

DML II

Mitschriften der Vorlesung von Dr. Jörg Vogel

Script von
Owczarek, Andreas
SS 2004

1. Kapitel: Aussagenlogik

§1. Logische Antinomien und Paradoxien

Die Paradoxie des Lügners

1. Fassung: stammt aus philosophischem Magazin (6. Jh. v. Chr.)

Ein Lügner soll folgende Frage beantworten:

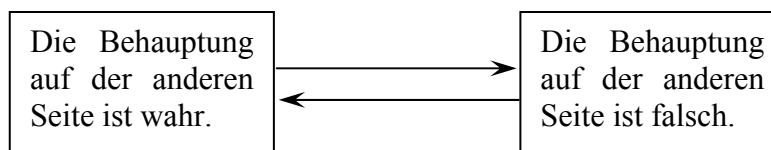
„Lügst du, wenn du sagst, dass du lügst?“

1. Antwort: „Ich lüge.“ → Dann lügt er also nicht.
2. Antwort: „Ich lüge nicht.“ → Dann ist es wahr, dass er lügt.

2. Fassung: Kreter Philosoph Epidemides

„Alle Kreter sind Lügner.“

3. Fassung: Pseudonym „Ich lüge.“
4. Fassung: „Dieser Satz ist nicht wahr.“
5. Fassung: „Diese Aussage ist falsch“
6. Fassung: „Visitenkarte“



gemeinsam: Sie erzwingen widersprüchliche Aussagen über die Wahrheitswerte der einzelnen Aussagen

Problem: Auflösung dieser Widersprüche

1. Deutung: Aristoteles „sophistische Abhandlungen“:
eine Aussage wird gebrochen und eine gehalten
(Seneku & Cicero)
2. Deutung: (12. Jh.)
 1. Sokrates schwört, dass alles das er sagt, falsch ist.
 2. Sokrates sagt: „Sie sind ein Stein.“
Also kann eine Person offensichtlich gleichzeitig lügen und die Wahrheit sagen.
3. Deutung: Wilhelm von Ocken: Aspekt der Selbstbezüglichkeit
→ eine Aussage, die die Begriffe „wahr“ und „falsch“ enthält, darf nicht im Referenzbereich dieser Begriffe einbezogen werden.
4. Deutung: Bertrand Russell:
Die Ursache für Lügner Paradoxien sind dieselben wie bei Mengen Paradoxien.
Sind Zirkelschlüssel, die von der Annahme ausgehen: „Eine Menge könne Elemente enthalten, die nur durch die Menge selbst definiert werden.“

Ausweg: „Typentheorie“

Objekte bilden Typ O (Dinge wie $x+y$) Aussagen über diese Objekte sind Typ 1 („ x ist schwarz“, „ y ist alt“)

Aussage über Aussage vom Typ 1 sind vom Typ 2 („schwarz ist eine Farbe“, „Alt ist eine zeitliche Eigenschaft“)

allgemein:

Eine Aussage über die Wahrheit oder Falschheit einer Aussage vom Typ n ist vom Typ $n+1$

5. Deutung: Alfred Tarski (1969) „proof + truth“

Ansatz:

Wir brauchen eine Unterscheidung zwischen 1. einer „Objektsprache“ – stellt den Gegenstand der Erörterung dar, für die die Wahrheitsdefinition angewendet werden und 2. einer „Metasprache“ – in der die Wahrheitsdef. erfolgen und die hieraus bezogenen Schlussfolgerungen.

Tarskis Wahrheitsdefinition:

Ein Satz ist wahr, wenn er den existierenden Zustand beschreibt.

Ein Satz ist falsch, wenn er den existierenden Zustand nicht beschreibt.

(semantische Wahrheitsdefinition)

Wir diskutieren den folgenden Satz:

(1) Der Satz auf Seite 75, Zeile 3-4 dieses Buches ist falsch.

Diesen Satz kürzt er mit dem Symbol „S“ ab.

Dieser Satz steht gerade auf Seite 75, Zeile 3-4 dieses Buches.

(2) „S“ ist dann, und nur dann falsch, wenn der Satz auf S. 75, Z. 3-4, dieses Buches falsch ist. Auf Grund der Wahrheitsdefinition können wir folgendes sagen

(3) „S“ ist dann, und nur dann wahr, wenn „S“ für den kompletten Satz (1) steht. Also können wir in jedes Vorkommen von „S“ Satz (1) substituieren.

Wir erhalten:

(4) „S“ ist nur dann wahr, wenn der Satz auf Seite 75, Zeile 3-4 des Buches falsch ist.

Vgl. von (3) und (4) führt zu:

(5) „S“ ist dann und nur dann wahr, wenn „S“ falsch ist.

Schlussfolgerung: Es ist unmöglich eine Definition von Wahrheit und Falschheit zu geben, wenn Metasprache von derselben Ordnung wie die Objektsprache ist.

1. Fazit: Alle natürlichen Sprachen sind inkonsequent in Bezug auf die Unterscheidung der Sprachebene (und erlauben genau aus diesem Grund Zirkelschlüsse).

Die Paradoxie des Lügners weist auf diese Inkonsequenz hin.

Dies ist ein Argument für die Einführung formaler Sprachen – wie eben die

Aussagenlogik, aber auch aller Programmiersprachen → denn gemeinsam ist, dass jede Definition zwei Ebenen hat:

- Syntax (Objektebene)

- Semantik (Metasprache)

2. Fazit: Bezug zu den Unvollständigkeitssätzen von Gödel.
Es gibt keine Axiomsysteme, die gleichzeitig vollständig (wahr) und widerspruchsfrei (falsch) sind.

Ein Aspekt der Logik ist die Untersuchung der Begriffe „Widerspruchsfreiheit“ und „formaler Beweis“.

Das Krokodil-Dilemma

Das Krokodil bricht nimmer sein Wort:

„Wenn du voraussagst was ich mit dem Kind mache, werde ich es nicht fressen“
(Autor: Alice im Wunderland)

Die Barbier-Paradoxie

„Barbier rasiert alle, die sich nicht selber rasieren. Wer rasiert Barbier?“
(Bertrand Russell 1918)

Analogie zur Russellschen Mengenautonomie

Wir teilen alle Männer in zwei Mengen
X... alle Männer, die sich selbst rasieren
Y... alle Männer, die sich nicht selbst rasieren

Frage: Zu welcher Menge gehört der Barbier?

1. Fall: $B \in X \rightarrow B \in Y$
2. Fall: $B \in Y \rightarrow B \in X$

d.h. $B \in X \leftrightarrow B \notin X$ genauso wie Russellsche Mengen: $R = \{M \mid M \notin M\}$

Frage: Wohin gehört R? $R \in R \leftrightarrow R \notin R$ Russellsches Paradoxon

Schlussfolgerung: Diesen Barbier gibt es nicht.

Die Mengen-Antinomie

Mengenbildung:

Wir definieren die folgende Menge: $R = \{M \mid M \notin M\}$ (alle Mengen M, die nicht Element der Menge M sind)

Frage:

Wo gehört R hin? D.h. hat R selbst diese Eigenschaft oder nicht? D.h. gilt $R \in R$ oder $R \notin R$?

1. Fall: angenommen $R \in R$: dann gilt $R \notin R$
2. Fall: angenommen $R \notin R$: dann gilt $R \in R$

Es ergibt sich folgende widersprüchliche Aussage (in jeder Situation falsch), denn $R \in R$ genau dann wenn (gdw) $R \notin R$!

Was ist eine Menge?

Cantor: Eine Menge ist eine Zusammenfassung von wohl unterscheidbaren Individuen, die Elemente der Menge heißen.

Schreibweise: $x \in M$

Die Elementbeziehung \in

Die Elementbeziehung beschreibt die Zuordnung zwischen Elementen und Mengen. Zwei Mengen sind folglich genau dann gleich, wenn Sie dieselben Elemente haben.

$A_{(\text{Menge})} = \{n_{(\text{Element})} \mid n \text{ ist Primzahl kleiner als } 10\}$

$B = \{x \mid x \text{ ist Lösung der Gleichung } (x-2)(x-3)(x-5)(x-7) = 0\}$

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

Eine Menge A heißt Teilmenge einer Menge B gdw jedes Element von A auch Element von B ist:

$$\hat{=} (a \in A \rightarrow a \in B) \text{ bzw. } A \subseteq B$$

Die Potenzmenge

$\wp(B) = \{A \mid A \subseteq B\}$ heißt **Potenzmenge** von B.

Einer-, Zweier-, Dreier-, Vierer- und Nullmenge

1 Nullmenge: $V = \emptyset$

4 Einermengen: $W = \{\{2\}, \{3\}, \{5\}, \{7\}\}$

6 Zweiermengen: $X = \{\{2, 3\}, \{2, 5\}, \{2, 7\}, \{3, 5\}, \{3, 7\}, \{5, 7\}\}$

4 Dreiermengen: $Y = \{\{2, 3, 5\}, \{3, 5, 7\}, \{2, 5, 7\}, \{2, 3, 7\}\}$

1 Vierermenge: $Z = \{\{2, 3, 5, 7\}\}$

$\wp(C) = \{V, W, X, Y, Z\}$

→ insgesamt erhält man folglich $2^4 = 16$ Teilmengen

Jede Menge mit n Elementen hat 2^n Teilmengen.

Zuordnung: $A \mapsto C \setminus A = \bar{A}$ (alle Elemente von C, die nicht zu A gehören bilden das **Komplement** von A)

§2. Syntax und Semantik der Aussage

Literaturhinweise: Uwe Schöning: ‚Logik für Informatiker‘
Dirk Siefkes: ‚Formalisieren und Beweisen‘

Eine **Aussage** ist ein sprachliches Gebilde von dem es *sinnvoll* ist, zu sagen, dass es entweder wahr oder falsch ist.

„sinnvoll“ → Das **Prinzip der Zweiwertigkeit (Tertium non datur)** ist das grundlegende Axiom der klassischen Aussagenlogik.

Beispiele:

1. „Es gibt unendlich viele Primzahlen.“
→ *wahre Aussage*
2. „Es gibt unendlich viele gerade Primzahlen.“
→ *wahre Aussage*
3. „Es gibt unendlich viele Primzahlzwillinge.“
→ *Aussage, deren Wahrheitswert nicht bekannt ist, dennoch ist sie entweder wahr oder falsch*
4. „Diese Aussage ist falsch.“ (Antinomie des Lügners)
→ *keine Aussage, da es nicht sinnvoll ist, ihr einen Wahrheitswert zuzuordnen*
5. „Diese Aussage ist keine Aussage.“
Ist dies ein Paradoxon?
 1. Fall: Es ist eine wahre Aussage. → Widerspruch!
 2. Fall: Es ist eine falsche Aussage. → kein Widerspruch
→ *kein Paradoxon, sondern eine falsche Aussage*
6. „Ist dies eine Aussage?“
→ *Ist keine Aussage, sondern eine Frage*

Schlüsse ziehen

Beispiele:

1. „In einem Supermarkt stehen 136 Apfelsinenkisten.“
„In jeder Kiste befinden sich mindestens 140 Apfelsinen.“
„In jeder Kiste befinden sich höchstens 166 Apfelsinen.“

Konsequenz: „Dann gibt es mindestens 6 Apfelsinenkisten, die dieselbe Anzahl von Apfelsinen enthalten.“

Frage: Ist das ein korrekter Schluss?

Antwort: Ja, wenn alle Aussagen (Voraussetzungen) wahr sind, ist auch die Konsequenz wahr.

Bei einem korrekten Schluss hat die Wahrheit der Voraussetzungen stets die Wahrheit der Konsequenz zur Folge.

2. „Alle Menschen sind klug.“
„Alle Primaten sind Menschen.“

Konsequenz: „Also sind Primaten klug.“

Frage: Ist das ein korrekter Schluss?

Antwort: Ja, obwohl alle Aussagen falsch sind.

3. „Alle Senatoren sind alt.“
„Alle 80er sind Senatoren.“

Konsequenz: „Also sind alle 80er alt.“

Frage: Ist das ein korrekter Schluss?

Antwort: Ja, obwohl alle Voraussetzungen falsch sind, ist die Konsequenz wahr.

4. „Einige Senatoren sind alt.“
„Einige Generäle sind Senatoren.“

Konsequenz: „Also sind einige Generäle alt.“

Frage: Ist das ein korrekter Schluss?

Antwort: Nein, obwohl Situationen möglich sind, wo alle Aussagen wahr sind. ABER:
Es gibt Situationen, wo die Voraussetzungen wahr sind, aber die Konsequenz falsch ist.

5. „Einige Studenten sind Schweden.“
„Einige Norweger sind Studenten.“

Konsequenz: „Also sind einige Norweger Schweden.“

Frage: Ist das ein korrekter Schluss?

Antwort: Nein, denn die Voraussetzungen sind wahr, die Konsequenz jedoch nicht.

6. „Die Anzahl der Sterne in unserer Milchstraße ist größer als vier und gerade.“

Konsequenz: „Also ist die Anzahl der Sterne unserer Milchstraße die Summe zweier Primzahlen.“

Frage: Ist das ein korrekter Schluss?

Antwort: Unbekannt, ob dieser Schluss korrekt ist, da der Wahrheitswert der Voraussetzung nicht bekannt ist, falls sie zutrifft, wäre die Konsequenz jedoch richtig.

Aussageverknüpfungen

Durch Formalisieren werden aus Aussagen **FORMELN**.

Beispiele:

1. „ $3 < 7$ “ \rightarrow A – Aussagenvariable (Platzhalter für eine Aussage)
2. „Jena ist die Hauptstadt Thüringens.“ \rightarrow B
3. „Alle Senatoren sind alt.“ \rightarrow C
4. „Einige Senatoren sind alt.“ \rightarrow D

Fakt: Die aussagenlogische Formalisierung (einfache Aussagen werden Platzhalter zugeordnet/ersetzt) spiegelt die Feinstruktur der Aussagen nicht wider.

Damit aber die Art und Weise der Verknüpfung zwischen Aussagen.

Beispiele für Verknüpfungen:

1. „A und B.“
„Sowohl A als auch B.“
„A aber auch B.“

 \Rightarrow **KONJUNKTION** \wedge
2. „A oder B.“

 \Rightarrow **AD-/DISJUNKTION** \vee
3. „Entweder A oder B.“

 \Rightarrow **ANTIVALENZ** \oplus
4. „Wenn A dann B.“
„A hat B zur Folge.“
„Wenn A so B.“

 \Rightarrow **IMPLIKATION (SUBJUNKTION)** \rightarrow
5. „A genau dann wenn B.“
„A dann und nur dann, wenn B.“

 \Rightarrow **BIJUNKTION (ÄQUIVALENZ)** \leftrightarrow
6. „Weder A noch B.“

 \Rightarrow **NIHILITION** \downarrow
7. „Nicht zugleich A und B.“

 \Rightarrow **UNVERTRÄGLICHKEIT** \uparrow
8. „Nicht A.“

 \Rightarrow **NEGATION** \neg

Syntax der Aussagenlogik

Aussagenlogische Formalisierung umfasst eine doppelte Reduktion:

1. Aussagen werden durch Variablen, sog. **Aussagenvariablen** ersetzt.
2. Aussagenverknüpfungen werden durch Symbole, sog. **Junktoren** ersetzt.

Damit ergibt sich ein Zeichenvorrat.

Aussagenvariablen: $\mathcal{A} = \{A_0, A_1, A_2, \dots\}$ (Menge der Aussagenvariablen)

Junktoren: $\wedge, \vee, \rightarrow, \leftrightarrow, \neg$

Hilfsvariablen: $(,)$

Definition (induktive Definition der aussagenlogischen Formeln)

Induktionsanfang: Jede Aussagenvariable ist eine Formel.

Induktionsschritt: Es seien F und G bereits Formeln. Dann sind auch:

1. $(F \wedge G)$,
2. $(F \vee G)$,
3. $(F \leftrightarrow G)$,
4. $(F \rightarrow G)$,
5. $\neg F$ Formeln.

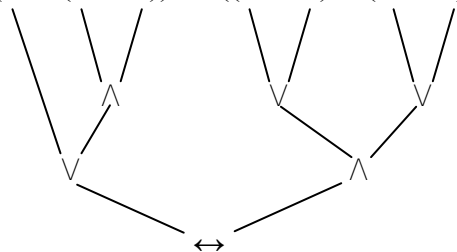
Induktionsschluss: Sonst gibt es keine Formeln.

Vereinbarungen:

1. einfachste Formeln sind die Aussagenvariablen aus \mathcal{A} , die daher atomare Formeln bzw. Atome heißen.
2. Mitteilungszeichen für Atome: $\neg A_0, A_1, A_2, \dots$
 $\neg A, B, C, \dots$
3. Mitteilungszeichen für Formeln: $\neg F, G, H, \dots$
4. Mitteilungszeichen (Bezeichner) für Mengen von Formeln:
 $\neg X, Y, Z$

Beispiele:

1. $(A \rightarrow (B \vee \neg B))$ – Diese Zeichenkette ist eine Formel gemäß der induktiven Definition.
2. $((A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C)))$



Jede Formel definiert (gemäß der induktiven Definition) einen **Strukturbaum**.

Syntax der Formeln

→ Jede Formel definiert ihren **Strukturbaum** (gemäß der induktiven Definition)

→ Damit ist es (prinzipiell) möglich für eine Zeichenreihe zu entscheiden, ob es eine Formel ist oder nicht.

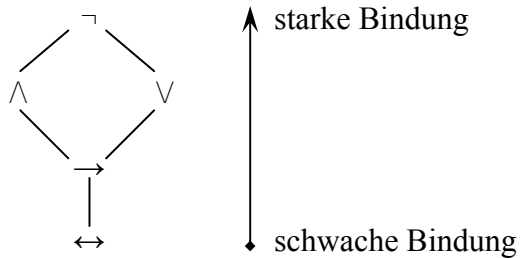
→ **Klammereinsparungsregel**

z.B. $(A \rightarrow (B \vee \neg B))$ geht über in:

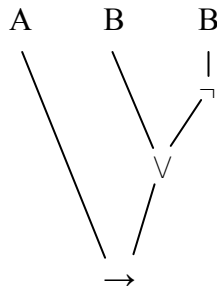
$A \rightarrow (B \vee \neg B)$ } Außenklammern entfallen

$A \rightarrow B \vee \neg B$ } Hierarchie der Junktoren

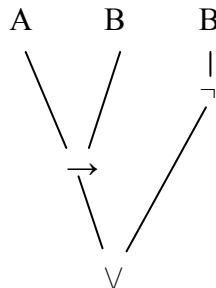
Hierarchie der Junktoren:



im Unterschied zu: $(A \rightarrow B) \vee \neg B$



⇒ Implikation



⇒ Disjunktion

Teilformeln:

Eine Formel F heißt Teilformel einer Formel G

1. F ist eine Formel und
2. F kommt in G vor (F ist ein Teilwert von G)

Beispiele:

Teilformeln von $A \rightarrow (B \vee \neg B)$:

- A, B
- $\neg B$
- $(B \vee \neg B)$
- $A \rightarrow (B \vee \neg B)$

aber:

- $A \rightarrow$ } keine Formel im Sinn der Syntax
 - $(A \rightarrow B)$ } Formel, die so nicht vorkommt
- sind keine Teilformeln!

Formelinduktion (Ausdrucksinduktion)

Beweismethode für Formeln gemäß der induktiven Definition der Syntax
 ε bezeichne eine Eigenschaft für Formeln

Schreibweise: $\varepsilon(F)$ Formel F hat die Eigenschaft ε

Wenn gilt:

Induktionsanfang: $\varepsilon(A)$ für alle Atome $A \in \mathcal{A}$ und

Induktionsschritt: mit $\varepsilon(F)$ und $\varepsilon(G)$ gilt

1. $\varepsilon(F \wedge G)$
2. $\varepsilon(F \vee G)$
3. $\varepsilon(F \rightarrow G)$
4. $\varepsilon(F \leftrightarrow G)$
5. $\varepsilon(\neg F)$

dann gilt: $\varepsilon(F)$ für alle Formeln

Semantik der Aussagenlogik

Die Menge der (zulässigen) Wahrheitswerte ist gegeben durch $B = \{0,1\} = \{\text{wahr, falsch}\}$
 \Rightarrow **boolesche Werte**

- I. Eine **Belegung** β ist eine Abbildung von der Menge der Atome in die Menge der Wahrheitswerte
$$\beta: \mathcal{A} \mapsto B \quad (\text{jedem Atom wird ein Wahrheitswert zugeordnet})$$
- II. Eine **Interpretation** I_β ist eine Abbildung von der Menge aller Formeln in die Menge der Wahrheitswerte, die auf folgende Weise als Fortsetzung von β definiert ist.

Induktionsanfang: $I_\beta(A) = \beta(A)$ für alle Atome $A \in \mathcal{A}$

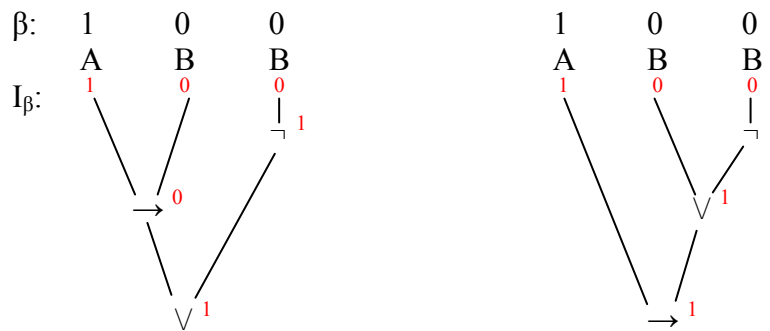
Induktionsschritt: für gegebene $I_\beta(F)$ und $I_\beta(G)$ wird definiert:

1. $I_\beta(F \wedge G) = \min\{I_\beta(F), I_\beta(G)\}$
2. $I_\beta(F \vee G) = \max\{I_\beta(F), I_\beta(G)\}$
3. $I_\beta(F \rightarrow G) = 1$ gdw $I_\beta(F) \leq I_\beta(G)$
4. $I_\beta(F \leftrightarrow G) = 1$ gdw $I_\beta(F) = I_\beta(G)$
5. $I_\beta(\neg F) = 1 - I_\beta(F)$

Kommentare:

- für eine Formel F heißt $I_\beta(F)$ der **Wert der Formel F bei der Belegung β**
–die **Formelinduktion** garantiert, dass bei gegebener Belegung β die Werte $I_\beta(F)$ für alle Formeln F definiert sind
– \mathcal{L}_{AL} bezeichnet die Menge aller aussagenlogischen Formeln: $I_\beta: \mathcal{L}_{AL} \mapsto B$
- Die formale Definition der Semantik der Aussagenlogik erlaubt ein formales Berechnen der Wahrheitswerte (Bedeutung) der Formeln.

Beispiele: Ausgangspunkt ist eine Belegung β



Dabei gilt das **Prinzip der Extensionalität** (Grundaxiom der Aussagenlogik).
→ der Wert einer zusammengesetzten Formel hängt von den Werten der Teilformeln ab, jedoch nicht von deren Inhalt.

