_i, v_j]_l))_{1 \leq i,j \leq n}.$$

Beweis:
Übungsaufgabe. □

Korollar
Für den transitiven Abschluß $C_G^* = (\hat{c}_{ij})$ der Matrix C_G gilt

$$\hat{c}_{ij} = c([v_i, v_j]).$$

Damit ist die Lösung des allgemeinen Wegproblems äquivalent zur Berechnung des transitiven Abschlusses einer Matrix über einem abgeschlossenen Halbring. Insbesondere läßt sich der transitive Abschluß M^* einer Matrix $M \in \mathbb{M}_{H,n}$, $H = (H, \oplus, \odot, 0, 1)$ mit Hilfe des Algorithmus von Kleene durch die Ausführung von $O(n^3)$ Operationen $\oplus, \odot$ und * aus H berechnen.
Interessanterweise ist auch die Produktbildung zweier Matrizen über einem abgeschlossenen Halbring H in ihrer Berechnungskomplexität äquivalent zur Berechnung des transitiven Abschlusses einer Matrix bzw. zur Lösung des allgemeinen Wegproblems, wie die beiden folgenden Sätze beweisen.

Satz 11.3

Kann der transitive Abschluß einer $n \times n$ Matrix über einem abgeschlossenen Halbring $H = (H, \oplus, \odot, 0, 1)$ durch die Ausführung von $T(n)$ Operationen $\oplus, \odot$ und * berechnet werden, dann gilt für die zur Multiplikation zweier $n \times n$ Matrizen erforderliche Anzahl $T'(n)$ von Operationen:

$$T'(n) = O(T(n)).$$

Beweis:

Seien $M, M' \in I\!M_{H,n}$. Wir zeigen, daß das Produkt $M \odot M'$ von M und M' über die Berechnung des transitiven Abschluß C^* der $3n \times 3n$ Matrix

$$C = \begin{pmatrix} 0 & M & 0 \\ 0 & 0 & M' \\ 0 & 0 & 0 \end{pmatrix}$$

berechnet werden kann.
Mit $E = E_n$ gilt nämlich:

$$C^* = \begin{pmatrix} E & M & M \odot M' \\ 0 & E & 0 \\ 0 & 0 & E \end{pmatrix}.$$

□

Satz 11.4

Kann das Produkt zweier $n \times n$ Matrizen über einem abgeschlossenen Halbring $H = (H, \oplus, \odot, 0, 1)$ durch die Ausführung von $T'(n)$ Operationen $\oplus, \odot$ und * berechnet werden, dann gilt für die zur Berechnung des transitiven Abschluß einer Matrix erforderlichen Anzahl $T(n)$ von Operationen

$$T(n) = O(T'(n)).$$