III. Jeder logische Junktor definiert eine sog. **Boolesche Funktion**:

$I_\beta(F)$	$I_\beta(G)$	$I_\beta(F \wedge G)$	$I_\beta(F \vee G)$	$I_\beta(F \rightarrow G)$	$I_\beta(F \leftrightarrow G)$	$I_\beta(\neg F)$	$I_\beta(\neg G)$
0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	0
1	0	0	1	0	0	0	1
1	1	1	1	1	1	0	0

Die formale Definition liefert die üblichen Wahrheitswerttabellen. Diese konkreten Funktionen haben konkrete Namen (Bezeichnungen):

et:	$\{0,1\}^2 \mapsto \{0,1\}$	}	zweistellige Boolesche Funktionen
vet:	$\{0,1\}^2 \mapsto \{0,1\}$		
seq:	$\{0,1\}^2 \mapsto \{0,1\}$		
äq:	$\{0,1\}^2 \mapsto \{0,1\}$		
non:	$\{0,1\} \mapsto \{0,1\}$	}	einstellige Boolesche Funktion

IV. Die formale Definition der Semantik entspricht der umgangssprachlichen Bedeutung der Aussageverknüpfungen.

Beispiele:

(**fett gedruckt** $\hat{=}$ formale Definition der Semantik (Junktor);
fett-kursiv gedruckt $\hat{=}$ umgangssprachlicher Formulierung)

Konjunktion: $I_{\beta}(F \wedge G) = 1$ gdw $I_{\beta}(F) = 1$ **und** $I_{\beta}(G) = 1$
Disjunktion: $I_{\beta}(F \vee G) = 1$ gdw $I_{\beta}(F) = 1$ **oder** $I_{\beta}(G) = 1$
Implikation: $I_{\beta}(F \rightarrow G) = 1$ gdw $I_{\beta}(F) = 0$ oder $I_{\beta}(G) = 1$,
d.h. $F \rightarrow G$ ist wahr, wenn gilt:
wenn F wahr ist, **dann** muss G wahr sein;

 $I_{\beta}(F \rightarrow G) = 0$ gdw $I_{\beta}(F) = 1$ oder $I_{\beta}(G) = 0$,
Wenn etwas Wahres etwas Falsches impliziert,
dann ist die gesamte Implikation falsch.

§3. Modelle, Äquivalenzen, Folgerungen

Gegeben sei eine Formel F und ein Belegung β : $\beta: \mathcal{A} \mapsto B$

In jeder konkreten Formel kommen nur endlich viele Atome aus der (unendlichen) Menge \mathcal{A} vor.

Schreibweise: $F(A_1, A_2, A_3, \dots, A_n)$ bedeutet: die Atome A_1 bis A_n kommen in F vor.

Der Wert von F hängt nur ab, von den Belegungen der Atome, die in F vorkommen

\Rightarrow Betrachtung der Belegung dieser Atome genügt

Eine solche Belegung heißt zu F **passende Belegung**.

Wir beschränken uns im Folgenden grundsätzlich auf passende Belegungen.

Definition

Es sei F eine Formel und β eine passende Belegung: $\beta: \{A_1, A_2, \dots, A_n\} \mapsto B$.

1. β heißt **Modell** für $F \leftrightarrow_{\text{df}} I_\beta(F) = 1$. (Eine Belegung β ist Modell für F , wenn sie die Formel F wahr macht.)
2. F ist **erfüllbar** $\leftrightarrow_{\text{df}}$ F besitzt ein Modell.
3. F ist **gültig** (Tautologie) $\leftrightarrow_{\text{df}}$ jede (passende) Belegung macht F wahr und ist somit Modell für F .
4. F ist **unerfüllbar** $\leftrightarrow_{\text{df}}$ jede Belegung ist kein Modell für F .

Modelle

F sei eine Formel, d.h. $F \in \mathcal{L}_{AL}$.

Eine Belegung β ist Modell für $F \leftrightarrow_{\text{df}} I_\beta(F) = 1$, d.h. β macht die Formel wahr.

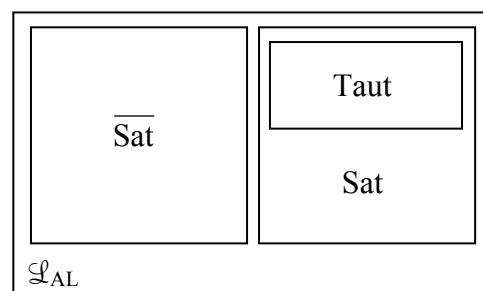
1. F ist erfüllbar \leftrightarrow es gibt eine Belegung β , die Modell für F ist.
2. F ist Tautologie \leftrightarrow jede Belegung β ist Modell für F .
3. F ist unerfüllbar \leftrightarrow keine Belegung β ist Modell für F .

Schreibweisen:

$\text{Sat} = \{F \in \mathcal{L}_{AL} \mid F \text{ ist erfüllbar}\}$

$\text{Taut} = \{F \in \mathcal{L}_{AL} \mid F \text{ ist Tautologie}\}$

$\overline{\text{Sat}} = \{F \in \mathcal{L}_{AL} \mid F \text{ ist unerfüllbar}\}$



Fakt: Für die Anwendungen der Logik in der Informatik sind insbesondere Tests der Form:

Gegeben sei eine Formel $F \in \mathcal{L}_{AL}$.

Frage: Ist $F \in \text{Sat}$? (Ist F erfüllbar?) oder

Frage: Ist $F \in \text{Taut}$? (Ist F gültig?)

klar ist: derartige Tests sind *prinzipiell* lösbar! Warum?

⇒ Für jede Formel wird jede passende Belegung β durchgeführt (durchgemustert), d.h. für jedes β wird $I_\beta(F)$ berechnet. Dies geht mechanisch.

Das Problem besteht nicht darin für ein gegebenes β $I_\beta(F)$ zu bestimmen, **aber** es kann ein Problem sein, alle Belegungen durchmustern zu müssen.

Die Formalisierung realweltlicher Probleme erzeugt Formeln mit/ in der Größenordnung von **100** Atomen $\rightarrow 2^{100} \approx 1,27 \cdot 10^{30}$ verschieden Belegungen

Was bedeutet dies?

Annahme: Wir haben einen Rechner, der etwa eine Million Belegungen pro Sekunde testen kann.

Dann gilt: $1000000 \approx 2^{20}$ Also benötigt der Rechner
 $2^{100}/2^{20} = 2^{80}$ Sekunden $\approx 5,6 \cdot 10^{18}$ h $\approx 3 \cdot 10^{16}$ Jahre
⇒ prinzipiell; praktisch jedoch sehr langwierig!

Zentrale Fragestellung: Gibt es **effiziente** (praktisch machbare) Erfüllbarkeitstests?

Wir betrachten praktisch handhabbare Probleme:

Beispiel einer Tautologie: $F := (A \leftrightarrow B) \leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A)) = (A \leftrightarrow B) \leftrightarrow (F_1 \wedge F_2)$
Begründung:

$I_\beta(A)$	$I_\beta(B)$	$I_\beta(A \leftrightarrow B)$	$I_\beta(A \rightarrow B)$	$I_\beta(B \rightarrow A)$	$I_\beta(F_1 \wedge F_2)$	$I_\beta(F)$
0	0	1	1	1	1	1
0	1	0	1	0	0	1
1	0	0	0	1	0	1
1	1	1	1	1	1	1

alle Belegungen
sind Modell für F

Definition

Es seien F und G aussagenlogische Formeln. F und G heißen **semantisch äquivalent** \leftrightarrow_{df} für alle passenden Belegungen gilt:

$$I_\beta(F) = I_\beta(G)$$

Schreibweise: $F \models G$

Satz: $F \models G$ gdw $(F \leftrightarrow G) \in \text{Taut}$

Beweis: Es sei $F \models G$, d.h. für alle Belegungen β gilt, $I_\beta(F) = I_\beta(G)$, d.h. für alle Belegungen β gilt: $I_\beta(F \leftrightarrow G) = 1$, d.h. $(F \leftrightarrow G) \in \text{Taut}$

Frage: Was ist der Unterschied zwischen „ \leftrightarrow “ und „ \models “?

„ \leftrightarrow “ ist ein **Symbol der Syntax** der Aussagenlogik, ein **logischer Junktor**, der die **Bijunktion** bezeichnet; deshalb ist $(F \leftrightarrow G)$ eine **Formel**.

aber:

$(F \models G)$ ist **keine Formel**.

„ \models “ ist ein **Symbol**, welche ein **zweistellige Relation über der Menge aller Formeln**, die **semantische Äquivalenz** bezeichnet.

Damit ist $F \models G$ ein **Aussage** über Formeln!

Jede aussagenlogische Formel F definiert ein **Boolesche Funktion**.

Boolesche Funktion

Es sei F eine Formel mit den Atomen A_1, A_2, \dots, A_n ; $F(A_1, A_2, \dots, A_n)$;
 F definiert auf folgende Weise eine n -stellige **Boolesche Funktion**.

$f_F: \{0,1\}^n \mapsto \{0,1\}$, wobei gilt:

$f_F: (x_1, \dots, x_n) = y$ gdw für $\beta(A_1) = x_1, \dots, \beta(A_n) = x_n$ gilt: $I_\beta(F) = y$

Beispiel:

Betrachtung von $F(A_1, A_2, A_3) := (A_1 \vee A_2) \rightarrow (A_1 \rightarrow A_3)$; Tabelle für f_F :

x_1	x_2	x_3	$f_F(x_1, x_2, x_3)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Fakt: Für zwei Formeln gilt $F \models G$ gdw $f_F = f_G$.

D.h. die semantische Äquivalenz ist eine Äquivalenzrelation über die Menge aller Formeln.

\Rightarrow d.h. \models ist reflexiv ($F \models F$)

\models ist symmetrisch ($F \models G \rightarrow G \models F$)

\models ist transitiv ($F \models G, G \models H \rightarrow F \models H$)

und bewirkt eine Zerlegung der Menge aller Formeln in Klassen äquivalenter Formeln.
 \Rightarrow z.B. alle Tautologien mit 3 Atomen liegen in ein und derselben Klasse

Rechenregeln für das Rechnen mit äquivalenten Formeln

1. $F \wedge G \models G \wedge F$
 $F \vee G \models G \vee F$ ||
 \Rightarrow **Kommutativität**
2. $F \wedge (G \wedge H) \models (F \wedge G) \wedge H$
 $F \vee (G \vee H) \models (F \vee G) \vee H$
 \Rightarrow **Assoziativität**
3. $F \wedge (F \vee G) \models F$
 $F \vee (F \wedge G) \models F$
 \Rightarrow **Absorption**
4. $\neg\neg F \models F$
 \Rightarrow **Doppelnegation**
5. $\neg(F \wedge G) \models \neg F \vee \neg G$
 $\neg(F \vee G) \models \neg F \wedge \neg G$
 \Rightarrow **De Morgan**
6. $F \wedge (G \vee H) \models (F \wedge G) \vee (F \wedge H)$
 $F \vee (G \wedge H) \models (F \vee G) \wedge (F \vee H)$
 \Rightarrow **Distributivregeln**
7. Es sei F eine Tautologie ($F \in \text{Taut}$). Dann ist:
 $F \wedge G \models G$ und $F \vee G \models F$
 \Rightarrow **Tautologieregeln**
8. Es sei $F \in \overline{\text{Sat}}$ (eine unerfüllbare Formel). Dann gilt:
9. $F \wedge G \models F$ und $F \vee G \models G$
 \Rightarrow **Unerfüllbarkeitsregeln**

Satz: (sog. Ersetzbarkeitstheorem)

Es seien F und E zwei Formeln mit der Eigenschaft $F \models E$. G sei eine Formel, die F als Teilformel enthält. H sei eine Formel, die entsteht, wenn irgendein Vorkommen von F in G durch E ersetzt wird.

Dann gilt: $H \models G$

\Rightarrow Rechtfertigung für die Umformung von Formeln

Beweis:

(durch Formelinduktion, d.h. wir zeigen: alle Formeln G besitzen die Ersetzbarkeitseigenschaft)

Induktionsanfang:

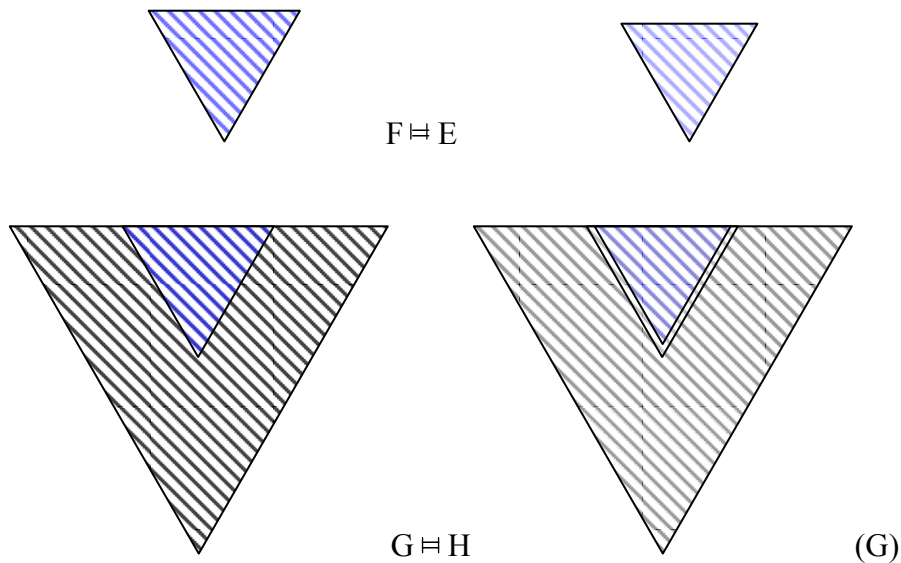
Es sei G ein Atom. D.h. es gibt ein $A \in \mathcal{A}$ mit $G = A$. Es sei F eine Teilformel von G.

Dann gilt: $F = A$

Also gilt $H = E$ und damit $G = A = F \models E = H$, d.h. $G \models H$.

Induktionsschritt:

1. Fall: Es sei $F = G$. Dann ist $H = E$ und damit gilt $G = F \models E = H$, d.h. $G \models H$.
2. Fall: Es sei F eine echte Teilformel von G : $F \neq G$
 - a. G sei eine Konjunktion, d.h. $G = (G_1 \wedge G_2)$ und es gilt: G_1 und G_2 haben die Ersetzbarkeitseigenschaft.
 Da F echte Teilformel von G ist, ist F Teilformel von G_1 oder von G_2 .
 O.B.d.A. sei F eine Teilformel von G_1 . H sei eine Formel, die entsteht indem irgendein Vorkommen von F durch E ersetzt wird. Dann gilt nach Induktionsvoraussetzung: $H_1 \models G_1$ und damit haben wir für irgendeine Belegung β $I_\beta(G) = \min\{I_\beta(G_1), I_\beta(G_2)\} = \min\{I_\beta(H_1), I_\beta(G)\}$.
 H sei eine Formel, die entsteht aus $H = H_1 \wedge G_2$: $I_\beta(G) = I_\beta(H)$
 Also gilt: $G \models H$
 - b. - d. (analog geht man bei Disjunktion, Implikation und Bijunktion vor)
 - e. G habe die Gestalt einer Negation, d.h. $G = G'$
 Nach Induktionsvoraussetzung erfüllt G' die Ersetzbarkeitseigenschaft. Da $F \neq G$ gilt: F ist eine Teilformel (sogar) von G' .
 H' sei eine Formel, die durch Ersetzen eines Vorkommens von F durch E in G' entsteht. Dann gilt $H' \models G'$.
 Weiter gilt: $H = \neg H'$ und für alle Belegungen β gilt:
 $I_\beta(H) = 1 - I_\beta(H') = 1 - I_\beta(G') = I_\beta(G)$.
 Also gilt: $H \models G$



Folgerung

Definition

Eine Formel G ist eine Folgerung einer Formel F , wenn \leftrightarrow_{df} jedes Modell von F ist auch Modell von G .

Schreibweise: $F \models G$

Es sei $F \models G$.

D.h. für alle Belegungen β gilt: $I_\beta(F) = 1 \Rightarrow I_\beta(G) = 1$;

D.h. für alle Belegungen β gilt: $I_\beta(F) \leq I_\beta(G)$;

D.h. für alle Belegungen β gilt: $I_\beta(F \rightarrow G) = 1$;

D.h. $F \rightarrow G$ ist eine Tautologie.

Satz: $F \models G$ (sprich: aus F folgt G bzw. G ist eine Folgerung von F) gdw $(F \rightarrow G) \in \text{Taut}$

Kommentar:

„ \rightarrow “ ist ein Symbol der Syntax und bezeichnet die Implikation und damit ist $F \rightarrow G$ eine Formel.

aber:

$F \models G$ ist **keine** Formel. „ \models “ bezeichnet eine zweistellige Relation für Formeln (**Folgerungsrelation**). Daher ist $F \models G$ eine Aussage über Formeln. „ \models “ ist somit ein Symbol der Semantik.

Es sei $F \models G$.

D.h. für alle Belegungen β gilt: $I_\beta(F) \leq I_\beta(G)$;

D.h. $f_F \leq f_G$; damit erfüllt die Folgerungsrelation \models folgende Eigenschaften:

1. Sie ist **reflexiv**, d.h. für alle Formeln gilt: $F \models F$
2. Sie ist **transitiv**, d.h. wenn aus $F \models G$ und $G \models H$, dann gilt $F \models H$

Diese beiden Eigenschaften charakterisieren die Folgerungsbeziehung \models als

Quasihalbordnung. Diese Quasihalbordnung liefert durch folgenden Ansatz eine Äquivalenzrelation.

allgemein: $F \sim G$ gdw $F \models G$ und $G \models F$

D.h. $F \sim G$ gilt gdw $f_F \leq f_G$ und $f_G \leq f_F$;

D.h. $F \sim G$ gdw $f_F = f_G$;

D.h. $F \sim G$ gdw $F \equiv G$.

Satz: $F \equiv G$ gdw $F \models G$ und $G \models F$

Beispiele:

1. $F := (A \rightarrow B) \wedge A$

$G := B$

Behauptung: Dann gilt $F \models G$.

Begründung:

Es sei β ein Modell von F, d.h. $I_\beta((A \rightarrow B) \wedge A) = 1$. Dann gilt $I_\beta(A) = 1$ und $I_\beta(B) = 1$.

D.h. $\beta(A) = 1$ und damit $\beta(B) = 1$. Also ist β auch ein Modell von G.

2. $F := (A \rightarrow B) \wedge \neg B$

$G := \neg A$

Behauptung: Dann gilt $F \models G$.

Begründung:

Es sei β ein Modell von F, d.h. $I_\beta((A \rightarrow B) \wedge \neg B) = 1$. Dann gilt $I_\beta(A \rightarrow B) = 1$ und

$I_\beta(\neg B) = 1$. D.h. $\beta(B) = 0$ und damit auch $\beta(A) = 0$. D.h. $I_\beta(\neg A) = 1$, d.h. β ist ein Modell von G.

Kommentar:

zu Beispiel 1:

Die Wahrheit von A garantiert die Wahrheit von B.

⇒ Die Wahrheit von A ist **hinreichend** für die Wahrheit von B.

zu Beispiel 2:

Ohne Wahrheit von B keine Wahrheit von A.

⇒ Die Wahrheit von B ist **notwendig** für die Wahrheit von A.

notwendige Bedingung:

in der Implikation $A \rightarrow B$ ist B notwendige Bedingung für A.

hinreichende Bedingung:

in der Implikation $A \rightarrow B$ ist A hinreichende Bedingung für B.

charakterisierende Bedingung:

ist eine Bedingung, die notwendig *und* hinreichend ist, d.h. in der Bijunktion $A \leftrightarrow B$ ist A charakterisierend für B.

§4. Normalformeln und HORN-Formeln

Definitionen

1. Eine Formel der Gestalt $F = A$ für $A \in \mathcal{A}$ heißt **positives Literal**.
Eine Formel der Gestalt $F = \neg A$ für $A \in \mathcal{A}$ heißt **negatives Literal**.
Damit sind **Literale** entweder Atome oder Negationen von Atomen.
2. Eine Formel der Gestalt $F = L_1 \vee L_2 \vee \dots \vee L_n$ für Literale L_1, L_2, \dots, L_n heißt **Disjunktionsterm** oder **Klausel**.
3. Eine Formel der Gestalt $F = L_1 \wedge L_2 \wedge \dots \wedge L_n$ für Literale L_1, L_2, \dots, L_n heißt **Konjunktionsterm**.
4. Eine Formel der Gestalt $F = D_1 \wedge D_2 \wedge \dots \wedge D_n$ für Klauseln D_1, D_2, \dots, D_n heißt **konjunktive Normalform (KNF)**.

Damit gilt:

$$F = D_1 \wedge D_2 \wedge \dots \wedge D_n$$

$$F = \bigwedge_{i=1}^n \left(\bigvee_{j=1}^{m_i} L_{ij} \right) \text{ für Literale } L_{ij}$$

$$F = (L_{11} \vee L_{11} \vee \dots \vee L_{1m_1}) \wedge (L_{21} \vee L_{21} \vee \dots \vee L_{2m_2}) \wedge (\dots) \wedge \dots \wedge L_{nm}$$

5. Eine Formel $F = K_1 \vee K_2 \vee \dots \vee K_n$ für Konjunktionsterme K_1, \dots, K_n heißt **disjunktive Normalform (DNF)**.

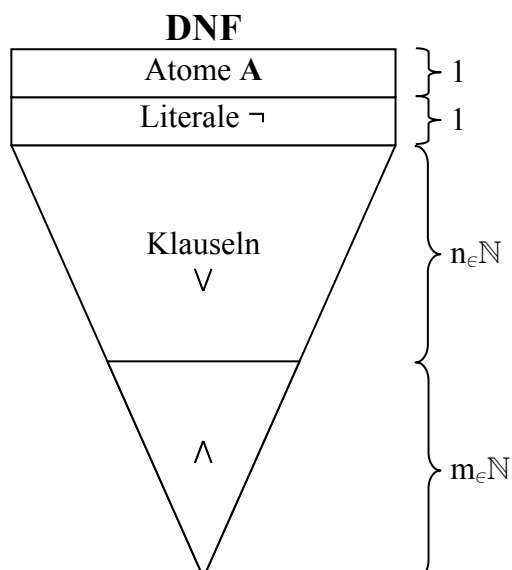
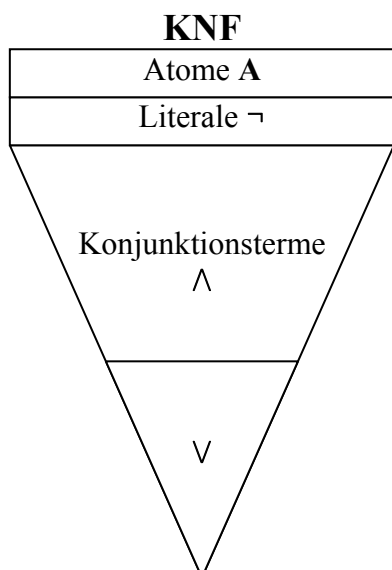
Damit gilt:

$$F = K_1 \vee K_2 \vee \dots \vee K_n$$

$$F = \bigvee_{i=1}^n \left(\bigwedge_{j=1}^{m_i} L_{ij} \right) \text{ für Literale } L_{ij}$$

$$F = (L_{11} \wedge L_{11} \wedge \dots \wedge L_{1m_1}) \vee (L_{21} \wedge L_{21} \wedge \dots \wedge L_{2m_2}) \vee (\dots) \vee \dots \vee L_{nm}$$

Normalformeln besitzen normierte Strukturbäume:



Satz:

Zu jeder aussagenlogischen Formel gibt es eine semantisch äquivalente Formel in KNF und eine semantisch äquivalente Formel in DNF.

Beweis durch Formelinduktion:

Wir zeigen: jede Formel F hat die „KNF-Eigenschaft“ und die „DNF-Eigenschaft“.

Induktionsanfang:

Zeigen: alle Atome $A \in \mathcal{A}$ besitzen die KNF- und DNF-Eigenschaft.

Es sei $F = A$. Dann ist F per Definition sowohl in KNF wie auch in DNF.

Induktionsschritt:

Es seien F und G aussagenlogische Formeln, die die „KNF-Eigenschaft“ und die „DNF-Eigenschaft“ erfüllen.

1. Fall:

Wir betrachten $H := (F \wedge G)$

Wir zeigen:

a. H besitzt die „KNF-Eigenschaft“:

Es sei $F = \bigwedge_{i=1}^n F_i$ und $G = \bigwedge_{j=1}^m G_j$ für Disjunktionsterme F_i und G_j . Dann gilt

$$H = (F \wedge G) \equiv \underbrace{\left(\bigwedge_{i=1}^n F_i \right) \wedge \left(\bigwedge_{j=1}^m G_j \right)}_{\text{ist in KNF}} = \bigwedge_{k=1}^{n+m} H_k \text{ für Disjunktionsterme } H_k.$$

b. H besitzt die „DNF-Eigenschaft“:

Es sei $F = \bigvee_{i=1}^{n'} F_i'$ und $G = \bigvee_{j=1}^{m'} G_j'$ für Konjunktionsterme F_i' und G_j' . Dann

$$\text{gilt } H = (F \wedge G) = \left(\bigvee_{i=1}^{n'} F_i' \right) \wedge \left(\bigvee_{j=1}^{m'} G_j' \right)$$

Die Anwendung des Distributivgesetzes liefert

$$\begin{aligned} H &= \bigvee_{i=1}^{n'} (F_i' \wedge \left(\bigvee_{j=1}^{m'} G_j' \right)) \\ &= \bigvee_{i=1}^{n'} \bigvee_{j=1}^{m'} (F_i' \wedge G_j') && n' \cdot m' \text{ viele Terme} \\ &= \bigvee_{k=1}^{n' \cdot m'} H_k' && \text{für Konjunktionsterme } H_k' \end{aligned}$$

2. Fall:

Wir betrachten $H := (F \vee G)$

Rechnung analog zu Fall 1!

3. Fall:

Wir betrachten $H := (F \rightarrow G)$

Es gilt: $H = (F \rightarrow G) \equiv \neg F \vee G$

Dies wird behandelt wie Fall 2. zusammen mit Fall 5.

4. Fall:

Wir betrachten $H := (F \leftrightarrow G)$

Es gilt: $H = (F \leftrightarrow G) \equiv (F \rightarrow G) \wedge (G \rightarrow F)$

Dies wird behandelt wie Fall 3 und Fall 1.

5. Fall:

Wir betrachten $H := \neg F$

Wir zeigen

a. H besitzt die „KNF-Eigenschaft“.

Es sei $F = \bigvee_{i=1}^n F_i$ für Konjunktionsterme F_i .
DNF (zu F)

Dann gilt: $H := \neg F = \neg \bigvee_{i=1}^n F_i$

nach De Morganscher Regel:

$H = \bigwedge_{i=1}^n (\neg F_i)$

Es sei $F_i = \bigwedge_{j=1}^{m_i} L_{ij}$. Damit gilt:

$H = \bigwedge_{i=1}^n \neg \left(\bigwedge_{j=1}^{m_i} L_{ij} \right)$

$= \bigwedge_{i=1}^n \bigvee_{j=1}^{m_i} \neg L_{ij}$

$= \bigwedge_{i=1}^n \bigvee_{j=1}^{m_i} \bar{L}_{ij}$ dabei ist $\bar{L}_{ij} = \begin{cases} \neg A & \text{falls } L_{ij} = A \\ A & \text{falls } L_{ij} = \neg A \end{cases}$

\Rightarrow Beseitigung von Doppelnegationen, welche keine Literale sind.

b. H besitzt die „DNF-Eigenschaft“.

Der Ausgangspunkt der dualen (analogen) Rechnung ist eine zu F äquivalente KNF.

$F = \bigwedge_{i=1}^{n'} F_i'$ für Disjunktionsterme F_i'

Dieser Beweis ist sogleich der **Nachweis der Korrektheit** des folgenden **Algorithmus zur Erzeugung einer äquivalenten KNF bzw. DNF**:

1. Algorithmus zur Erzeugung äquivalenter KNF und DNF

(in Globalschritten)

1. Schritt: **Ersetzen** aller Teilformeln $F \leftrightarrow G$ durch $(F \rightarrow G) \wedge (G \rightarrow F)$
 \Rightarrow danach besitzt der Term keine Bijunktionen
2. Schritt: **Ersetzen** aller Teilformeln $F \rightarrow G$ durch $\neg F \vee G$
 \Rightarrow danach besitzt der Term weder Bijunktionen noch Implikationen
3. Schritt: „**Nach-innen-ziehen**“ bzw. „**Nach-oben-ziehen**“ der Negationen gemäß der De Morganschen Formeln: $\neg(F \wedge G) = (\neg F \vee \neg G)$ sowie $\neg(F \vee G) = (\neg F \wedge \neg G)$ bei

gleichzeitiger Beseitigung von Doppelnegationen

⇒ danach stehen alle Negationen unmittelbar vor Atomen (im Baum in der 2. Schicht)

4. Schritt:

- a. Bestimmen der KNF; d.h. „**Disjunktionen nach innen ziehen**“ gemäß des Distributivgesetzes: $F \vee (G \wedge H) = (F \vee G) \wedge (F \vee H)$

Ergebnis: Konjunktive Normalform

- b. Bestimmen der DNF; d.h. „**Konjunktionen nach innen ziehen**“ gemäß des Distributivgesetzes: $F \wedge (G \vee H) = (F \wedge G) \vee (F \wedge H)$

Ergebnis: Disjunktive Normalform

5. Schritt: „**Kürzen**“

- a. bei KNF:

$$F = (A \vee B) \wedge \dots \wedge (\neg C \vee \dots \vee B \vee \dots \vee B) \wedge (D \vee A \vee \dots \vee \neg D \vee \dots)$$

⇒ Dopplung kann gestrichen werden:

$$F = \dots \wedge (\neg C \vee \dots \vee B \vee \dots \vee \neg B) \wedge \dots$$

⇒ Anwenden der Tautologieregel (Streichen des gesamten Terms!):

$$F = \dots \wedge (\neg C \vee \dots \vee B \vee \dots \vee \neg B), \text{ denn } (D \vee \neg D) \in \text{Taut}$$

- b. bei DNF:

$$F = (B \wedge D) \vee \dots \vee (\neg A \wedge B \wedge \dots \wedge \neg A) \vee (B \wedge \dots \wedge \neg B \wedge F)$$

⇒ Dopplung kann gestrichen werden:

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

⇒ Anwenden der Unerfüllbarkeitsregel (Streichen des gesamten Terms!):

$$F = \dots \vee (\neg A \wedge B \wedge \dots \wedge \neg A), \text{ denn } (B \wedge \neg B) \in \text{Sat}$$

2. Verfahren zur Erzeugung

(mit weniger Rechenaufwand!!)

Ausgangspunkt für die Erzeugung ist eine **Wahrheitstabelle (WWT)**

Gegeben sei eine Formel F mit den Atomen A_1, \dots, A_n : $F = (A_1, \dots, A_n)$.

Wir betrachten zugehörige WWT: f_F^n

	$\beta(A_1)$	$\beta(A_2)$	\dots	$\beta(A_n)$	$I_\beta(F) = f_F$
Zeile 0	0	0	\dots	0	y_0
	\vdots	\vdots		\vdots	
Zeile i	x_1	x_2	\dots	x_n	y_i
	\vdots	\vdots		\vdots	
Zeile 2^n-1	1	1	\dots	1	y_{2^n-1}

Dann gilt:

$$i = \sum_{j=1}^n x_j \cdot 2^{n-j}$$

insbesondere gilt: $0 = \sum_{j=1}^n 0 \cdot 2^{n-j}$ und $2^n - 1 = \sum_{j=1}^n 1 \cdot 2^{n-j}$

Stets ist $(x_1, x_2, \dots, x_n) \in \{0, 1\}^n$. Wir definieren zwei Teilmengen von $\{0, 1\}^n$.

$N_F = \{(x_1, x_2, \dots, x_n) \mid \text{für } \beta(A_1) = x_1, \dots, \beta(A_n) = x_n \text{ gilt } I_\beta(F) = 0\}$

$E_F = \{(x_1, x_2, \dots, x_n) \mid \text{für } \beta(A_1) = x_1, \dots, \beta(A_n) = x_n \text{ gilt } I_\beta(F) = 1\}$

Es gilt: $N_F \cup E_F = \{0,1\}^n$ und $N_F \cap E_F = \emptyset$

Wir definieren spezielle Terme:

$$I. \quad A_i^{x_i} = \begin{cases} A_i & \text{falls } x_i = 1 \\ \neg A_i & \text{falls } x_i = 0 \end{cases} \quad (\text{für } x_i \in \{0,1\})$$

Es gilt: $I_\beta(A_i^{x_i}) = 1$ gdw $\beta(A_i) = x_i$

Weiter sei $A_1^{x_1} \wedge A_2^{x_2} \wedge \dots \wedge A_n^{x_n}$ eine **Elementarkonjunktion**.

Dann gilt: $I_\beta(A_1^{x_1} \wedge A_2^{x_2} \wedge \dots \wedge A_n^{x_n}) = 1$ gdw $\beta(A_1) = x_1, \dots, \beta(A_n) = x_n$

D.h. eine Elementarkonjunktion ist für genau eine Belegung **erfüllt**.

$$II. \quad A_i^{\bar{x}_i} = \begin{cases} \neg A_i & \text{falls } x_i = 1 \\ A_i & \text{falls } x_i = 0 \end{cases} \quad (\text{für } x_i \in \{0,1\})$$

Es gilt: $I_\beta(A_i^{\bar{x}_i}) = 0$ gdw $\beta(A_i) = x_i$

weiter sei $A_1^{\bar{x}_1} \vee A_2^{\bar{x}_2} \vee \dots \vee A_n^{\bar{x}_n}$ eine **Elementardisjunktion**.

Dann gilt: $I_\beta(A_1^{\bar{x}_1} \vee A_2^{\bar{x}_2} \vee \dots \vee A_n^{\bar{x}_n}) = 0$ gdw $\beta(A_1) = x_1, \dots, \beta(A_n) = x_n$

D.h. eine Elementardisjunktion ist für genau einen Belegung **nicht erfüllt**.

Wir definieren:

$$1. \quad F_D := \bigvee_{(x_1, \dots, x_n) \in E_F} (A_1^{x_1} \wedge A_2^{x_2} \wedge \dots \wedge A_n^{x_n})$$

\Rightarrow Disjunktion von Konjunktionstermen \Rightarrow DNF
 \Rightarrow besondere DNF: Kanonische DNF – KDNF denn es gilt für alle Belegungen β :
 $I_\beta(F_D) = 1$ gdw $I_\beta(F) = 1$. D.h. $F_D \models F$

$$2. \quad F_K := \bigwedge_{(x_1, \dots, x_n) \in N_F} (A_1^{\bar{x}_1} \vee A_2^{\bar{x}_2} \vee \dots \vee A_n^{\bar{x}_n})$$

\Rightarrow Konjunktion von Disjunktionstermen \Rightarrow KNF
 \Rightarrow besondere KNF: Kanonische KNF – KKNF denn es gilt für alle Belegungen β :
 $I_\beta(F_K) = 0$ gdw $I_\beta(F) = 0$. D.h. $F_K \models F$

Fakt:

Jede n-stellige Boolesche Funktion $f_F^{(n)}$ gibt es eine Formel F_K in KKNF und KDNF.

So dass $f_{F_K} = f$ und $f_{F_D} = f$.

$$F_K := \bigwedge_{(x_1, \dots, x_n) \in N_F} (A_1^{\bar{x}_1} \vee A_2^{\bar{x}_2} \vee \dots \vee A_n^{\bar{x}_n})$$

$$F_D := \bigvee_{(x_1, \dots, x_n) \in E_F} (A_1^{x_1} \wedge A_2^{x_2} \wedge \dots \wedge A_n^{x_n})$$

Bemerkung: Jede n-stellige Boolesche Funktion $f^{(n)}$ ist durch eine **Codenummer** identifiziert.

	x_1	x_2	x_n	$f^{(n)}$
Zeile 0	0	0	0	y_0
	\vdots	\vdots		\vdots	
Zeile i	x_1	x_2	x_n	y_i
	\vdots	\vdots		\vdots	
Zeile 2^n-1	1	1	1	y_{2^n-1}

Für den Eintrag i in der Zeile i:
$$i = \sum_{j=1}^n x_j \cdot 2^{n-j} = x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \dots + x_{n-1} \cdot 2^1 + x_n \cdot 2^0$$

Binärdarstellung von i

f ist bestimmt durch eine Eintragung $y_0, y_1, \dots, y_{2^n-1}$. Sie liefert die folgende **Codenummer**:

$$\text{Code}(f^{(n)}) = \sum_{k=0}^{2^n-1} y_k \cdot 2^k$$

HORN-Formeln (A. Horn)

Definition

Eine aussagenlogische Formel F ist eine **Horn-Formel** \leftrightarrow_{df}

1. F ist KNF
2. jede Klausel von F enthält *höchstens* ein positives Literal.

Beispiele:

1. $(A \vee \neg B \vee \neg C) \wedge (C \vee \neg D) \wedge (\neg A \vee \neg B) \wedge \neg C \wedge D$
2. $(\neg A \vee B \vee \neg D) \wedge (A \vee \neg D) \wedge \neg C \wedge D$
3. $A \vee B$ (\Rightarrow in KNF, eine Klausel; auch in DNF **aber keine** Horn-Formel, da 2 pos. Lit.)

Frage: Gibt es zu jeder Formel F eine äquivalente Horn-Formel F_H ?

Antwort: Nein, z.B. o.g. Beispiel 3, d.h. Horn-Formeln sind keine Normalformeln.

Bedeutung der Horn-Formeln für die Informatik

1. prozedurale Bedeutung (in Form von Prolog-Anweisungen)
2. **effiziente (!)** Erfüllbarkeitstests

zu 1)

Jede Horn-Formel (HF) lässt sich umformen als Konjunktion von Implikationen.

1. $(A \vee \neg B \vee \neg C) = A \vee \neg(B \wedge C) = (B \wedge C) \rightarrow A$
2. $(C \vee \neg D) = \neg D \vee C = D \rightarrow C$

3. $\neg A \vee \neg B = \neg(A \wedge B) = \neg(A \wedge B) \vee 0 = (A \wedge B) \rightarrow 0$
Dabei ist „0“ ein Symbol für eine unerfüllbare Formel, z.B. $0 := A \wedge \neg A$.
4. $\neg C = \neg C \vee 0 = C \rightarrow 0$
5. $D = 0 \vee D = \neg 0 \vee D = 1 \vee D = 1 \rightarrow D$
Dabei ist „1“ ein Symbol für eine gültige Formel, z.B. $1 := A \vee \neg A$.

für Beispiel 1 gilt:

$$(A \vee \neg B \vee \neg C) \wedge (C \vee \neg D) \wedge (\neg A \vee \neg B) \wedge \neg C \wedge D \models \\ (B \wedge C \rightarrow A) \wedge (D \rightarrow C) \wedge (A \wedge B \rightarrow 0) \wedge (C \rightarrow 0) \wedge (1 \rightarrow D)$$

für Beispiel 2 gilt:

$$(\neg A \vee B \vee \neg D) \wedge (A \vee \neg D) \wedge \neg C \wedge D \models \\ (A \wedge D \rightarrow B) \wedge (D \rightarrow A) \wedge (C \rightarrow 0) \wedge (1 \rightarrow D)$$

zu 2)

Behauptung: Algorithmus
Eingabe: HORN-Formel (als Konjunktion von Implikationen)

1. Schritt:

Markiere alle Vorkommen von Atomen A, für die es Implikationen der Gestalt $(1 \rightarrow A)$ gibt.

2. Schritt:

while in F gibt es Teilformeln der Gestalt

- i. $A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow B$ oder
- ii. $A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow 0$

wobei alle Atome A_1, \dots, A_n markiert sind

do if Fall (i) *then* Markiere alle Vorkommen von B

else Ausgabe: „unerfüllbar“

3. Schritt:

Ausgabe: „erfüllbar“

Satz:

1. Markierungsalgorithmus ist für alle Horn-Formeln als Eingabe korrekt.
2. Falls die Ausgabe „erfüllbar“ erscheint, dann liefert die Belegung $\beta(A) = 1$ für alle markierten Atome A ein Modell für F.
3. Für eine Horn-Formel mit n Atomen stoppt der Algorithmus nach höchstens n Durchläufen!
⇒ Damit hat dieser Algorithmus **linearen Aufwand**.

Beweis:

zu 3) In jedem Durchlauf wird ein Atom markiert, also ist nach höchstens n Durchläufen nichts mehr zu markieren ⇒ Algorithmus ist beendet.

zu 2) Beweis durch Beweisen des folgenden **Lemmas**:

Für alle Belegungen β gilt: falls β ein Modell für F ist, dann gilt für alle Atome A, in F: falls A markiert ist, dann ist $\beta(A) = 1$.

Beweis des Lemmas (induktiv):

- a) Die Behauptung gilt für alle Atome A , die in Klauseln der Gestalt $(1 \rightarrow A)$ vorkommen.
Da ein Modell für F , Modell jeder Klausel ist, gilt:
 β ist Modell für F gdw
 β ist Modell für alle Klauseln gdw
 β ist Modell für alle $(1 \rightarrow A)$ gdw
 $\beta(A) = 1$ für alle diese A .
- b) Die Behauptung gilt für alle Atome B , die im 2. Schritt markiert werden.
Denn es gilt: falls $(A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow B)$ eine Teilformel von F ist und alle Atome A_1, A_2, \dots, A_n markiert sind, bedeutet dies für alle Modelle β von F :
 $\beta(A_1) = \beta(A_2) = \dots = \beta(A_n) = 1$ und es gilt $I_\beta(A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow B) = 1$ gdw $\beta(B) = 1$.

zu 1)

- a) Die Aussage unerfüllbar ist korrekt. (Widerspruchsbeweis – indirekt)
Annahme: Antwort ist „falsch“! D.h. F besitzt ein Modell, β sei ein Modell für F .

Die Aussage unerfüllbar passiert im 2. Schritt für eine Teilformel der Gestalt

$A_1 \wedge \dots \wedge A_n \rightarrow 0$ (Fall ii.), wobei alle A_1, \dots, A_n markiert sind.

Nach bewiesenem Lemma gilt: $\beta(A_1) = \beta(A_2) = \dots = \beta(A_n) = 1$

Hieraus folgt $I_\beta(A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow 0) = 0$, da $\beta(0) = 0$ für alle Belegungen β .

Also ist β doch kein Modell für F . **Widerspruch!!!**

- b) Die Aussage „erfüllbar“ ist ebenfalls korrekt.
Es sei G eine beliebige Klausel von F .

1. Fall: $G = (1 \rightarrow A) \equiv A$. Dann ist $\beta(A) = 1$ ein Modell für G .

2. Fall:

$G = (A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow B)$ und alle Atome A_1, A_2, \dots, A_n sind markiert, dann ist $\beta(A_1) = \beta(A_2) = \dots = \beta(A_n) = 1 = \beta(B)$ ein Modell für G .

3. Fall:

$G = (A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow B)$ und **nicht** alle Atome A_1, A_2, \dots, A_n sind markiert.
O.B.d.A. sei A_1 nicht markiert, dann ist $\beta(A_1) = 0$ ein Modell für G .

4. Fall:

$G = (A_1 \wedge A_2 \wedge \dots \wedge A_n \rightarrow 0)$ und die Aussage „unerfüllbar“ ist nicht erfolgt. Also sind nicht alle Atome A_1, A_2, \dots, A_n markiert.

O.B.d.A. sei A_1 nicht markiert. Dann ist $\beta(A_1) = 0$ ein Modell für G .

§5. Die Folgerungsrelation und der Endlichkeitssatz

Wissen:

- $F \models G \leftrightarrow$ jedes Modell von F ist auch Modell von G
 \leftrightarrow für alle β gilt: wenn $I_\beta(F) = 1$, dann $I_\beta(G) = 1$
 \leftrightarrow für alle β gilt: $I_\beta(F) \leq I_\beta(G)$
 $\leftrightarrow f_F \leq f_G$
 $\leftrightarrow (F \rightarrow G) \in \text{Taut}$

Eigenschaften der Folgerungsrelation

Definition

Es sei X eine Menge von Formeln aus \mathcal{L}_{AL} . Eine Belegung $\beta: \mathcal{A} \mapsto B$ ist Modell von $X \leftrightarrow_{df}$ für alle $F \in X$ gilt: β ist Modell von F (d.h. für alle $F \in X$ gilt, $I_\beta(F) = 1$).

X ist erfüllbar \leftrightarrow_{df} X besitzt ein Modell.

X ist gültig \leftrightarrow_{df} jede Belegung β ist Modell von X

Bemerkung:

1. Es gilt **nicht**: X ist erfüllbar gdw alle Formeln F aus X sind erfüllbar!

Beispiel:

$$X = \{A, \neg A\}$$

$\Rightarrow A$ ist erfüllbar, $A \in \text{Sat}$

$\Rightarrow \neg A$ ist erfüllbar, $\neg A \in \text{Sat}$

aber: es gibt kein Modell für X , denn $\beta(A) = 1$ gdw $\beta(\neg A) = 0$

2. Es gilt: X ist gültig, wenn alle Formeln $F \in X$ gültig sind.

Definition

Es seien X und Y Formelmengen und F eine Formel.

1. $X \models F$, d.h. F ist eine **Folgerung aus der Menge** X gdw \leftrightarrow_{df} jedes Modell von X ist Modell von F .
2. $X \models Y$, d.h. Y ist eine **Folgerungsmenge** von $X \leftrightarrow_{df}$ jedes Modell von X ist Modell von Y .

Satz 1: (Satz über die Formalisierung mathematischer Beweisprinzipien)

- | | |
|---|--|
| 1. $\{F \rightarrow G, G \rightarrow F\} \models F \leftrightarrow G$ | <i>Schema für Äquivalenzbeweis</i> |
| 2. $\{\neg G \rightarrow \neg F\} \models F \rightarrow G$ | <i>Kontrapositionsbeweis</i> |
| 3. $\{F \rightarrow G, G \rightarrow H\} \models F \rightarrow H$ | <i>Kettenschluss</i> |
| 4. $\{F \rightarrow G, \neg F \rightarrow G\} \models G$ | <i>Beweis durch Fallunterscheidung (2 Fälle)</i> |
| 5. $\{F \rightarrow G, F \rightarrow \neg G\} \models \neg F$ | <i>indirekter Beweis</i> |
| 6. $\{F \rightarrow G, F\} \models G$ | <i>Modus ponens</i> |
| 7. $\{F \rightarrow G, \neg G\} \models \neg F$ | <i>Modus tollens</i> |

- | | |
|--|---|
| 8. $\{F\} \models F \vee G$ | <i>Abschwächung der Disjunktion</i> |
| 9. $\{F \wedge G\} \models F$ | <i>Abschwächung der Konjunktion</i> |
| 10. $\{F \rightarrow G \vee H\} \models F \wedge \neg G \rightarrow H$ | <i>Konklusion-Prämissen-Tausch/Verlagerung</i> |
| 11. $\{F \rightarrow (G \rightarrow H)\} \models F \wedge G \rightarrow H$ | <i>Prämissen-Verlagerung</i> |
| 12. $\models F \vee \neg F$ | <i>Tertium non datur</i> |
| | \Rightarrow Satz vom ausgeschlossenen Dritten |

Beweis von Satz 1:

- 1) Grundsätzliche Methode besteht im Nachweis: jedes Modell von X ist Modell von F; mit Hilfe der WWT:

z.B.: $X = \{F \rightarrow G, G \rightarrow F\} \models F \leftrightarrow G$

$I_\beta(F)$	$I_\beta(G)$	$I_\beta(F \rightarrow G)$	$I_\beta(G \rightarrow F)$	$I_\beta(F \leftrightarrow G)$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

alle Modelle von X sind
Modell von $F \leftrightarrow G$

- 2) Andere Methode besteht in der Auswertung „kritischer Belegungen“:

z.B.: $\{\neg G \rightarrow \neg F\} \models F \rightarrow G$

„Kritisch“ sind Belegungen mit $I_\beta(F \rightarrow G) = 0$. Wir wissen $I_\beta(F \rightarrow G) = 0$

gdw $I_\beta(F) = 1$ und $I_\beta(G) = 0$ ist,

gdw $I_\beta(\neg F) = 0$ und $I_\beta(\neg G) = 1$,

gdw $I_\beta(\neg G \rightarrow \neg F) = 0$,

gdw β ist kein Modell von $\neg G \rightarrow \neg F$.

D.h. die kritischen Belegungen der rechten Seite sind keine Modelle der linken Seite.

Bemerkung:

Einige Relationen lassen sich umkehren.

z.B.: $F \leftrightarrow G \models \{F \rightarrow G, G \rightarrow F\}$

$F \rightarrow G \models \neg G \rightarrow \neg F$

(Die Gültigkeit beider Richtungen bedeutet gerade die semantische Äquivalenz!)

- 3) „Tertium non datur“

Fakt:

Wenn $Y \subseteq X$, dann gilt $\text{Mod}(X) \subseteq \text{Mod}(Y)$. Dabei bezeichnet $\text{Mod}(X)$ die Menge aller Modelle von X. Da $\emptyset \subseteq X$, gilt: $\text{Mod}(X) \subseteq \text{Mod}(\emptyset)$

Vereinbarung: Jede Belegung β ist Modell der leeren Menge \emptyset .

Dann gilt: $\emptyset \models F$ gdw jedes Modell von X ist Modell von F

gdw jede Belegung β ist Modell von F

gdw $F \in \text{Taut}$

$\emptyset \models F$ gdw $F \in \text{Taut}$

„F gilt ohne jegliche Vorbedingung.“

„F ist bedingungslos wahr.“

Damit gilt:

$F \models G$ gdw $\emptyset \models (F \rightarrow G)$ gdw $(F \rightarrow G) \in \text{Taut}$

Weitere Eigenschaften der Folgerungsrelation

Satz 2:

- | | | |
|--|---|-----------------------------|
| 1. Wenn $X \subseteq Y$, dann $Y \models X$
insbesondere gilt: $X \models X$ | } | Reflexivität |
| 2. Wenn $X \models Y$ und $Y \models Z$, dann $X \models Z$ | | |
| 3. Wenn $X \subseteq Z$ und $X \models Z$, dann $Y \models Z$ | } | Monotonieeigenschaft |

Satz 3: (Beziehung der Folgerungsrelation zu anderen semantischen Grundbegriffen)

- Folgerung & Tautologie:**
Es sei $F \in \text{Taut}$, dann gilt: $X \cup \{F\} \models G$ gdw $X \models G$
insbesondere gilt: $\emptyset \models G$ gdw $F \models G$ gdw $G \in \text{Taut}$
- Folgerung & Erfüllbarkeit:**
 $X \models F$ gdw $X \cup \{\neg F\}$ unerfüllbar
insbesondere gilt: $\emptyset \models F$ gdw $F \in \text{Taut}$ gdw $\neg F \in \overline{\text{Sat}}$
- Folgerung & Implikation:**
 $X \models (F \rightarrow G)$, dann $X \cup \{F\} \models G$
insbesondere gilt: $\emptyset \models (F \rightarrow G)$ gdw $(F \rightarrow G) \in \text{Taut}$ gdw $F \models G$
- Folgerung & Konjunktion:**
 $\{F_1, F_2, \dots, F_n\} \models G$ gdw $(F_1 \wedge F_2 \wedge \dots \wedge F_n) \models G$;
 $X \models \{G_1, G_2, \dots, G_m\}$ gdw $X \models (G_1 \wedge G_2 \wedge \dots \wedge G_m)$
 $\{F_1, F_2, \dots, F_n\} \models Y$ gdw $(F_1 \wedge F_2 \wedge \dots \wedge F_n) \models Y$;

Beweis von Aussage 1:

Voraussetzung: $F \in \text{Taut}$

„ \rightarrow “ Es sei $X \cup \{F\} \models G$ gegeben:

\Rightarrow Jedes Modell $X \cup \{F\}$ ist ein Modell für G .

\Rightarrow Für alle β gilt; wenn β ein Modell von X ist und $I_\beta(F) = 1$ ist, dann ist β ein Modell für G .

\Rightarrow Für alle β gilt: wenn β Modell von X ist, dann ist β ein Modell für G .

\Rightarrow D.h. $X \models G$

„ \leftarrow “ Es sei $X \models G$. Dann gilt erst recht: $X \cup \{F\} \models G$ (Monotonie)

Beweis von Aussage 2:

Voraussetzung ist: $X \models F$

„ \rightarrow “ Behauptung: $X \cup \{\neg F\}$ ist unerfüllbar.

Annahme: $X \cup \{\neg F\}$ ist erfüllbar.

Dann gibt es eine Belegung b die Modell von $X \cup \{\neg F\}$ ist. D.h. für dieses β gilt, β ist Modell von X und β ist Modell von $\neg F$ ($I_\beta(\neg F) = 1$). Andererseits gilt, dass $X \models F$: d.h. β ist Modell von F . D.h. $I_\beta(F) = 1$ und damit gilt $I_\beta(\neg F) = 0$. **Widerspruch!!!**

Also ist $X \cup \{\neg F\}$ unerfüllbar!

Folgerung und Widersprüchlichkeit

indirekter Beweis:

allgemeine Situation: Wollen eine Aussage F beweisen.

Annahme: $\neg F$

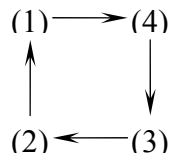
$$\models (\neg F \rightarrow G)$$
$$\models (\neg F \rightarrow \neg G)$$
$$\mathbb{F}$$

Eine Formelmenge X ist **widersprüchlich** \leftrightarrow_{df} es gibt eine Formel F , so dass einerseits $X \models F$ und andererseits $X \models \neg F$.

X ist widersprüchlich, falls es eine Formel F gibt mit $F \in X$ und $\neg F \in X$.

Die folgenden Aussagen sind äquivalent:

- Beweis von Satz 4:** in Form eines „Ringbeweises“:



- Also gilt erst recht: $X \models 1$ und es gilt $1 \models \neg 0$

Folgerung 1:

Die folgenden Aussagen sind äquivalent:

1. X ist widersprüchlich.
2. $X \models 0$
3. Es gibt eine Formel G , die nicht aus X folgt.
4. X ist erfüllbar.

Hinweis:

Versuchen sie diese Folgerung in Form eines Ringbeweises zu beweisen.

Folgerung 2:

$X \models F$ gdw $X \cup \{\neg F\}$ widersprüchlich.

Hinweis:

Satz 3 (2): $X \models F$ gdw $X \cup \{\neg F\}$ unerfüllbar.

Beweis:

Voraussetzung: $X \cup \{\neg F\}$ ist unerfüllbar.

Behauptung: $X \models F$

indirekter Beweis: es sei β ein Modell von X . Dann ist β kein Modell von $\neg F$, da $X \cup \{\neg F\}$ kein Modell hat.

D.h. aber $I_\beta(\neg F) = 0$,

d.h. $I_\beta(F) = 1$,

d.h. β ist Modell von F .

Folgerung und formale Theorien

Definition

Es sei X eine (beliebige, unendliche) Formelmenge.

Dann heißt $Fl(X) := \{G \in \mathcal{L}_{AL} \mid X \models G\}$ **Folgerungshülle** von X .

Damit ist $Fl: \{X \mid X \subseteq \mathcal{L}_{AL}\} \mapsto \{Y \mid Y \subseteq \mathcal{L}_{AL}\}$, d.h. $Fl: \mathfrak{R}(\mathcal{L}_{AL}) \mapsto \mathfrak{R}(\mathcal{L}_{AL})$

Also ist Fl eine Abbildung, ein sog. **Operator**.

Eigenschaften dieser Abbildung:

1. $X \subseteq Fl(X)$, da $X \models X$ (Satz 2 (1)) und per Definition: $X \models Fl(X) \Rightarrow$ **Reflexivität**
2. Wenn $X \subseteq Y$, dann $Fl(X) \subseteq Fl(Y)$ (Satz 2 (3)) \Rightarrow **Monotonie**
3. $Fl(Fl(X)) = Fl(X)$ wegen Satz 2 (2) \Rightarrow **Transitivität**

Diese drei Eigenschaften charakterisieren Fl als Hüllenoperator.

Beweis:

Klar ist: $Fl(X) \subseteq Fl(Fl(X))$ wegen (1). Es bleibt z.Z.: $Fl(Fl(X)) \subseteq Fl(X)$.

Es sei $G \in Fl(Fl(X))$. D.h. Es gilt: $Fl(X) \models G$. Natürlich gilt: $X \models Fl(X)$.

Also gilt $X \models G$, aufgrund der Transitivität, d.h. $G \in Fl(X)$

Dabei gilt folgende allgemeine Definition:

Definition

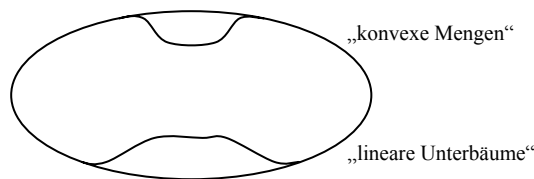
Eine Abbildung $\Gamma: \mathfrak{R}(M) \mapsto \mathfrak{R}(M)$ heißt **Hüllenoperator** über der Menge $M \leftrightarrow_{\text{df}}$

1. für alle $X \subseteq M$: $X \subseteq \Gamma(X)$ \Rightarrow Einbettung
2. für alle $X, Y \subseteq M$: $X \subseteq Y \Rightarrow \Gamma(X) \subseteq \Gamma(Y)$ \Rightarrow Monotonie
3. für alle $X \subseteq M$: $\Gamma(\Gamma(X)) = \Gamma(X)$ \Rightarrow Abgeschlossenheit

Beispiele für Hüllenoperatoren:

aus der Geometrie: konvexe Hülle

aus der Linearen Algebra: lineare Hülle



Definitionen

Eine Menge X heißt **abgeschlossen** beziehungsweise $\text{Fl} \leftrightarrow_{\text{df}} \text{Fl}(X) = X$.

Eine Menge von Formeln T heißt **formale Theorie** $\leftrightarrow_{\text{df}} \text{Fl}(T) = T$.

Damit ist jede formale Theorie deduktiv abgeschlossen.

Mit einer Menge von Grundannahmen gehören auch alle Folgerungen aus diesen Annahmen zur Theorie. Die Grundannahmen heißen üblicherweise **Axiome**.

Dann gilt: $T = \text{Fl}(Ax)$ und $\text{Fl}(\text{Fl}(Ax)) = \text{Fl}(T) = T$.

Die Folgerungen aus den Axiomen heißen üblicherweise **Sätze der Theorie**.

Eine formale Theorie heißt **axiomisierbar** $\leftrightarrow_{\text{df}}$ es gibt eine (endliche) Menge Ax von Axiomen, so dass $T = \text{Fl}(Ax)$

Stand bisher:

„ $X \models F$ “ formalisiert folgenden Zusammenhang:

Aus einer Menge X (Voraussetzungen) lässt sich eine Behauptung F schlussfolgern.

Das Symbol \models steht für „beweisen“; es steht **nicht** für „Beweis“.

Betrachtung: Jeder Beweis ist endlich.

D.h. für das Folgern von F aus X benötigt man endlich viele Schritte.

Beispiel:

$X = \{A_1, A_1 \rightarrow A_2, A_2 \rightarrow A_3, \dots\}$ (X ist unendlich.)

Frage: Lässt sich z.B. A_{17} aus X beweisen?

Antwort: Ja, denn:

1. Schritt: $\{A_1, A_1 \rightarrow A_2\} \models A_2$

2. Schritt: $\{A_2, A_2 \rightarrow A_3\} \models A_3$

⋮

16. Schritt: $\{A_{16}, A_{16} \rightarrow A_{17}\} \models A_{17}$

\Rightarrow Tatsächlich folgt A_{17} bereits aus einer endlichen Teilmenge von X :

$X_{\text{fin}} = \{A_1, A_1 \rightarrow A_2, A_2 \rightarrow A_3, \dots, A_{16} \rightarrow A_{17}\}$

Der Endlichkeitssatz**Satz 5, A:**

Es sei X eine (beliebige, unendliche) Formelmeng und es sei F eine Formel.

$X \models F$ (A₁) gdw es gibt eine endliche Teilmenge $X_{\text{fin}} \subseteq X$, so dass $X_{\text{fin}} \models F$ (A₂).

Satz 5, B:

Es sei X eine (beliebige, unendliche) Formelmeng und es sei F eine Formel.

X ist unerfüllbar (B₁) gdw es gibt eine endliche Teilmenge $X_{\text{fin}} \subseteq X$, so dass X_{fin} unerfüllbar ist (B₂).

Satz 5, C:

Es sei X eine (beliebige, unendliche) Formelmeng und es sei F eine Formel.

Alle endlichen Teilmengen $X_{\text{fin}} \subseteq X$ sind erfüllbar (C₁) gdw X ist erfüllbar (C₂).

Wir erklären die logische Beziehung zwischen den Sätzen A, B und C:

Satz A: $A_1 \leftrightarrow A_2$ trivial ist: $A_2 \rightarrow A_1$

Satz B: $B_1 \leftrightarrow B_2$ trivial ist: $B_2 \rightarrow B_1$

Satz C: $C_1 \leftrightarrow C_2$ trivial ist: $C_2 \rightarrow C_1$

Weiter gilt: $C_2 \models \neg B_1$ und $C_1 \models \neg B_2$

Damit gewinnt Satz C die Gestalt: $\neg B_2 \rightarrow \neg B_1$ gdw $B_1 \leftrightarrow B_2$.

Es bleibt also **z.Z.:** $A_1 \rightarrow A_2$ und $B_1 \rightarrow B_2$

Wir zeigen: aus Satz A folgt Satz B: $\{A_1 \rightarrow A_2\} \models \{B_1 \rightarrow B_2\}$

Voraussetzung: X ist unerfüllbar (B₁), d.h. $X \models 0$ (Satz 4).

Wegen $(A_1 \rightarrow A_2)$ gilt: Es gibt eine endliche Teilmenge X_{fin} von X , so dass $X_{\text{fin}} \models 0$, d.h. X_{fin} ist unerfüllbar (Satz 4). Also erhalten wir: $B_1 \rightarrow B_2$

Wir zeigen: aus Satz B folgt Satz A: $\{B_1 \rightarrow B_2\} \models \{A_1 \rightarrow A_2\}$

Voraussetzung: $X \models F$ (A₁)

Dann gilt $X \cup \{\neg F\}$ ist unerfüllbar (Folgerung 2, Satz 4). Wegen $(B_1 \rightarrow B_2)$ gilt: es gibt eine endliche Teilmenge $X_{\text{fin}} \subseteq X \cup \{\neg F\}$ die unerfüllbar ist.

Wir betrachten: $X_{\text{fin}} := X'_{\text{fin}} \setminus \{\neg F\}$

1. Fall:

X_{fin} ist (bereits ohne $\neg F$) unerfüllbar. Dann gilt: aus X_{fin} folgt jede Formel (Satz 4).

Also auch $X_{\text{fin}} \models F$

2. Fall:

X_{fin} ist erfüllbar. D.h. es gibt ein Modell β von X_{fin} . Mit Sicherheit ist β kein Modell von

$\neg F$ (sonst wäre β ein Modell von $X_{\text{fin}} \cup \{\neg F\}$, also ein Modell von X'_{fin}).

Also gilt: $I_\beta(\neg F) = 0$, d.h. $I_\beta(F) = 1$.

Dies bedeutet: jedes Modell von X_{fin} ist Modell von F ; also $X_{\text{fin}} \models F$.

Also erhalten wir $A_1 \rightarrow A_2$.

Fazit: Alle drei Sätze sind äquivalent.

Es bleibt z.Z.: $(A_1 \rightarrow A_2)$ oder $(B_1 \rightarrow B_2)$ oder $(C_1 \rightarrow C_2)$.

Wir zeigen: $(C_1 \rightarrow C_2) \Rightarrow$ Beweis aus Satz C

Voraussetzung: Jede endliche Teilmenge $X_{\text{fin}} \subseteq X$ besitzt ein Modell.

Behauptung: X besitzt ein Modell.

Schwierigkeit: Konstruktion eines Modells von X aus der Vielzahl der (inkonsistenten)

Modelle für die endliche Teilmenge X_{fin} .

Deshalb: Wir „ordnen“ die Menge X :

Für unendlich viele Formeln hat man unendlich viele Atome:

$\{A_1, A_2, \dots, A_n\} = \mathcal{A}$

Wir definieren Teilmengen X_n von X :

$X_n = \{F \in X \mid \text{In } F \text{ kommen höchstens die Atome } A_1, A_2, \dots, A_n \text{ vor}\}$

Dann gilt: $X_1 \subseteq X_2 \subseteq X_3 \subseteq \dots$ mit: $\bigcup_{n=1}^{\infty} X_n = X$

Diese Teilmenge X_n können alle (noch) unendlich sein:

z.B. $X_1 = \{A_1, (A_1 \vee A_1, \dots)\}$ $Y_1 = \{A_1\}$

\Rightarrow maximal: $A_1, \neg A_1, A_1 \wedge A_1, A_1 \vee A_1$ } hier einstellige boolesche Funktion

Aber:

In jeder Menge X_n gibt es höchstens endlich viele Formeln, die Paarweise nicht äquivalent sind.

Begründung:

Es kann nur so viele Paare nichtäquivalenter Formeln geben, wie es Paare verschiedener boolescher Funktionen mit höchstens n Stellen gibt.

★ $\left\{ \begin{array}{l} Y_n \text{ sei eine Teilmenge von } X_n \text{ mit maximaler Zahl von Paaren nicht äquivalenter} \\ \text{Formeln. D.h. jedes Modell von } Y_n \text{ ist auch Modell von } X_n. \text{ (Begründung: Es sei } H \\ \text{irgendeine Formel aus } X_n, \text{ die nicht in } Y_n \text{ vorkommt. Das } H \text{ ist nicht in } Y_n, \text{ weil es} \\ \text{dort Formeln } G \text{ gibt mit } G \models H. \text{) Wenn } \beta \text{ ein Modell von } Y_n \text{ ist, ist } \beta \text{ Modell von } G \\ \text{und damit von } H. Y_n \text{ ist endlich für jedes } n \geq 1. \end{array} \right.$

Nach Voraussetzung ist jedes Y_n erfüllbar. Dann ist für jedes $n \geq 1$: β_n Modell von X_n wegen ★

Damit ist $(\beta_n)_{n=1}^{\infty}$ eine Familie von Modellen für $(X_n)_{n=1}^{\infty}$.

Wobei gilt: für $n \geq k$ ist β_n Modell für X_k .

★★ { D.h. β_n ist Modell $X_n, X_{n-1}, \dots, X_2, X_1$.

Wir brauchen ein Modell für X .

Wir konstruieren aus der Folge $(\beta_n)_{n=1}^\infty$ eine Abbildung β in Stufen (induktiv):

0. Stufe: (Initialisierung des Prozesses)

$\beta := \emptyset$

unendliche Indexmenge: $I := \{1, 2, 3, \dots\} = \{n \mid n \in \mathbb{N}\}$

(n+1). Stufe: \langle Fixieren den Wert von β für das Atom $A_{n+1}\rangle$

if $\beta_i(A_{n+1}) = 1$ für unendlich viele Indizes;

then $\beta := \beta \cup \{(A_{n+1}, 1)\}$ (d.h. $\beta(A_{n+1}) = 1$)

und $I := I \setminus \{i \mid \beta_i(A_{n+1}) = 0\}$

sonst $\beta := \beta \cup \{(A_{n+1}, 0)\}$ (d.h. $\beta(A_{n+1}) = 0$)

und $I := I \setminus \{i \mid \beta_i(A_{n+1}) = 1\}$

Dann gilt:

1. β ist eine Abbildung von \mathcal{A} nach $B = \{0, 1\}$. β ist also eine Belegung.

2. Nach jeder Stufe bleibt die Indexmenge I stets unendlich.

Begründung (induktiv):

I sei unendlich vor der $(n+1)$. Stufe.

a. Es bleiben unendlich viele $\beta_i(A_{n+1}) = 1$ aus I .

b. Es bleiben aus den I unendlich viele $\beta_i(A_{n+1}) = 0$ übrig.

3. β ist ein Modell von X , d.h. β ist Modell für **alle** F aus X .

Es sei F eine Formel $F \in X$, $X = \bigcup_{n=1}^\infty X_n$. Es sei n_0 der kleinste Index, so dass $F \in X_{n_0}$.

Dann gilt nach der Stufe n_0 folgendes:

Es gibt keinen Index j_{n_0} mit der die Eigenschaft $\beta_{j_{n_0}}(A_{n_0}) \neq \beta(A_{n_0})$.

Aber es gibt auch keinen Index j_{n_0-1} mit $\beta_{j_{n_0-1}}(A_{n_0-1}) \neq \beta(A_{n_0-1})$

(Also wegen $\star\star$)

\vdots

Es gibt keinen Index j_1 mit $\beta_{j_1}(A_1) \neq \beta(A_1)$.

D.h. aber es gilt für alle Indizes:

$$\beta_i(A_{n_0}) \neq \beta(A_{n_0})$$

\vdots

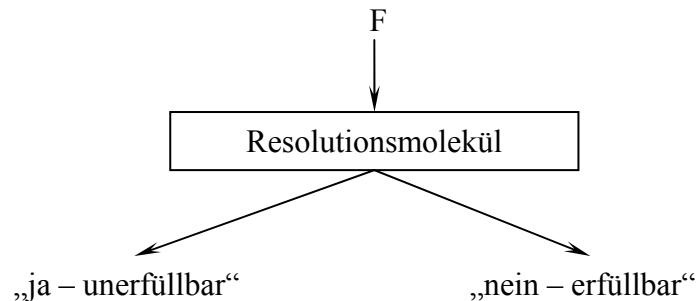
$$\beta_i(A_1) \neq \beta(A_1)$$

$\Rightarrow \beta_{n_0}$ ist Modell von F und damit ist β Modell von F .

§6. Die aussagenlogische Resolution

Ziel: Algorithmus zum Test auf **Unerfüllbarkeit** einer aussagenlogischen Formel F.

Eingabe:



Ausgabe:

Bemerkung:

1. **Frage:** $X \models F$?

Umformulierungen:

- Endlichkeitssatz: Es gibt eine endliche Teilmenge $X_{\text{fin}} = \{F_1, \dots, F_k\}$, so dass $\{F_1, \dots, F_k\} \models F$
- gdw $\{F_1, \dots, F_k\} \cup \{\neg F\}$ unerfüllbar
- gdw $\{F_1 \wedge \dots \wedge F_k \wedge \neg F\}$ ist unerfüllbar

2. **Frage:** $F \in \text{Taut}$ gdw $\neg F \in \overline{\text{Sat}}$?

Allgemein: Jedes Kalkül hat die Gestalt $K = \{\text{Ob}, \text{Reg}\}$ wobei gilt:

Ob ist eine Menge von Objekten die zu testen sind. (hier: ist Ob eine Menge der aussagenlogischen Formeln \mathcal{L}_{AL} .)

Reg ist eine Menge von Regeln, die auf die Objekte angewendet werden. (hier: eine einzige Regel zur Formelmanipulation, d.h. eine syntaktische Regel – frei von Semantik)

Jedes **Kalkül** ist im Bezug auf einen konkreten Test formuliert! (hier: Test auf Unerfüllbarkeit)

Dazu müssen zwei Eigenschaften erfüllt werden:

- Korrektheit** des Kalküls: d.h. die Antwort „ja“ ist nicht falsch. hier: Keine erfüllbare Formel bekommt die Antwort „ja – unerfüllbar“.
- Vollständigkeit** des Kalküls: hier: **Jede** unerfüllbare Formel bekommt die Antwort „ja – unerfüllbar“.

Eingabe: eine beliebige aussagenlogische Formel

Frage: In welcher Form ist die Eingabe gegeben?

Wissen:

In jeder Formel F gibt es eine äquivalente KNF, d.h.

$$\begin{aligned}
 F &= \left(\bigwedge_{i=1}^n \left(\bigvee_{j=1}^m L_{ij} \right) \right) \\
 &= (L_{11} \vee \dots \vee L_{1n_1}) \wedge (L_{21} \vee \dots \vee L_{2n_2}) \wedge \dots \wedge (L_{n1} \vee \dots \vee L_{nm_n})
 \end{aligned}$$

Wir schreiben:

$$= \{ \{ L_{11}, \dots, L_{1n_1} \}, \{ L_{21}, \dots, L_{2n_2} \}, \dots, \{ L_{n1}, \dots, L_{nm_n} \} \}$$

Wir schreiben die Konjunktion von Disjunktionen von Literalen als **Menge von Mengen von Literalen**, d.h. als **Klauselmenge**.

Beispiele:

$$F_1 = A_1 \wedge (A_2 \vee \neg A_3) \wedge (A_2 \vee A_2 \vee \neg A_3)$$

$$F_2 = A_1 \wedge (A_2 \vee \neg A_3)$$

$$F_3 = (A_1 \vee A_1) \wedge (A_2 \vee \neg A_3 \vee \neg A_3)$$

$$\text{alle liefern: } F = \{\{A_1\}, \{A_2, \neg A_3\}\}$$

Die Darstellung als Klauselmenge erlaubt eine, im Bezug auf Idempotenz, kürzeste Darstellung.

Die Zuordnung: Formeln \mapsto Klauselmenge ist nicht eineindeutig, aber es gilt:
Falls F_1 und F_2 dieselbe Klauselmenge liefern, dann gilt $F_1 \models F_2$,
insbesondere $F_1 \in \text{Sat}$ gdw $F_2 \in \overline{\text{Sat}}$.

Fazit:

Im Bezug auf den Test gehen bei der Darstellung einer Formel als Klauselmenge keine Informationen verloren.

Eingabe: Klauselmenge F

Definition

Gegeben sei eine Klauselmenge F .

Eine Klausel R heißt **Resolvent** zweier Klauseln K_1 und K_2 von $F \leftrightarrow_{\text{df}}$ es gibt ein Literal L , so dass $L \in K_1$ und $\bar{L} \in K_2$ und es gilt:

$$R = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\bar{L}\}) \text{ mit } \bar{L} \begin{cases} A & \text{falls } L = \neg A \\ \neg A & \text{falls } L = A \end{cases}$$

Beispiel:

$$K_1 = \{A_1, \neg A_2, A_3, A_4\}$$

$$K_2 = \{\neg A_1, A_2, A_3, A_5\}$$

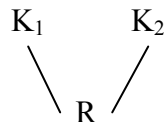
Dann sind:

$$R_1 = \{\neg A_2, A_3, A_4, A_2, A_5\}$$

$$R_2 = \{A_1, A_3, A_4, \neg A_1, A_5\}$$

zwei Resolventen von K_1 und K_2

Schreibweise:



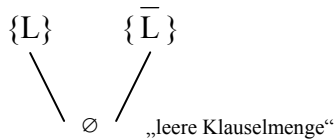
Das ist eine **symbolische** Schreibweise für die **einzige** und syntaktische Regel des Kalküls!

Spezialfall:

$$K_1 = \{L\} \text{ und } K_2 = \{\bar{L}\}$$

Dann gilt: $R = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\bar{L}\}) = \emptyset \cup \emptyset = \emptyset$

symbolisch:



„leere Klauselmenge“

Falls $K_1 = \{L\}$ und $K_2 = \{\bar{L}\}$ Klauselmengen von F sind, dann ist $F \in \text{Sat}$!

Begründung:

Eine Belegung β ist Modell von F gdw sie ist Modell jeder Klausel von F , aber es gibt keine Belegung der Modelle von K_1 und K_2 ist!

Haben: Die leere Klausel \emptyset als „Indiz“ für Unerfüllbarkeit.

Frage: Was passiert durch mehrfache Anwendung der Resolutionsregel?

Satz: (Das Resolutionslemma)

Es sei F eine Klauselmengen und R Resolvent zweier Klauseln K_1 und K_2 von F .

Dann gilt: $F \models F \cup \{R\}$

Beweis:

Wir zeigen: 1. $F \models F \cup \{R\}$

und 2. $F \cup \{R\} \models F$

zu 2) gilt trivialerweise aufgrund der Reflexivität

zu 1)

trivial ist $F \models F$ (aufgrund der Reflexivität)

Es bleibt zu zeigen: $F \models R$

Es sei $L \in K_1$ und $\bar{L} \in K_2$ und $R = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\bar{L}\})$

Es sei β ein Modell von F ; zu zeigen ist β ist ein Modell von R .

Fallunterscheidung:

1. Es sei β ein Modell von L . Dann gilt: β ist kein Modell von \bar{L} .

Aber:

β ist Modell von K_2 , aber ist β Modell von $K_2 \setminus \{\bar{L}\}$ und damit von $R = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\bar{L}\})$.

2. Es sei β kein Modell von L .

Aber:

β ist Modell von K_1 , aber damit ist β Modell von $K_1 \setminus \{L\}$ und somit von R .

Definition

I. Es sei F eine Klauselmengen $\text{Res}(F) := F \cup \{R \mid R \text{ ist Resolvent zweier Klauseln von } F\}$

II. induktiv:

$\text{Res}^0(F) := F$

$\text{Res}^{n+1}(F) := \text{Res}(\text{Res}^n(F))$

III. $\text{Res}^*(F) := \bigcup_{n \in \mathbb{N}} \text{Res}^n(F)$ heißt **Reduktionshülle** von F .

$$1. \quad \overline{\text{Res}^1(F)} = \text{Res}(F) = F \cup \{R \mid R \text{ ist Resolvent}\}$$
$$F \models \text{Res}^1(F) \models \text{Res}^2(F) \models \dots \models \text{Res}^n(F) \models \dots \models \text{Res}^*(F)$$

$\text{Res}^{n_0-1}(F)$ zwei Klauseln $K_1 = \{L\}$ und $K_2 = \{\bar{L}\}$ und $K_1 \quad K_2$.

$$\begin{array}{cc} K_1 & K_2 \\ & \searrow \quad \swarrow \\ & \emptyset \end{array}$$

3. Die Zuordnung: $F \mapsto \text{Res}^*(F)$ ist Hüllenoperator:

- # Resolutionskalkül

Eingabe:

$$\begin{array}{c} K_1 \quad K_2 \\ \diagdown \quad \diagup \\ R(K_1 \setminus \{L\}) \cup \\ (K_2 \setminus \{\bar{L}\}) \end{array}$$

- „Ist F unerfüllbar?“
- Anzeige: „ $\emptyset \in \text{Res}^*(F)$ “?
- Test einer semantischen Eigenschaft erfolgt aufgrund syntaktischer Merkmale

induktiv: $\text{Res}^0(F) := F$

Dabei ist $\text{Res}(F) = F \cup \{R \mid R \text{ ist Resolvent}\}$.

$$\text{Res}^*(F) := \bigcup_{n \in \mathbb{N}} \text{Res}^n(F)$$

sicher: Korrektheit des Verfahrens, d.h. falls $\emptyset_{\epsilon} \text{Res}^*(F)$ (\Rightarrow dies ist Anzeige für unerfüllbar), dann ist F tatsächlich unerfüllbar

Lemma (über die Terminierung der Resolution)

Für jede Klauselmenge F gibt es eine natürliche Zahl k_F , so dass $\text{Res}^*(F) = \text{Res}^{k_F}(F)$!

Beweis: Wir zeigen:

- I. Für jedes F gibt es eine natürliche Zahl k_F mit der Eigenschaft, dass $\text{Res}^{k_F+1}(F) = \text{Res}^{k_F}(F)$
- II. Falls $\text{Res}^{k_F+1}(F) = \text{Res}^{k_F}(F)$ gilt, dann ist $\text{Res}^*(F) = \text{Res}^{k_F}(F)$.
(Resolution wird nach endlich vielen Schritten stationär!!)

zu I)

Für jede endliche Klauselmenge F gilt: Es gibt eine natürliche Zahl n , so dass in F nur die Atome A_1, A_2, \dots, A_n vorkommen. (Dabei ist $\mathcal{A} = \{A_1, A_2, \dots\}$ eine Nummerierung aller Atome.) Für diese Atome ist die Menge verschiedener Klauseln beschränkt:

für jedes Atom sind vier Fälle (pro Klausel) möglich:

1. A kommt vor
2. $\neg A$ kommt vor
3. A und $\neg A$ kommt vor
4. beide kommen nicht vor

Damit gibt es höchstens 4^n verschiedene Klauseln! In jedem Einzelschritt der Resolution wird eine neue Klausel resolviert – oder keine. D.h. nach spätestens **4^n Einzelschritten** ist nichts neues mehr zu resolvieren. Damit ist $k_F = 4^n$ eine **obere Schranke** (grob) für $\text{Res}^{k_F+1}(F) = \text{Res}^{k_F}(F)$.

zu II)

Falls $\text{Res}^{k_F+1}(F) = \text{Res}^{k_F}(F)$, dann gilt:

$$(IA) \quad \text{Res}^{k+2}(F) =_{\text{df}} \text{Res}(\text{Res}^{k+1}(F)) = \text{Res}(\text{Res}^k(F)) = \text{Res}^{k+1}(F) = \text{Res}^k(F)$$

$$(IS) \quad \text{Res}^{k+n}(F) = \text{Res}^k(F)$$

$$\text{Dies liefert } \text{Res}^*(F) = \bigcup_{n=0}^{\infty} \text{Res}^n(F) = \bigcup_{n=0}^k \text{Res}^n(F) = \text{Res}^k(F).$$

Wir zeigen

Vollständigkeit des Kalküls

Falls F unerfüllbar ist, dann gilt $\emptyset \in \text{Res}^*(F)$.

Es sei F irgendeine unerfüllbare Klauselmenge.

1. **Fall:** F ist unendlich.

Endlichkeitssatz: Dann existiert eine endliche Teilmenge F_{fin} von F die unerfüllbar ist.

O.B.d.A. kann 2. Fall angenommen werden!

2. **Fall:** F ist endlich.

Beweis durch vollständige Induktion: über die Anzahl n der Atome A_1, \dots, A_n die in F vorkommen.

(IA)

$n = 0$ (d.h. in F kommen keine Atome vor)
Dann ist $F = \{\emptyset\}$ und damit ist $\emptyset \in \text{Res}^*(F)$.

(IV)

Es sei $n \in \mathbb{N}$ eine natürliche beliebige Zahl, aber fest: Für jede Klauselmenge G , die unerfüllbar ist und in der nur die Atome A_1, \dots, A_n vorkommen, gilt: $\emptyset \in \text{Res}^*(G)$.

(IB – Induktionsbehauptung)

Es sei F eine unerfüllbare Klauselmenge in der die Atome A_1, \dots, A_n, A_{n+1} vorkommen. Dann gilt auch: $\emptyset \in \text{Res}^*(F)$

(IB – Induktionsbeweis) „Befreien“ von A_{n+1}

Ausgehend von F definieren wir zwei neue Klauselmengen F_0 und F_1 auf folgende Weise:

F_0 :

- i. überall wo A_{n+1} (positiv) in einer Klausel von F vorkommt, wird es gestrichen.
- ii. überall wo $\neg A_{n+1}$ in einer Klausel von F vorkommt, wird diese Klausel gestrichen.

F_1 :

- i. überall wo $\neg A_{n+1}$ (positiv) in einer Klausel von F vorkommt, wird es gestrichen.
- ii. überall wo A_{n+1} in einer Klausel von F vorkommt, wird diese Klausel gestrichen.

Wir erhalten zwei Klauselmengen in denen nur die Atome A_1, \dots, A_n vorkommen.

Behauptung:

F_0 und F_1 sind beide unerfüllbar!

Beweis für F_0 :

Annahme: F_0 sei erfüllbar.

Dann gibt es eine Belegung β_0 die Modell von F_0 ist. Dann ist aber

$\beta(A) := \begin{cases} \beta_0(A) & \text{falls } A \in \{A_1, \dots, A_n\} \\ 0 & \text{falls } A \in \{A_{n+1}\} \quad (A = A_{n+1}) \end{cases}$ ein Modell von F .

★ $\left\{ \begin{array}{l} \text{Wir gewinnen aus } F_0 \text{ die Klauseln von } F \text{ zurück, in dem wir die ursprünglichen} \\ \text{Vorkommen von } A_{n+1} \text{ wieder einsetzen (jede solche Klausel bleibt wahr unter} \\ \text{der Belegung } \beta). \text{ Und indem wir jede ursprüngliche Klausel in der } \neg A_{n+1} \\ \text{vorkommt wieder einsetzen (jede solche Klausel wird wahr unter } \beta, \text{ denn es} \\ \text{gilt } I_\beta(\neg A_{n+1}) = 1). \text{ Also wäre } \beta \text{ ein Modell von } F. \textbf{Widerspruch!!!} \text{ (da } F \\ \text{unerfüllbar!} \end{array} \right.$

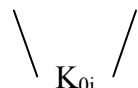
Also gilt für F_0 und F_1 die Induktionsvoraussetzung

0. $\emptyset \in \text{Res}^*(F_0)$ und

1. $\emptyset \in \text{Res}^*(F_1)$.

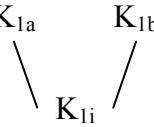
(0.) Es gibt eine Folge von Klauseln $K_{01}, K_{02}, \dots, K_{0s}$ mit folgenden Eigenschaften:

- a. $K_{0s} = \emptyset$ und
- b. für alle $i = 1, \dots, s$ gilt: K_{0i} ist eine Klausel von F_0 oder es gibt zwei Klauseln K_{0a} und K_{0b} mit $a, b < i$ und

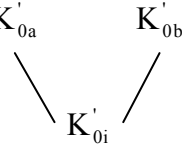


(1.) Analog dazu gibt es eine Folge von Klauseln $K_{11}, K_{12}, \dots, K_{1t}$ mit folgenden Eigenschaften:

- $K_{1t} = \emptyset$ und
- für alle $i = 1, \dots, t$ gilt: K_{1i} ist eine Klausel von F_1 oder es gibt zwei Klauseln K_{1a} und K_{1b} mit $a, b < i$ und



Gemäß (★) gewinnen wir aus der Klauselmenge F_0 die Klauselmenge F zurück und wir betrachten die so gewonnene Folge $K'_{01}, K'_{02}, \dots, K'_{0s}$. Dann gilt: K'_{0i} ist Klausel aus F oder

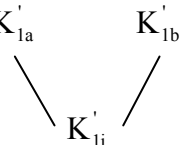


für $a, b < i$ und $K'_{0s} = \emptyset$ oder $K'_{0s} = \{A_{n+1}\}$.

- Fall: $K'_{0s} = \emptyset \Rightarrow$ Dann gilt: $\emptyset \in \text{Res}^*(F)$
- Fall: $K'_{0s} = \{A_{n+1}\}$

Ebenso für (1.) bzw. F_1 :

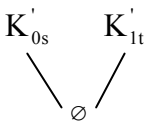
Gemäß (★) gewinnen wir aus der Klauselmenge F_1 die Klauselmenge F zurück und wir betrachten die so gewonnene Folge $K'_{11}, K'_{12}, \dots, K'_{1s}$. Dann gilt: K'_{1i} ist Klausel aus F oder



für $a, b < i$ und $K'_{1t} = \emptyset$ oder $K'_{1t} = \{\neg A_{n+1}\}$.

- Fall: $K'_{1t} = \emptyset \Rightarrow$ Dann gilt: $\emptyset \in \text{Res}^*(F)$
- Fall: $K'_{1t} = \{\neg A_{n+1}\}$

Für die verbleibenden 2. Fälle liefert ein weiterer Resolutionsschritt: K'_{0s} K'_{1t}
Also auch $\emptyset \in \text{Res}^*(F)$.



Fazit: Resolutionssatz der Aussagenlogik:

Es sei F eine Klauselmenge. Dann gilt: F ist unerfüllbar gdw $\emptyset \in \text{Res}^*(F)$.

Algorithmus:

Eingabe: Formel F

Vorprozess: Bestimme äquivalente KNF und daraus die Klauselmenge F .

$n := 0, \text{Res}(n) = F$

//Initialisierung

repeat

$n := n+1, \text{Res}(n) = \text{Res}(\text{Res}(n-1))$

until $\emptyset \in \text{Res}(n)$ **or** $\text{Res}(n) = \text{Res}(n-1)$

if $\emptyset \in \text{Res}(n)$ **then** „unerfüllbar“ **else** „erfüllbar“ **//Ausgabe**

2. Kapitel: Kombinatorik – Die Kunst des Abzählens

Frage:

Gegeben sei eine Menge M . Wie viele Elemente hat M ?

Der Schwierigkeit, diese Frage zu beantworten, hängt wesentlich von der Art des Gegebenseins der Menge ab!

In der Informatik, z.B. sind es Fragen nach dem zeitlichen Aufwand von Algorithmen. (Die zu untersuchenden Mengen sind gegeben durch die Ausführungsschritte von solchen Algorithmen. Schwierig wird es bei Schleifen und Fallunterscheidungen!)

Zur Beantwortung dieser Frage stellt die Kombinatorik eine Sammlung von Grundaufgaben bereit, die in Kombination angewandt werden können.

§7. Elementare Abzählregeln und kombinatorische Grundaufgaben

Abzählregeln

1. Summenregel:

Gegeben seien a_1 Elemente vom Typ A_1 und a_2 Elemente vom Typ A_2 .

Frage:

Auf wie viele Weisen lässt sich ein Element von Typ A_1 oder A_2 auswählen?

Antwort: $a_1 + a_2$

Voraussetzung ist, dass sich die Typen ausschließen (A_1 und A_2 schließen sich wechselseitig aus.)

Begründung:

Es seien $M_1 = \{x \mid x \text{ ist Element vom Typ } A_1\}$ und $M_2 = \{x \mid x \text{ ist Element vom Typ } A_2\}$.

Die Voraussetzung liefert: $M_1 \cap M_2 = \emptyset$ (disjunkte Menge)

Dann gilt: $\text{card}(M_1 \cup M_2) = \text{card } M_1 + \text{card } M_2$

Verallgemeinerung:

Diese Regel gilt auch für beliebige endliche Anzahlen k von sich paarweise ausschließenden Typen A_1, A_2, \dots, A_k .

Es gilt: $\text{card}(M_1 \cup M_2 \cup \dots \cup M_k) = \text{card}(M_1) + \text{card}(M_2) + \dots + \text{card}(M_k)$ unter der Bedingung, dass $M_i \cap M_j = \emptyset$ für $i \neq j$.

2. Produktregel:

Gegeben seien a_1 Elemente vom Typ A_1 und a_2 Elemente vom Typ A_2 .

Frage:

Auf wie viele Weisen lässt sich ein Paar (x_1, x_2) auswählen mit den Eigenschaften: x_1 ist vom Typ A_1 und x_2 vom Typ A_2 ?

Antwort: $a_1 \cdot a_2$

Begründung:

$M_1 \times M_2 = \{(x_1, x_2) \mid x_1 \in M_1, x_2 \in M_2\}$ und es gilt: $\text{card}(M_1 \times M_2) = \text{card}(M_1) \cdot \text{card}(M_2)$

Verallgemeinerung:

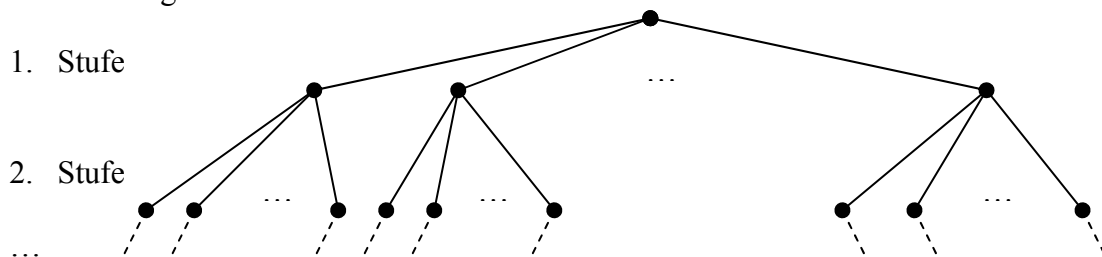
Diese Regel gilt auch für beliebige endliche Anzahlen k vom Typ A_1, A_2, \dots, A_k .

Es gilt: $\text{card}(M_1 \times M_2 \times \dots \times M_k) = \text{card}(M_1) \cdot \text{card}(M_2) \cdot \dots \cdot \text{card}(M_k)$

Die Frage nach der Anzahl der k -Tupel lässt sich auffassen, als ein k -stufiger Entscheidungsprozess:

1. Stufe: a_1 Möglichkeiten für die Wahl eines Elements A_1
2. Stufe: a_2 Möglichkeiten für die Wahl eines Elements A_2
- ⋮
- k. Stufe: a_k Möglichkeiten für die Wahl eines Elements A_k

Entscheidungsbaum:



Die Anzahl $a_1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_k$ der verschiedenen Möglichkeiten entspricht gerade der Anzahl der verschiedenen Pfade in diesem Baum. Die ist gleich der Anzahl der Blätter in diesem Baum.

3. Gleichheitsregel:

Gegeben seien zwei Typen A_1 und A_2 , so dass für die zugehörige Menge $M_1 = \{x_1 \mid x_1 \text{ vom Typ } A_1\}$ und $M_2 = \{x_2 \mid x_2 \text{ vom Typ } A_2\}$ gilt:

Es gibt eine Bijunktion zwischen M_1 und M_2 . Dann gibt es genau so viele Möglichkeiten ein Element vom Typ A_1 zu wählen, wie es Möglichkeiten gibt ein Element vom Typ A_2 zu wählen.

Begründung:

Es gibt eine Bijunktion zwischen M_1 und M_2
 gdw M_1 und M_2 sind gleichmächtig ($M_1 \sim M_2$)
 gdw $\text{card}(M_1) = \text{card}(M_2)$.

Anwendung:

Gegeben sei eine Menge M mit m Elementen.

1. Frage:

Wie viele m -Tupel aus Nullen und Einsen gibt es?

Produktregel:

1. Stufe: zwei Möglichkeiten zur Besetzung der ersten Komponente
2. Stufe: zwei Möglichkeiten zur Besetzung der zweiten Komponente
- ...

m. Stufe: zwei Möglichkeiten zur Besetzung der m-ten Komponente

Der zugehörige Entscheidungsbaum ist der vollständige binäre Baum der Tiefe m! Also gilt: $2 \cdot 2 \cdot 2 \cdot \dots \cdot 2 = 2^m$ Möglichkeiten, d.h.

$$\text{card}(\{x_1, x_2, \dots, x_m \mid x_i \in \{0,1\} \text{ für } i = 1, \dots, m\}) = \text{card}(\{0,1\}^m) = 2^m$$

2. Frage:

Wie viele Elemente enthält die Potenzmenge von M?

Es sei M gegeben als $M = \{y_0, y_1, \dots, y_m\}$.

1. Feststellung:

Jede Teilmenge N von M lässt sich identifizieren mit einem Tupel aus $\{0,1\}^m$. Jedes $N \subseteq M$ lässt sich charakterisieren durch seine charakteristische Funktion χ_N , wobei

$$\chi_N(m) = \begin{cases} 1 & \text{falls } y \in N \\ 0 & \text{falls } y \notin N \end{cases}, y \in M (\chi_N(y_1), \chi_N(y_2), \dots, \chi_N(y_m))$$

2. Feststellung:

Die Zuordnung $N \mapsto \{\chi_N(y_1), \chi_N(y_2), \dots, \chi_N(y_m)\}$ ist bijektiv zwischen $\mathcal{P}(M)$ und $\{0,1\}^m$.

Also gilt: $\text{card}(\mathcal{P}(M)) = \text{card}(\{0,1\}^m) = 2^m$

4. Die Regel vom zweifachen Abzählen

Gegeben sei eine binäre Relation $R: R \subseteq M \times N$.

Wir definieren:

$$R_N(x) := \{y \mid y \in N \wedge (x,y) \in R\} \quad (x \in M)$$

$$R_M(y) := \{x \mid x \in M \wedge (x,y) \in R\} \quad (y \in N)$$

Weiter sei $r_N(x) = \text{card}(R_N(x))$ und $r_M(y) = \text{card}(R_M(y))$.

$$\text{Dann gilt: } \sum_{x \in M} r_N(x) = \sum_{y \in N} r_M(y)$$

Begründung:

$$\sum_{x \in M} r_N(x) = \sum_{x \in M} \text{card}(R_N(x)) = \text{card}(R) = \sum_{y \in N} \text{card}(R_M(y)) = \sum_{y \in N} r_M(y)$$

Es sei $M = N = \{1, 2, \dots, 8\}$ und $R = \{(x,y) \mid x,y \in M \wedge x \mid y\}$.

Das Kreuzprodukt $M \times N$ lässt sich in Form einer $m \times n$ Matrix darstellen. Darin lässt sich die Relation R durch ihre charakteristische Funktion χ_R beschreiben:

zum Beispiel: 8×8 Matrix

	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	0	1	0	1	0	1	0	1
3	0	0	1	0	0	1	0	0
4	0	0	0	1	0	0	0	1
5	0	0	0	0	1	0	0	0
6	0	0	0	0	0	1	0	0
7	0	0	0	0	0	0	1	0
8	0	0	0	0	0	0	0	1

$$\text{Es gilt: } \sum_{x \in M} r_N(x) = \sum_{y \in N} r_M(y) = 20$$

Grundaufgaben

		Anordnungen (Variationen)	Auswählen
Reihenfolge \ Wiederholung		wird berücksichtigt	wird nicht berücksichtigt
ist nicht erlaubt		Permutation ohne Wiederholung	Kombination ohne Wiederholung
ist erlaubt		Permutation mit Wiederholung	Kombination mit Wiederholung

Gebräuchliche Denkmodelle in der Kombinatorik

Das sog. Urnenmodell

Reihenfolge \ Wiederholung		wird berücksichtigt	wird nicht berücksichtigt
ist nicht erlaubt		<ul style="list-style-type: none"> Reihenfolge der Ziehung der Kugeln wird berücksichtigt gezogene Kugeln werden nicht zurück gelegt 	<ul style="list-style-type: none"> Reihenfolge der Ziehung der Kugeln bleibt unberücksichtigt gezogene Kugeln werden nicht zurückgelegt
ist erlaubt		<ul style="list-style-type: none"> Reihenfolge der Ziehung wird berücksichtigt gezogene Kugeln werden zurückgelegt 	<ul style="list-style-type: none"> Reihenfolge der Ziehung unberücksichtigt gezogene Kugeln werden zurückgelegt

Schubfachmodell

Reihenfolge \ Wiederholung		wird berücksichtigt	wird nicht berücksichtigt
ist nicht erlaubt		<ul style="list-style-type: none"> unterscheidbare Gegenstände pro Schubfach höchstens ein Gegenstand 	<ul style="list-style-type: none"> identische Gegenstände pro Schubfach nur ein Gegenstand
ist erlaubt		<ul style="list-style-type: none"> unterschiedliche Gegenstände pro Schubfach mehrere Gegenstände 	<ul style="list-style-type: none"> identische Gegenstände pro Schubfach mehrere Gegenstände

Sprechweise:

Im folgenden sei N stets eine Menge mit n Elementen, d.h. $\text{card}(N) = n$
 \Rightarrow „ N ist eine n -Menge“ (grundsätzlich endliche Mengen!)

1. Permutation ohne Wiederholung

Definition

Eine r-Permutation einer n-Menge N ist \leftrightarrow_{df} ist ein r-Tupel verschiedener Elemente aus N.

D.h. eine r-Permutation von N ist ein Element $(x_1, x_2, \dots, x_r) \in N^r$ wobei gilt: $x_i \neq x_j$ für $i \neq j$.
Klar ist: r ist durch n beschränkt! $r \leq n$

Frage:

Wie viele solcher r-Tupel gibt es?

Schreibweise:

$P(n, r)$ bezeichnet die Anzahl aller r-Tupel einer n-Menge!

Satz:

$$P(n, r) = n(n-1) \cdot \dots \cdot (n-r+1)$$

Beweis:

Dieses Ergebnis ist eine Anwendung der Produktregel: zu Grunde liegt ein r-stufiger Entscheidungsprozess:

1. Stufe: n Möglichkeiten, ein Element aus N zu ziehen
2. Stufe: (n-1) Möglichkeiten, ein weiteres Element aus N zu ziehen
- ...
- r. Stufe: $[n-(r-1)]$ Möglichkeiten ein r-tes Element aus N zu ziehen

wichtiger Spezialfall:

$$P(n, r) = r(r-1) \cdot \dots \cdot 2 \cdot 1$$

Schreibweise: $r! = r(r-1) \cdot \dots \cdot 2 \cdot 1$ für natürliche Zahlen r „r-Fakultät“

$$\text{Damit } P(n, r) = \frac{n!}{(n-r)!}$$

Schreibweise: $n^r = n(n-1) \cdot \dots \cdot (n-r+1) = r! \binom{n}{r}$ „fallende Faktorielle“

2. Permutation mit Wiederholung

Definition

Eine r-Permutation mit Wiederholung einer n-Menge N ist \leftrightarrow_{df} ein r-Tupel von Elementen aus N.

D.h. eine r-Permutation mit Wiederholung einer n-Menge N ist ein Element $(x_1, \dots, x_r) \in N^r$.
Dies ist aufzufassen als eine Abbildung einer r-Menge R in die n-Menge N.

Satz: n^r ist die Anzahl aller r -Tupel der n -Menge N .

Begründung:

Auch dies ist eine Anwendung der Produktregel mit r -stufigem Entscheidungsprozess mit je n Möglichkeiten.

3. Kombination ohne Wiederholung

Definition

Eine r -Permutation einer n -Menge N ist \leftrightarrow_{df} ist eine r Teilmenge von N .
Klar ist: $r \leq n$

Schreibweise:

$C(n,r)$ bezeichnet die Anzahl der r -Permutationen einer n -Menge N .

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

Beweis:

Frage: Welcher Zusammenhang besteht zwischen der r -Permutation und der r -Kombination?

Antwort: Jede r -Teilmenge von N lässt sich auf genau $P(n,r) = r!$ Weisen anordnen;
d.h. $P(n,r) = P(n,r) \cdot C(n,r)$

also gilt: $\frac{P(n,r)}{P(n,r)} = C(n,r) = \frac{n^r}{r!} = \frac{n!}{(n-r)!r!}$

Schreibweise: $\binom{n}{r} = C(n,r) = \frac{n!}{(n-r)!r!}$ „ n über r “ heißt **Binomialkoeffizient**.

4. Kombination mit Wiederholung

Beobachtung:

In einer gegebenen Menge N kommt es *weder* auf die **Reihenfolge** der Elemente an, *noch* auf die **Vielfachheit** der Elemente.

zum Beispiel: $\{1,1,2,2,3,3\} = \{1,2,3\} = \{3,3,3,1,2,2\} = \dots$

Fakt:

Bei **Multi-Mengen** kommt es auf die Vielfachheit der Elemente an!

Für Multi-Mengen gilt:

$\{1,1,2,2,3,3\} \neq \{1,2,2,3,3,3\}$ und $\text{card}(\{1,1,2,2,3,3\}) = 6 = \text{card}(\{1,2,2,3,3,3\})$

Definition

Eine r -Kombination mit Wiederholung einer n -Menge N ist \leftrightarrow_{df} eine **r -Multi-Teilmenge** von N .

Satz: $\binom{n+r-1}{r}$ ist die Anzahl der r -Kombination mit Wiederholung einer n -Menge.

Beweis:

1. Variante: Anwendung der Gleichheitsregel:

Gegeben sei die n -Menge $N = \{1, 2, \dots, n\}$. Eine r -Multi-Teilmenge von N ist gegeben durch a_1, a_2, \dots, a_r wobei alle diese $a_i \in N$ mit der Eigenschaft $a_i \leq a_{i+1}$ für $i = 1, 2, \dots, r-1$ gilt.

Schreibweise: für eine solche r -Multi-Teilmenge von N : $\{a_1 \leq a_2 \leq \dots \leq a_r\}$

X sei die Menge aller r -Multi-Teilmengen von N .

D.h. $X =_{df} \{\{a_1 \leq a_2 \leq \dots \leq a_r\} \mid a_i \in N, a_i \leq a_{i+1} \text{ für } i = 1, \dots, r-1\}$

Gesucht wird: $\text{card}(X)$

Wir betrachten folgende Menge M .

$M := \{1, 2, \dots, n, n+1, \dots, n+r-1\}$

Y sei die Menge aller r -Teilmengen von M !

Dann gilt: die Anzahl der Elemente von Y ist: $\text{card}(Y) = \binom{n+r-1}{r}$

Behauptung: $X \sim Y$ (X und Y sind gleichmächtig bzw. äquivalent)

Schreibweise: für die Elemente aus Y : $\{b_1 < b_2 < \dots < b_r\}$

Zuordnung:

φ der Elemente aus X in Elemente aus Y : $\varphi(\{a_1 \leq a_2 \leq \dots \leq a_r\}) := \{a_1 < a_2 + 1 < \dots < a_r + (r-1)\}$

Dann gilt: $1 \leq a_1 = b_1$ und \dots und $a_r \leq n$ und damit $a_r + (r-1) = b_r \leq n + (r-1)$

Also gilt: $b_1, b_2, \dots, b_r \in M$

Da $a_i \leq a_{i+1} \Rightarrow b_i = a_i + (i-1) \leq a_{i+1} + (i-1) < a_{i+1} + i = b_{i+1}$. D.h. b_1, b_2, \dots, b_r ist eine r -Teilmenge von M . Diese Zuordnung ist bijektiv zwischen X und Y .

Wir definieren die Umkehrabbildung ψ von Y auf X .

$\psi(\{b_1 < b_2 < \dots < b_r\}) := \{b_1 \leq b_2 - 1 \leq b_3 - 2 \leq \dots \leq b_r - (r-1) \leq n\}$

Es gilt: $\psi \circ \varphi = \text{Id}_X$

2. Variante:

Wir untersuchen eine geeignete Codierung (Darstellung) von r -Multi-Teilmengen der n -Menge N . Dazu verwenden wir folgendes Alphabet: $\sum \{*, |\}$

Dabei ist „|“ ein Trennsymbol mit der Vereinbarung, dass vor dem i -ten Trennsymbol der Vielfachheit des i -ten Elementes von N stehen. Und „*“ ist ein Platzhalter für die Vielfachheiten.

zum Beispiel:

$N = \{1,2,3,4\}$ und betrachten 6-Multi-Teilmengen:

$\{1,2,2,4,4,4\}$ sei codiert durch $\{**||***\}$

Frage: Wie viele solcher Codewörter gibt es?

Es gibt pro Wort r Platzhalter „*“ und $(n-1)$ Trennsymbole „|“. Also hat ein solches Codewort $r + (n-1) = n + r - 1$ Plätze (Symbole). Auf diesen Plätzen sind r Symbole * unterzubringen. Dafür gibt es so viele Möglichkeiten, wie es r -Teilmengen einer $(n+r-1)$ -Menge gibt:

also:
$$\binom{n+r-1}{r}$$

§8. Binomialkoeffizienten

Frage: Woher kommt der Name?

Satz: Der binomische Satz: $(x + y)^n = \sum_{r=0}^n \binom{n}{r} x^{n-r} y^r$

Beweis:

Die n -Klammern $(x + y)$ der linken Seite werden aufgefasst als n Schubfächer. Das Distributivgesetz $[(x + y)z = xz + yz]$ formt ein Produkt von Summen $(x + y) \cdot \dots \cdot (x + y)$ in eine Summe der Form $x^i y^j$ mit $i + j = n$. Ein Produkt der Form $x^{n-r} y^r$ entsteht genau dann,

wenn aus genau r Fächern der Term y gewählt wird. Dafür $\binom{n}{r}$ Möglichkeiten.

weitere Eigenschaften:

Satz:

1. Symmetrie: $\binom{n}{r} = \binom{n}{n-r}$
2. Rekursion: $\binom{n+1}{r+1} = \binom{n}{r} + \binom{n}{r+1}$

Beweis:

zu 1) mit Hilfe der Gleichheitsregel:

Gegeben sei eine n -Menge N . Die Zuordnung, die jeder Teilmenge A von N ihr Komplement $\bar{A} = N \setminus A$ zuordnet, ist eineindeutig von der Menge aller r -Teilmengen von N auf die Menge aller $(n-r)$ -Teilmengen von N .

zu 2) mit Hilfe der Gleichheits- und Summenregel:

Gegeben sei eine Menge M mit $n+1$ Elementen. a sei ein beliebiges, aber fixiertes Element aus M . Wir klassifizieren die $(r+1)$ -Teilmengen von M danach, ob sie a enthalten oder nicht!

- i. Es gibt $\binom{n+1}{r+1}$ $(r+1)$ -Teilmengen von M .
- ii. Wir betrachten $(r+1)$ -Teilmengen, die a enthalten. Jede solche Teilmenge enthält von den verbleibenden n Elementen von $M \setminus \{a\}$ genau r verschiedene.
Also gibt es $\binom{n}{r}$ derartige Teilmengen.
- iii. Wir betrachten die Teilmengen, die a nicht enthalten. Jede solche Teilmenge enthält von den verbleibenden n Elementen von M $(r+1)$ verschiedene Elemente von $M \setminus \{a\}$.
Also gibt es $\binom{n}{r+1}$ derartige Teilmengen.

Diese Rekursion erlaubt eine Berechnung der Binomialkoeffizienten im PASCALschen

Dreieck. Dabei gilt stets $\binom{n}{0} = 1$ (Anzahl der Teilung mit 0 Elementen) und $\binom{n}{n} = 1$ (Anzahl der Teilung mit n Elementen).

$$\begin{array}{ccccccc}
& & & & \binom{0}{0} = 1 & & \\
& & & & & & \\
& & \binom{1}{0} = 1 & & \binom{1}{1} = 1 & & \\
& & & & & & \\
& \binom{2}{0} = 1 & & \binom{2}{1} = 2 & & \binom{2}{2} = 1 & \\
& & & & & & \\
\binom{3}{0} = 1 & & \binom{3}{1} = 3 & & \binom{3}{2} = 3 & & \binom{3}{3} = 1 \\
& & & & & & \\
\binom{4}{0} = 1 & & \binom{4}{1} = 4 & & \binom{4}{2} = 6 & & \binom{4}{3} = 4 & & \binom{4}{4} = 1
\end{array}$$

Spezialfälle des Binomischen Satzes:

1. $x = 1, y = 1 \quad (1+1)^n = \sum_{r=0}^n \binom{n}{r} = 2^n$

Diese Summe ist die **Zeilensumme** im Pascalschen Dreieck; gibt eine Klassifizierung aller Teilmengen einer n -Menge (insgesamt 2^n) nach der Anzahl r der Elemente dieser Teilmengen (jeweils $\binom{n}{r}$ für $r = 0, 1, \dots, n$).

2. $x = 1, y = -1 \quad (1+(-1))^n = \sum_{r=0}^n \binom{n}{r} 1^{n-r} (-1)^r = 0$

Dies ist äquivalent zu $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \dots$

Dies bedeutet für eine gegebene n -Menge ist die Anzahl aller Teilmengen mit gerader Anzahl von Elementen gleich der Anzahl aller Teilmengen mit ungeraden Anzahl von Elementen.

Die Anzahl beträgt damit 2^{n-1} .

3. $x = 1, y = x \quad (1+x)^n = \sum_{r=0}^n \binom{n}{r} x^r$

rechte Seite: Polynom in x mit $\binom{n}{r}$ als Koeffizienten

linke Seite: Funktion $(1+x)^n$ ohne Binomialkoeffizienten, aber mit allen Informationen über diese.

$(1+x)^n$ heißt **erzeugende Funktion** für die Binomialkoeffizienten $\binom{n}{r}$.

Damit ist $(1+x)^n$ eine konkrete erzeugende Funktion für ein konkretes Abzählproblem.

Methode: Abzählproblem durch erzeugende Funktion zu betrachten!

weitere Eigenschaften:

Wie sieht es mit „**Spaltensummen**“ aus?

Ansatz: unterer Index fixieren; oberen Index laufen lassen!

Dies führt auf Diagonalen im Pascalschen Dreieck von rechts oben nach links unten und damit auf Summen der Form $\binom{r}{r} + \binom{r+1}{r} + \binom{r+2}{r} + \dots$.

Um eine Summe bilden zu können, brauchen wir einen Schnitt etwa in der m-ten Zeile:

$\binom{r}{r} + \binom{r+1}{r} + \binom{r+2}{r} + \dots + \binom{m}{r}$. Dabei ist $m \geq r$. Wir setzen $\binom{n}{r} = 0$ falls $r > n$! Damit

erhalten wir Summen der Form $\sum_{i=0}^m \binom{i}{r}$, d.h. **obere Summation**.

Satz über die obere Summation: $\sum_{i=0}^m \binom{i}{r} = \binom{m+1}{r+1}$

Beweis mit Hilfe der Rekursionsbeziehung:

$$\begin{aligned} \sum_{i=0}^m \binom{i}{r} &= \binom{r}{r} + \binom{r+1}{r} + \binom{r+2}{r} + \binom{r+3}{r} + \dots + \binom{m}{r} \\ &= \binom{r+1}{r+1} + \binom{r+1}{r} + \binom{r+2}{r} + \binom{r+3}{r} + \dots + \binom{m}{r} \\ &= \binom{r+2}{r+1} + \binom{r+2}{r} + \binom{r+3}{r} + \dots + \binom{m}{r} \\ &= \binom{r+3}{r+1} + \binom{r+3}{r} + \dots + \binom{m}{r} \\ &= \binom{r+4}{r+1} + \dots + \binom{m}{r} = \binom{m}{r+1} + \binom{m}{r} = \binom{m+1}{r+1} \end{aligned}$$

neuer Ansatz: Diagonalen von links oben nach rechts unten

Es entstehen Summen der Form $\binom{r}{0} + \binom{r+1}{1} + \binom{r+2}{2} + \dots + \underbrace{\binom{r+m}{m}}_{\text{Schnitt in der Zeile (m+r)}}$.

Dies liefert Summen der Form $\sum_{i=0}^m \binom{r+i}{i}$, d.h. **parallele Summation**.

Satz über die parallele Summation: $\sum_{i=0}^m \binom{r+i}{i} = \binom{r+m+1}{m+1}$

Beweis: Übung!

Anwendung der Binomialkoeffizienten

„Geordnete Zahlenpartitionen“

Frage: Auf wie viele Weisen lässt sich 10 in 6 positive Summanden zerlegen?

z.B. $10 = 1 + 1 + 1 + 2 + 2 + 3$

$p_z(n, k)$ bezeichnet die Anzahl der verschiedenen geordneten Möglichkeiten die Zahl n in k positive Summanden zu zerlegen.

Satz: $p_z(n, k) = \binom{n-1}{k-1}$

Beweis mit Hilfe der Gleichheitsregel:

$\binom{n-1}{k-1}$ ist die Anzahl der $(k-1)$ -Teilmengen einer $(n-1)$ -Menge.

Schreibweise:

für geordnete k -Zerlegungen von n : $a_1 + a_2 + a_3 + \dots + a_n = n$

für das k -Tupel $(a_1, a_2, a_3, \dots, a_n)$ wobei $\sum = n$ und $1 \leq a_i$ ($i = 1, \dots, k$)

Wir definieren eine (eindeutige) Zuordnung:

$$\varphi(„a_1 + a_2 + a_3 + \dots + a_n“) := \{a_1, a_1 + a_2, \dots, a_1 + \dots + a_n\}$$

von der Menge der geordneten k -Zahlpartitionen auf die Menge $(k-1)$ -Teilmengen von $\{1, 2, \dots, n-1\}$ mit der Umkehrabbildung:

$$\psi(\{b_1, b_2, \dots, b_{k-1}\}) := b_1 + (b_2 - b_1) + (b_3 - b_2) + \dots + (n - b_k)$$

Produkte von Binomialkoeffizienten

Satz (Vandermondsche Identität): $\binom{m+n}{r} = \sum_{k=0}^r \binom{m}{k} \binom{n}{r-k}$

Beweis:

Gegeben seien zwei disjunkte Mengen M mit m Elementen und N mit n Elementen.

Dann ist $\binom{m+n}{r}$ die Anzahl der r -Teilmengen von $M \cup N$.

Wir klassifizieren die r -Teilmengen von $M \cup N$ nach der Anzahl k Elemente in M . Es sei $A \subseteq M \cup N$ mit $\text{card}(A) = r$ und $\text{card}(A \cap M) = k$. Dann gilt $\text{card}(A \cap N) = r - k$. Also hat jede solche Menge zwei Komponenten: einen M -Anteil und einen N -Anteil.

Es gibt $\binom{n}{k}$ Möglichkeiten, den M -Anteil zu wählen und es gibt $\binom{n}{r-k}$ Möglichkeiten, den N -Anteil zu wählen.

Die Produktregel liefert $\binom{n}{k} \binom{n}{r-k}$ Möglichkeiten zur Bestimmung von A .

Die Summenregel liefert $\sum_{k=0}^r \binom{n}{k} \binom{n}{r-k}$ Möglichkeiten.

Satz: $\binom{m}{r} \binom{r}{k} = \binom{m}{k} \binom{m-r}{k-r}$

Beweis: Übung!

Multinomialkoeffizienten

Die Symmetrieeigenschaft lautet: $\binom{n}{r} = \binom{n}{n-r}$

anders geschrieben, ergibt sich: $\binom{a+b}{a} = \binom{a+b}{b} =: \binom{a+b}{a, b}$

Klar ist: $\binom{a+b}{a, b} = \frac{(a+b)!}{a!b!}$ Dies ist ein **Binomialkoeffizient**.

Verallgemeinerung: Trinomialkoeffizient: $\boxed{\binom{a+b+c}{a, b, c} := \frac{(a+b+c)!}{a!b!c!}}$

Satz: (Trinomialsatz)

Ausgangspunkt:

$$(x+y+z)^n \Rightarrow \text{ein Produkt von Summen mit } (x+y+z)^n = \sum_{\substack{a+b+c=n \\ 0 \leq a, b, c \leq n}} \binom{a+b+c}{a, b, c} x^a y^b z^c$$

Definition

Für $k > 0$ und für natürliche Zahlen $a_i \geq 0$ für $1 \leq i \leq k$ ist:

$$\binom{a_1 + a_2 + \dots + a_k}{a_1, a_2, \dots, a_k} := \frac{(a_1 + a_2 + \dots + a_k)!}{a_1! a_2! \dots a_k!}$$

Satz: (Multinomialsatz)

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{\substack{a_1 + a_2 + \dots + a_k = n \\ 0 \leq a_1, a_2, \dots, a_k \leq n}} \binom{a_1 + a_2 + \dots + a_k}{a_1, a_2, \dots, a_k} x_1^{a_1} x_2^{a_2} \dots x_k^{a_k}$$

Beweis:

$$\begin{aligned} \binom{a_1 + a_2 + \dots + a_k}{a_1, a_2, \dots, a_k} &= \frac{(a_1 + a_2 + \dots + a_k)!}{a_1! a_2! \dots a_k!} \cdot \frac{(a_2 + a_3 + \dots + a_k)!}{(a_2 + a_3 + \dots + a_k)!} \\ &= \frac{(a_1 + a_2 + \dots + a_k)!}{a_1! (a_2 + a_3 + \dots + a_k)!} \cdot \frac{(a_2 + a_3 + \dots + a_k)!}{a_2! a_3! \dots a_k!} = \binom{a_1 + a_2 + \dots + a_k}{a_2 + \dots + a_k} \cdot \binom{a_2 + a_3 + \dots + a_k}{a_2, a_3, \dots, a_k} \\ &= \underbrace{\binom{a_1 + a_2 + \dots + a_k}{a_2 + \dots + a_k}}_{\text{Bino min koeffizient}} \cdot \underbrace{\binom{a_2 + a_3 + \dots + a_k}{a_3 + \dots + a_k}}_{\text{Bino min koeffizient}} \cdot \binom{a_3 + a_4 + \dots + a_k}{a_3, a_4, \dots, a_k} = \dots \\ &= \binom{a_1 + a_2 + \dots + a_k}{a_2 + \dots + a_k} \cdot \binom{a_2 + a_3 + \dots + a_k}{a_3 + \dots + a_k} \cdot \dots \cdot \binom{a_{k-1} + a_k}{a_k} \\ &= \binom{a_1 + a_2 + \dots + a_k}{a_1, a_2, \dots, a_k} \end{aligned}$$

Ausgehend von der linken Seite $(x_1 + x_2 + \dots + x_k)^n$ liefert das Distributivgesetz eine Summe von Produkten der Form $x_1^{i_1} \cdot x_2^{i_2} \cdot \dots \cdot x_k^{i_k}$, wobei gilt: $i_1 + i_2 + \dots + i_k = n$.

Für die 1. Komponente $x_1^{a_1}$ gibt es genau $\binom{n}{a_1}$ Möglichkeiten.

Für die 2. Komponente $x_2^{a_2}$ gibt es genau $\binom{n-a_1}{a_2}$ Möglichkeiten, aus den verbleibenden $(n-a_1)$ Klammern x_2 auszuwählen.

...

Für die $(k-1)$. Komponente $x_{k-1}^{a_{k-1}}$ gibt es genau $\binom{n-a_1-a_2-\dots-a_{k-2}}{a_{k-1}}$ Möglichkeiten, aus den verbleibenden $(n-a_1-a_2-\dots-a_{k-2})$ Klammern x_{k-1} auszuwählen.

Für die k . Komponente $x_k^{a_k}$ bleibt genau eine Möglichkeit aus den verbleibenden a_k Klammern alle für x_k zu nehmen.

Die Produktregel liefert für diesen k -stufigen Entscheidungsprozess:

$$\binom{n}{a_1} \cdot \binom{n-a_1}{a_2} \cdot \binom{n-a_1-a_2}{a_3} \cdot \dots \cdot \binom{n-a_1-a_2-\dots-a_{k-2}}{a_{k-1}} \cdot 1$$

$$= \binom{a_1+a_2+\dots+a_k}{a_2+\dots+a_k} \cdot \binom{a_2+a_3+\dots+a_k}{a_3+\dots+a_k} \cdot \dots \cdot \binom{a_{k-1}+a_k}{a_k}$$

Mehrfachanordnungen

Frage:

Wie viele unterscheidbare Anordnungen der Buchstaben des folgenden Wortes gibt es?

$\overset{1}{M} \overset{1}{A} \overset{1}{T} \overset{1}{H} \overset{1}{E} \overset{2}{M} \overset{2}{A} \overset{2}{T} \overset{1}{I} \overset{1}{K} \overset{2}{K} \overset{1}{L} \overset{3}{A} \overset{1}{U} \overset{1}{S} \overset{2}{U} \overset{1}{R}$

Ansatz:

Es sind 17 Plätze zu belegen, für paarweise unterscheidbare Buchstaben. Es gibt $17!$ solche Anordnungen!

Wir zählen Vielfachheiten der auftretenden Buchstaben:

$M - 2x \quad E - 1x \quad U - 2x$
 $A - 3x \quad I - 1x \quad R - 1x$
 $T - 2x \quad K - 2x \quad S - 1x$
 $H - 1x \quad L - 1x$

D.h. für den Buchstaben M fallen je $2!$ Anordnungen zusammen:

$\dots M_2 \dots M_1 \dots = \dots M_1 \dots M_2 \dots \rightarrow \dots M \dots M \dots$

Analoges gilt für alle Vielfachheiten! Daraus folgt:

es gibt $\frac{17!}{2! \cdot 3! \cdot 2! \cdot 1! \cdot 1! \cdot 1! \cdot 2! \cdot 1! \cdot 2! \cdot 1! \cdot 1!}$ unterscheidbare Anordnungen dieses Wortes!

Dies ist ebenfalls ein Multinomialkoeffizient.

Definition

$p_k(n; a_1, a_2, \dots, a_k)$ bezeichnet die Anzahl der Mehrfachanordnungen von k unterscheidbaren Objekten, wobei das erste Objekt genau a_1 -mal vorkommt und das zweite Objekt genau a_2 -mal vorkommt usw. und letztlich das k -te Objekt genau a_k -mal vorkommt.

Satz:
$$p_k(n; a_1, a_2, \dots, a_k) = \frac{n!}{a_1! a_2! \dots a_k!} = \binom{a_1 + a_2 + \dots + a_k}{a_1, a_2, \dots, a_k}$$

Spezialfall:

1. $p_k(n; \underbrace{1, 1, 1, \dots, 1}_{n\text{-mal}}) = n!$

Permutation ohne Wiederholung

2. Rekursiver Zusammenhang:

$$p_k(n; a_1, a_2, \dots, a_k) \cdot a_1! = p_k(n; \underbrace{1, \dots, 1}_{a_1\text{-mal}}, a_2, \dots, a_k)$$

§9. Das Inklusion-Exklusion-Prinzip

Betrachten:

Die PIN-Codes von EC-Karten. Das sind vierstellige Wörter über dem Alphabet $Z = \{0, 1, \dots, 9\}$.

Frage:

Wie viele Wörter aus Z^4 gibt es, die (mindestens) eine „1“ und (mindestens) eine „2“ und (mindestens) eine „3“ enthalten?

Verallgemeinerung:

$$Z^r =_{\text{df}} \{z_1 z_2 \dots z_r \mid z_i \in Z \text{ für } 1 \leq i \leq r\}$$

Wir definieren folgende Mengen:

$$A_i^r = \{z_1 z_2 \dots z_r \in Z^r \mid \text{für mindestens einen Index } j \text{ gilt } z_j = i, \text{ für } i = 1, 2, 3\}$$

Damit lautet die Frage: $\text{card}(A_1^r \cap A_2^r \cap A_3^r) = ?$

Umformulierung des Problems:

Für $i = 1, 2, 3$ sei K_i^r die Menge aller Wörter aus Z^r , die die Ziffern „i“ nicht enthalten:

$$\text{Damit gilt: } K_i^r = Z^r \setminus A_i^r \text{ für } i = 1, 2, 3$$

$$\text{und weiter: } A_1^r \cap A_2^r \cap A_3^r = Z^r \setminus (K_1^r \cap K_2^r \cap K_3^r).$$

Dies führt auf die neue Frage: $\text{card}(K_1^r \cap K_2^r \cap K_3^r) = ?$

1. Ansatz:

$$\text{card}(K_1^r \cap K_2^r \cap K_3^r) = \text{card}(K_1^r) + \text{card}(K_2^r) + \text{card}(K_3^r)$$

(Dieser Ansatz resultiert aus der Summenregel, die gilt jedoch nur für disjunkte Mengen! Unsere sind jedoch nicht disjunkt!)

2. Ansatz:

$$\text{card}(K_1^r \cap K_2^r \cap K_3^r) = \text{card}(K_1^r) + \text{card}(K_2^r) + \text{card}(K_3^r)$$

$$= \text{card}(K_1^r \cap K_2^r) - \text{card}(K_2^r \cap K_3^r) - \text{card}(K_3^r \cap K_1^r)$$

Auch dieser Ansatz ist noch nicht korrekt! Denn: Es gibt Wörter die weder eine „1“ noch eine „2“ noch eine „3“ enthalten! Diese werden auf der rechten Seite nicht korrekt gezählt!

3. Ansatz:

$$\left. \begin{aligned} \text{card}(K_1^r \cup K_2^r \cup K_3^r) &= \underbrace{\text{card}(K_1^r) + \text{card}(K_2^r) + \text{card}(K_3^r)}_{\text{Inklusion}} \\ &\quad - \underbrace{\text{card}(K_1^r \cap K_2^r) - \text{card}(K_2^r \cap K_3^r) - \text{card}(K_3^r \cap K_1^r)}_{\text{Exklusion}} \\ &\quad + \underbrace{\text{card}(K_1^r \cap K_2^r \cap K_3^r)}_{\text{Inklusion}} \end{aligned} \right\} (*)$$

Frage: Stimmt diese Gleichung (*)?

Begründung: Fallunterscheidung:

1. Fall:

Wir betrachten Wörter (aus $K_1^r \cap K_2^r \cap K_3^r$), die zu genau einer der drei Mengen gehören.

Fakt: Ein solches Wort wird links genau einmal gezählt und rechts auch genau einmal.

2. Fall:

Wir betrachten Wörter, die zu genau zwei der drei Mengen gehören.

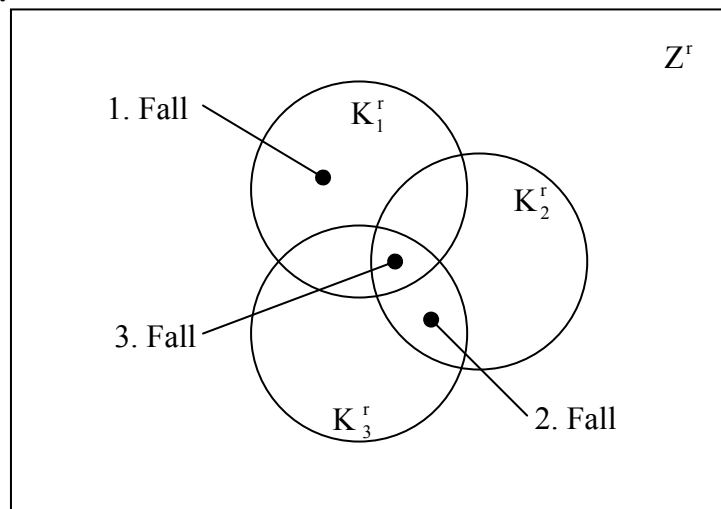
Fakt: Ein solches Wort wird auf der rechten zweimal hinzugezählt (1. Zeile) und einmal abgezogen (2. Zeile).

3. Fall:

Wir betrachten Wörter, die zu allen drei Mengen gehören.

Fakt: Ein solches Wort wird rechts dreimal hinzugezählt (1. Zeile) und dreimal abgezogen (2. Zeile) und einmal hinzugezählt (3. Zeile).

Venn-Diagramm:



Damit gilt: da $\text{card}(K_i^r) = 9^r$ für $i = 1, 2, 3$
und $\text{card}(K_i^r \cap K_j^r) = 8^r$ für $i \neq j$
und $\text{card}(K_1^r \cap K_2^r \cap K_3^r) = 7^r$:
 $\text{card}(K_1^r \cup K_2^r \cup K_3^r) = 3 \cdot 9^r - 3 \cdot 8^r + 7^r$

Damit gilt für die ursprüngliche Frage:

$$\text{card}(A_1^r \cap A_2^r \cap A_3^r) = \text{card}(Z^r) - \text{card}(K_1^r \cup K_2^r \cup K_3^r) = 10^r - 3 \cdot 9^r + 3 \cdot 8^r - 7^r$$

\Rightarrow typ.: Summe mit alternierenden Vorzeichen

Verallgemeinerung:

Für beliebig viele Mengen K_1, K_2, \dots, K_n ; $n \geq 2$. Jede dieser Mengen K_i werde durch eine Eigenschaft (einen Typ) E_i definiert:

Daraus folgt:

$$K_i = \{x \in U \mid x \text{ erfüllt die Eigenschaft } E_i \text{ bzw. ist vom Typ } E_i\}$$

Für den Fall, dass sich diese Eigenschaften wechselseitig nicht ausschließen, sind die Mengen paarweise nicht disjunkt!

Frage:

Wie viele Elemente besitzt $K_1 \cup K_2 \cup K_3 \cup \dots \cup K_n$?

D.h. wie viele Elemente erfüllen (mindestens) eine der gegebenen n Eigenschaften?

Wir definieren die folgenden Hilfsgrößen:

$$n = \binom{n}{1} \text{ Summanden } S_1 =_{\text{df}} \text{card}(K_1) + \text{card}(K_2) + \dots + \text{card}(K_n)$$

$$\begin{aligned} \binom{n}{2} \text{ Summanden } S_2 =_{\text{df}} & \text{card}(K_1 \cap K_2) + \text{card}(K_1 \cap K_3) + \dots + \text{card}(K_1 \cap K_n) \\ & + \text{card}(K_2 \cap K_3) + \dots + \text{card}(K_2 \cap K_n) \\ & \quad \ddots \\ & + \text{card}(K_{n-1} \cap K_n) \end{aligned}$$

usw.

kürzer:

$$S_1 = \sum_{i=1}^n \text{card}(K_i)$$

$$S_2 = \sum_{i_1=1}^n \sum_{i_2=i_1+1}^n \text{card}(K_{i_1} \cap K_{i_2})$$

$$S_3 = \sum_{i_1=1}^n \sum_{i_2=i_1+1}^n \sum_{i_3=i_2+1}^n \text{card}(K_{i_1} \cap K_{i_2} \cap K_{i_3})$$

\vdots

noch kürzer:

$$S_2 = \left\{ \sum_{1 \leq i_1 < i_2 \leq n} \text{card}(K_{i_1} \cap K_{i_2}) \right\} \left\{ \binom{n}{2} \text{ Summanden} \right.$$

$$S_3 = \left\{ \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \text{card}(K_{i_1} \cap K_{i_2} \cap K_{i_3}) \right\} \left\{ \binom{n}{3} \text{ Summanden} \right.$$

$$S_j = \left\{ \sum_{\substack{1 \leq j \leq n \\ 1 \leq i_1 < \dots < i_j \leq n}} \text{card}(K_{i_1} \cap K_{i_2} \cap \dots \cap K_{i_j}) \right\} \left\{ \binom{n}{j} \text{ Summanden} \right.$$

$$\begin{aligned} S_n &= \left\{ \sum_{1 \leq i_1 < \dots < i_n \leq n} \text{card}(K_{i_1} \cap K_{i_2} \cap \dots \cap K_{i_n}) \right\} \left\{ \binom{n}{n} 1 \text{ Summand} \right. \\ &= \text{card}(K_1 \cap K_2 \cap K_3 \cap \dots \cap K_n) \end{aligned}$$

$S_{\text{gesamt}} \dots$ Anzahl der Elemente des Grundbereichs U (Universum)

$S^* \dots$ Anzahl der Elemente des Grundbereichs U , die (mindestens) eine Eigenschaft E_1, E_2, \dots, E_n erfüllen

D.h. natürlich: $S_* = \text{card}(K_1 \cup K_2 \cup \dots \cup K_n)$

Weiter sei:

$S_0 \dots$ Anzahl der Elemente des Grundbereichs U , die keine Eigenschaft E_1, E_2, \dots, E_n erfüllen

D.h. $S_0 = \text{card}(U \setminus (K_1 \cup K_2 \cup \dots \cup K_n)) = \text{card}(\overline{K_1} \cap \overline{K_2} \cap \dots \cap \overline{K_n})$

$\overline{K_i}$ bezeichnet das Komplement von K_i relativ zu U .

wenn $A_i = \overline{K_i} : S_0 = \text{card}(A_1 \cap A_2 \cap \dots \cap A_n)$

Satz: (Inklusion-Exklusion-Prinzip (IEP))

$$S_* = S_1 - S_2 + S_3 - \dots + (-1)^{n-1} S_n$$

→ Addition ⇒ Inklusion

→ Subtraktion ⇒ Exklusion

$$S_0 = S_{\text{gesamt}} - S_*$$

$$S_0 = S_{\text{gesamt}} - S_1 + S_2 - S_3 + \dots + (-1)^n S_n$$

Beweis:

durch Fallunterscheidung: n Fälle

Fall j: Untersuchen der Vielfachheit der Elemente, die zu genau j der n Mengen gehören
(Jedes solches Element wird auf der linken Seite einmal gezählt.)
auf der rechten Seite:

im Term S_1 : Element wird j-mal gezählt = $\binom{j}{1}$

im Term S_2 : $\binom{j}{2}$ -mal gezählt

im Term S_3 : $\binom{j}{3}$ -mal gezählt

⋮

im Term S_j : $\binom{j}{j} = 1$ mal

im Term S_{j+1} : 0 mal

⋮

im Term S_n : 0 mal

Daraus ergibt sich für die Vielfachheit auf der rechten Seite:

$$\begin{aligned} S_* &= \binom{j}{1} - \binom{j}{2} + \binom{j}{3} - \binom{j}{4} + \dots + (-1)^{j-1} \binom{j}{j} + \underbrace{(-1)^j \cdot 0 + (-1)^{j+1} \cdot 0 + \dots + (-1)^{n-1} \cdot 0}_{=0} \\ &= \left[\binom{j}{0} - \binom{j}{1} \right] + \left[\binom{j}{1} - \binom{j}{2} \right] + \dots + (-1)^{j-1} \binom{j}{j} \\ &= \binom{j}{0} - \left[\binom{j}{0} - \binom{j}{1} + \binom{j}{2} - \dots + (-1)^j \binom{j}{j} \right] \\ &= 1 - [(1-1)^j] = 1 \end{aligned}$$

Anwendungen des IEP

1. „Umordnungen“:

Damit ist eine Umordnung eine Bijektion einer n -Menge ohne Fixpunkte.

Aufgabe:

Gegeben seien n verschiedene Briefe und n adressierte Umschläge. Wie viele Möglichkeiten gibt es, dass kein Brief im zugehörigen Umschlag steckt?

Modell:

Beschreiben die Aufgabe mittels Zuordnung der Mengen $N = \{1, 2, \dots, n\}$ auf sich selbst.

Schreibweise:
$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ \Pi(1) & \Pi(2) & \Pi(3) & \dots & \Pi(n-1) & \Pi(n) \end{pmatrix}$$

Dabei ist Π eine Bijektion von N auf sich selbst!

Definition

Ein Element $i \in N$ heißt **Fixpunkt** von $\Pi \leftrightarrow_{\text{df}} \Pi(i) = i$. Eine Bijektion Π besitzt die Eigenschaft $E_i \leftrightarrow_{\text{df}} \Pi(i) = i$. (damit $E_i(\Pi) \Leftrightarrow \Pi(i) = i$)

Umformulierung der Aufgabe:

Wie viele der Permutationen von N auf sich selbst besitzen keinen Fixpunkt, d.h. erfüllen die Eigenschaft E_1, \dots, E_n nicht?

Übersetzt auf das IEP heißt dies: Bestimme S_0 !

Dabei ist $S_{\text{gesamt}} = n!$ und $S_0 = S_{\text{gesamt}} - S_1 + S_2 - S_3 + \dots + (-1)^n S_n$.

Dabei bleibt S_1, S_2, \dots, S_n zu bestimmen. Dazu definieren wir für $1 \leq i_1 < i_2 < \dots < i_j \leq n$ eine Hilfsgröße $S_{i_1 i_2 i_3 \dots i_j}$ als die Anzahl der Bijektionen, die die Eigenschaften

$E_{i_1}, E_{i_2}, \dots, E_{i_j}$ erfüllen!

D.h. gesucht ist die Anzahl der Bijektionen von N auf sich selbst mit $\Pi(i_1) = i_1$ und $\Pi(i_2) = i_2$ und ... und $\Pi(i_j) = i_j$. Für die verbleibenden $(n-j)$ Argumente von Π gibt es $(n-j)!$ Möglichkeiten der Zuordnung!

Also gilt: $S_{i_1 i_2 i_3 \dots i_j} = (n-j)!$ und $S_j = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq n} S_{i_1 i_2 i_3 \dots i_j} = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq n} (n-j)! = \binom{n}{j} (n-j)!$

Damit ergibt sich für die gesuchte Anzahl:

$$S_0 = \binom{n}{0} \cdot n! - \binom{n}{1} \cdot (n-1)! + \binom{n}{2} \cdot (n-2)! - \dots + (-1)^n \binom{n}{n} \cdot 0!$$

Frage: Was ist der Zahlenwert von S_0 ?

Exkurs in die Analysis:

Satz: (Potenzreihe der Exponentialfunktionen)

Es gilt:

$$1) e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad \text{und} \quad 2) \left| \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \right| \leq \frac{1}{(n+1)!}$$

speziell für $x = -1$ gilt:
$$e^{-1} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = 1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \cdot \frac{1}{n!} + \dots$$

andererseits:

$$\begin{aligned} S_0 &= n! - \frac{n!}{(n-1)! \cdot 1!} (n-1)! + \frac{n!}{(n-2)! \cdot 2!} (n-2)! - \dots + (-1)^n \cdot \frac{n!}{n! \cdot 0!} \cdot 0! \\ &= n! \cdot \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \cdot \frac{1}{n!} \right] \end{aligned}$$

und damit:
$$S_0 = n! \left[\sum_{n=0}^{\infty} \frac{(-1)^n}{n!} - \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \right]$$

also:
$$n! \cdot \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} - S_0 = n! \cdot \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!}$$

damit gilt:
$$\left| \frac{n!}{e} - S_0 \right| = n! \cdot \left| \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \right| \leq n! \cdot \frac{1}{(n+1)!} = \frac{1}{n+1}$$

also gilt:
$$S_0 \approx \frac{n!}{e}$$

(d.h. S_0 ist diejenige natürliche Zahl, die am „dichtesten“ an $\frac{n!}{e}$ liegt!)

Zusatzfrage:

Wie groß ist die Wahrscheinlichkeit dafür, bei einer zufällig gewählten Bijektion eine solche zu erwischen, die keine Fixpunkte hat?

⇒ gefragt ist also nach der relativen Häufigkeit:

$$\text{relative Häufigkeit} = \frac{\text{Anzahl der günstigen Möglichkeiten}}{\text{Anzahl aller Möglichkeiten}} = \frac{S_0}{n!} \approx \frac{n!}{e \cdot n!} = \frac{1}{e} \approx 0,3679$$

Dieser Wert ist unerwarteter Weise unabhängig vom gegebenen Wert n !

2. „Surjektionen“:

Aufgabe:

Gegeben seien eine m -Menge M mit den Elementen $a_1, a_2, a_3, \dots, a_m$ und eine n -Menge N mit den Elementen $b_1, b_2, b_3, \dots, b_n$ mit der Eigenschaft $n \leq m$!

Bestimme die Anzahl aller Surjektionen von M auf N .

$$\text{Surj}(M, N) =_{\text{df}} \{f \mid f: M \rightarrow N\}$$

D.h. bestimme die Kardinalität $\text{card}(\text{Surj}(M, N))$!

Als Grundbereich legen wir fest: $\text{Abb}(M, N) =_{\text{df}} \{f \mid f: M \rightarrow N\}$

Hierfür gibt:
$$S_{\text{gesamt}} = \text{card}(\text{Abb}(M, N)) = n^m$$

Bemerkung:

$$\text{Inj}(M, N) =_{\text{df}} \{f \mid f: M \xrightarrow{1-1} N\}$$

Dies fordert $n \geq m$ und liefert: $\text{card}(\text{Inj}(M, N)) = n^{\underline{m}} = n \cdot (n-1) \cdot \dots \cdot (n-m+1)$

Wir definieren folgende Eigenschaften E_1, \dots, E_n :

Eine Abbildung $f: M \rightarrow N$ hat die Eigenschaft $E_i \leftrightarrow_{\text{df}} b_i \in W_f = \{b \in N \mid \forall a \in M: f(a) = b\}$

Damit gilt: $f \in \text{Surj}(M, N) \rightarrow f$ besitzt keine der Eigenschaften E_1, \dots, E_n und

$$\text{card}(\text{Surj}(M, N)) = S_0 = S_{\text{gesamt}} - S_1 + S_2 - S_3 + \dots + (-1)^n S_n$$

Aufgabe: Bestimmen von S_1, \dots, S_n

Wir definieren ähnlich wie eben für $1 \leq i_1 < i_2 < \dots < i_j \leq n$ Hilfsgrößen $S_{i_1 i_2 i_3 \dots i_j}$ als die

Anzahl der Abbildungen $f \in \text{Abb}(M, N)$, die die Eigenschaften $E_{i_1}, E_{i_2}, \dots, E_{i_j}$ erfüllen!

f erfüllt genau diese Eigenschaften, wenn gilt: $b_{i_1} \notin W_f, b_{i_2} \notin W_f, \dots, b_{i_j} \notin W_f$

D.h. für ein solches f gilt: $f: M \rightarrow N \setminus \{b_{i_1}, \dots, b_{i_j}\}$

D.h. für ein solches f gilt: $f \in \text{Abb}(M, N \setminus \{b_{i_1}, \dots, b_{i_j}\})$

Es gilt genau: $(n-j)^m$ solcher Abbildungen

und damit gilt: $S_{i_1 i_2 i_3 \dots i_j} = (n-j)^m$

$$\text{und } S_j = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq n} S_{i_1 i_2 i_3 \dots i_j} = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq n} (n-j)^m = \binom{n}{j} (n-j)^m$$

und damit ergibt sich die gesuchte Anzahl S_0 :

$$S_0 = \binom{n}{0} \cdot n^m - \binom{n}{1} \cdot (n-1)^m + \binom{n}{2} \cdot (n-2)^m - \dots + (-1)^n \binom{n}{n} \cdot 0^m$$

$$S_0 = \sum_{j=0}^n (-1)^j \cdot \binom{n}{j} \cdot (n-j)^m = \text{card}(\text{Surj}(M, N))$$

(Dabei sind wiederum m und n vorgegeben und fixiert!)

D.h. S_0 ist eigentlich ein Wert $S_{m,n,0}$

3. Die Eulersche ϕ -Funktion

Definition

$\phi(n) =_{\text{df}} \text{card}\{m \mid 1 \leq m \leq n \wedge m \text{ ist teilerfremd zu } n\}$ weiter gilt: m ist teilerfremd zu $n \leftrightarrow \text{ggT}(m, n) = 1$.

Beispiel:

$\text{ggT}(12, 15) = 3 \rightarrow$ nicht teilerfremd

$\text{ggT}(14, 15) = 1 \rightarrow$ teilerfremd

- falls $n = p$ eine Primzahl ist, dann gilt: $\phi(p) = p-1$, da alle $1 \leq m \leq p-1$ nicht p als Teiler haben

- falls $n = p^k$ eine Primzahlpotenz ist, dann gilt: $\varphi(p^k) = p^k \cdot \underbrace{\left(1 - \frac{1}{p}\right)}_{\substack{\text{alle Vielfachen von } p \\ \text{haben mit } p^k \text{ den} \\ \text{gemeinsamen Teiler } p}} = p^k \cdot \left(1 - \frac{1}{p}\right)$

Wertetabelle:

n	1	2	3	4	5	6	7	8	9
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Beispiel:

$n = 360$

Betrachten der Primzahlzerlegung: $360 = 2^3 \cdot 3^2 \cdot 5$

Eine Zahl $m \in \{1, 2, \dots, 360\}$ ist teilerfremd zu $n \leftrightarrow m$ ist durch keine d Primzahlen 2, 3 und 5 teilbar.

Wir definieren die folgenden Eigenschaften:

für $p = 2, 3, 5 \Rightarrow m$ erfüllt die Eigenschaft $E_p \leftrightarrow_{\text{df}} 1 \leq m \leq 360$ ist teilerfremd zu 360 $\leftrightarrow m$ erfüllt keine der Eigenschaften E_2, E_3 und E_5 .

Damit gilt: $\varphi(360) \stackrel{\text{IEP}}{=} S_0 = S_{\text{gesamt}} - S_1 + S_2 - S_3 \}$ 3 Eigenschaften

wobei gilt: $S_{\text{gesamt}} = 360$

Es bleibt zu bestimmen: S_1, S_2, S_3

$$1. \quad S_1 = \text{card}\{m \mid E_2(m)\} + \text{card}\{m \mid E_3(m)\} + \text{card}\{m \mid E_5(m)\}$$

wobei $\text{card}\{m \mid E_2(m)\} = \text{card}\{m \mid 2 \text{ ist Teiler von } m \wedge 1 \leq m \leq 360\}$

$$\text{d.h.} \quad \text{card}\{m \mid m \text{ ist gerade und durch 2 teilbar} \wedge 1 \leq m \leq 360\} = \frac{360}{2} = \underline{\underline{180}}$$

$$\text{weiter gilt:} \quad \text{card}\{m \mid m \text{ ist durch 3 teilbar} \wedge 1 \leq m \leq 360\} = \frac{360}{3} = \underline{\underline{120}}$$

$$\text{und:} \quad \text{card}\{m \mid m \text{ ist durch 5 teilbar} \wedge 1 \leq m \leq 360\} = \frac{360}{5} = \underline{\underline{72}}$$

$$\text{und somit:} \quad S_1 = 180 + 120 + 72 = \underline{\underline{372}}$$

$$2. \quad S_2 = \text{card}\{m \mid E_2(m) \wedge E_3(m)\} + \text{card}\{m \mid E_2(m) \wedge E_5(m)\} + \text{card}\{m \mid E_3(m) \wedge E_5(m)\}$$

$$\text{card}\{m \mid E_2(m) \wedge E_3(m)\} =$$

$$\text{card}\{m \mid m \text{ ist durch 2 und 3 teilbar} \wedge 1 \leq m \leq 360\} = \frac{360}{2 \cdot 3} = \underline{\underline{60}}$$

$$\text{card}\{m \mid E_2(m) \wedge E_5(m)\} =$$

$$\text{card}\{m \mid m \text{ ist durch 2 und 5 teilbar} \wedge 1 \leq m \leq 360\} = \frac{360}{2 \cdot 5} = \underline{\underline{36}}$$

$$\text{card}\{m \mid E_2(m) \wedge E_3(m)\} =$$

$$\text{card}\{m \mid m \text{ ist durch 3 und 5 teilbar} \wedge 1 \leq m \leq 360\} = \frac{360}{3 \cdot 5} = \underline{\underline{24}}$$

$$\text{Daraus folgt:} \quad S_2 = 60 + 36 + 24 = \underline{\underline{120}}$$

$$3. \quad S_2 = \text{card}\{m \mid E_2(m) \wedge E_3(m) \wedge E_5(m)\} = \text{card}\{m \mid m \text{ ist durch 2, 3 und 5 teilbar}\}$$

$$= \text{card}\{m \mid m \text{ ist durch 10 teilbar}\} = \frac{360}{2 \cdot 3 \cdot 5} = \underline{\underline{12}}$$

$$\text{Also gilt: } \varphi(360) = 360 - 372 + 120 - 12 \Rightarrow \varphi(360) = \underline{\underline{96}}$$

Frage:

Gibt es einen besseren Weg? In wie fern ist eine Verallgemeinerung möglich? Ist diese möglich?

Satz: (Fundamentalsatz der Arithmetik)

Für jede natürliche Zahl $n > 1$ gibt es eine eindeutig bestimmte, geordnete Zerlegung in Primzahlpotenzen. D.h. $n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \dots \cdot p_k^{e_k}$ für $p_1 < p_2 < p_3 < \dots < p_k$. Für $1 \leq m \leq n$ gilt: m ist teilerfremd zu $n \leftrightarrow m$ ist weder durch p_1 noch p_2 noch ... noch p_k teilbar.

Wir definieren für $1 \leq i \leq k$ die Eigenschaft E_{p_i} durch $E_{p_i}(m) \leftrightarrow_{\text{df}} m$ ist durch p_i teilbar.

Damit gilt: m ist teilerfremd zu n ($1 \leq m \leq n$) $\leftrightarrow m$ erfüllt keine Eigenschaft E_{p_i} ($1 \leq i \leq k$).

$$\varphi(m) \stackrel{\text{IEP}}{=} S_0 = S_{\text{gesamt}} - S_1 + S_2 - S_3 + \dots + (-1)^k S_k$$

wobei unser Beispiel zeigt:

$$S_1 = \sum_{i=1}^k \text{card}\{m \mid E_{p_i}(m)\} = \sum_{i=1}^k \frac{n}{p_i} = \frac{n}{p_1} + \frac{n}{p_2} + \frac{n}{p_3} + \dots + \frac{n}{p_k} \left\{ \binom{k}{1} \text{ Summanden} \right.$$

$$S_2 = \sum_{1 \leq i_1 < i_2 \leq k} \text{card}\{m \mid E_{p_{i_1}}(m) \wedge E_{p_{i_2}}(m)\} = \sum_{1 \leq i_1 < i_2 \leq k} \frac{n}{p_{i_1} p_{i_2}} \\ = \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \dots + \frac{n}{p_1 p_k} + \frac{n}{p_2 p_3} + \dots + \frac{n}{p_2 p_k} + \dots + \frac{n}{p_{k-1} p_k} \left\{ \binom{k}{2} \text{ Summanden} \right.$$

$$S_3 = \sum_{1 \leq i_1 < i_2 < i_3 \leq k} \text{card}\{m \mid E_{p_{i_1}}(m) \wedge E_{p_{i_2}}(m) \wedge E_{p_{i_3}}(m)\} = \sum_{1 \leq i_1 < i_2 < i_3 \leq k} \frac{n}{p_{i_1} p_{i_2} p_{i_3}} \left\{ \binom{k}{3} \text{ Summanden} \right.$$

\vdots

$$S_n = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq k} \text{card}\{m \mid E_{p_{i_1}}(m) \wedge E_{p_{i_2}}(m) \wedge \dots \wedge E_{p_{i_k}}(m)\} \\ = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq k} \frac{n}{p_{i_1} p_{i_2} \cdot \dots \cdot p_{i_k}} = \frac{n}{p_1 p_2 p_3 \cdot \dots \cdot p_k} \left\{ \binom{k}{k} = 1 \text{ Summanden} \right.$$

Insgesamt ergeben sich durch IEP genau 2^k Summanden für

$$\varphi(n) = n \cdot \left(1 - \underbrace{\frac{1}{p_1} - \frac{1}{p_2} - \dots - \frac{1}{p_k}}_{S_1} + \underbrace{\frac{1}{p_1 p_2} + \dots + \frac{1}{p_1 p_k} + \dots + \frac{1}{p_{k-1} p_k}}_{S_2} - \dots + (-1)^k \cdot \underbrace{\frac{1}{p_1 p_2 \cdot \dots \cdot p_k}}_{S_k} \right) \\ = n \cdot \left[\left(1 - \frac{1}{p_1} \right) \cdot \left(1 - \frac{1}{p_2} \right) \cdot \dots \cdot \left(1 - \frac{1}{p_k} \right) \right]$$

Satz:

Eine Formel für die φ -Funktion $\varphi(m) = n \cdot \prod_{\substack{p \mid n \\ p \text{ ist Teiler} \\ \text{von } n}} \left(1 - \frac{1}{p} \right)$.

Damit gilt:

$$\text{z.B.} \quad \varphi(6) = 6 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 6 \cdot \frac{1}{2} \cdot \frac{2}{3} = \underline{2}$$

$$\varphi(360) = 360 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = \underline{96}$$

weitere Eigenschaften der φ -Funktion:

Satz: (Die φ -Funktion ist multiplikativ)

Für natürliche Zahlen $m, n > 1$, die zueinander teilerfremd sind gilt: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Beweis: (ausgehend vom Fundamentalsatz)

Es gilt:

$$m = q_1^{f_1} q_2^{f_2} \cdot \dots \cdot q_l^{f_l}$$

$$n = p_1^{e_1} p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$$

nach Voraussetzung gilt: $\{q_1, q_2, \dots, q_l\} \cap \{p_1, p_2, \dots, p_k\} = \emptyset$

Dann gilt:

Eine Primzahl p ist Teiler von $m \cdot n$ genau dann wenn gilt: entweder p ist Teiler von m oder p ist Teiler von n .

Hieraus folgt:

$$\varphi(m \cdot n) = (m \cdot n) \cdot \prod_{p \mid (m \cdot n)} \left(1 - \frac{1}{p}\right) = (m \cdot n) \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right) \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

$$\varphi(m \cdot n) = \underbrace{m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right)}_{\varphi(m)} \cdot \underbrace{n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)}_{\varphi(n)}$$

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

Beispiele:

$$\varphi(6) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = \underline{2}$$

$$\varphi(360) = \varphi(8) \cdot \varphi(9) \cdot \varphi(5) = 4 \cdot 4 \cdot 6 = \underline{96}$$

Allgemein:

$$\varphi(n) = \varphi(p_1^{e_1} p_2^{e_2} \cdot \dots \cdot p_k^{e_k}) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdot \dots \cdot \varphi(p_k^{e_k})$$

$$= p_1^{e_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{e_2} \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot p_k^{e_k} \left(1 - \frac{1}{p_k}\right)$$

$$= (p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}) \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

$$\varphi(n) = n \cdot \prod_{p_i \mid n} \left(1 - \frac{1}{p_i}\right)$$

§10. Stirling – Zahlen

Wissen: $\text{card}(\text{Surj}(M,N)) = \sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m \quad (n \leq m)$

andere Sicht:

Im Schubfachmodell bedeutet dies: Anzahl der Möglichkeiten m verschiedene Kugeln auf n nummerierte (aber sonst gleiche) Schubfächer zu verteilen, wobei keines der Schubfächer leer bleibt.

Frage: Welchen Effekt hat die Entfernung der Nummern der Schubfächer?

Eine Verteilung von m unterscheidbaren Kugeln auf n identische Schubfächer entsprechen $n!$ Verteilungen auf die nummerierten Schubfächer (da es $n!$ Möglichkeiten der Nummerierung gibt!).

Also gibt es: $\frac{1}{n!} \cdot \sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m$ verschiedene Möglichkeiten der Verteilung von m unterscheidbaren Kugeln auf n identische Fächer!

Stirling-Zahlen zweiter Art

Definition

Für $m \geq n > 0$ heißt

$$S_{m,n} =_{\text{df}} \frac{1}{n!} \cdot \sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m \quad \text{Stirling-Zahl zweiter Art.}$$

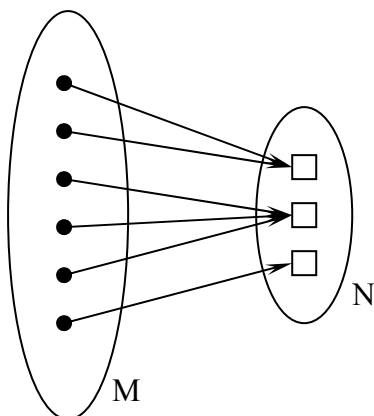
Folgerung:

$\text{card}(\text{Surj}(M,N)) = n! \cdot S_{m,n} \Rightarrow$ Zusammenhang zwischen Stirling-Zahl und Surjektionen

Beispiel:

$m = 6: M = \{1,2,3,4,5,6\}$

$n = 3: N = \{a,b,c\}$



$f: M \mapsto N$

eine solche Surjektion f ist vollständig charakterisierbar durch die Folge seiner Urbilder:

$$(f^{-1}(a), f^{-1}(b), f^{-1}(c)) = (\{1,2\}, \{3,4,5\}, \{6\})$$

Jede Surjektion $f: M \rightarrow N$ bewirkt eine **geordnete** Zerlegung von M in $n=3$ Klassen.

Definition

Es sei M eine m -Menge ($m > 0$).

$\zeta \subseteq \mathcal{P}(M)$ heißt n -Zerlegung von M ($m \geq n$) $\leftrightarrow_{\text{df}}$

1. $\zeta = \{Z_1, Z_2, \dots, Z_n\}$
2. $\emptyset \neq Z_i \subseteq M$ für $1 \leq i \leq n$
3. $\bigcup_{i=1}^n Z_i = M$
4. $Z_i \cap Z_j = \emptyset$ falls $i \neq j$

Damit gilt:

Die Anzahl der Verteilungen von m unterscheidbaren Kugeln auf n identische Fächer entspricht gerade der Anzahl der n -Zerlegungen einer m -Menge. Deshalb gilt der folgende Satz:

Satz:

Die Anzahl der n -Zerlegungen einer m -Menge ($0 < n \leq m$) ist bestimmt durch $S_{m,n}$.

Betrachtung spezieller Werte für $S_{m,n}$:

$$S_{m,1} = 1$$

$$S_{m,m} = 1$$

$$S_{m,m-1} = \binom{m}{2}$$

$$S_{m,2} = 2^{m-1} - 1$$

Frage: Gibt es eine Rekursion – ähnlich wie bei den $\binom{m}{n}$?

Ansatz:

Wir klassifizieren die n -Zerlegung von M nach einem fixierten Element $a \in M$, so dass a entweder (i) eine Klasse $\{a\}$ bildet oder (ii) in einer größeren Klasse enthalten ist.

zu i) Es müssen die verbleibenden $m-1$ Elemente auf $n-1$ Klassen verteilt werden.

Hierfür gibt es genau $S_{m-1,n-1}$ Möglichkeiten.

zu ii) Zunächst sind $m-1$ Elemente auf n Klassen zu verteilen:

Hierfür gibt es $S_{m-1,n}$ Möglichkeiten.

Anschließend ist das „ a “ einer dieser Klassen zuzuordnen. Dafür gibt es jeweils n Möglichkeiten. Für diesen zweistufigen Entscheidungsprozess liefert die Produktregel $S_{m-1,n} \cdot n$ Möglichkeiten.

Dies liefert:

Satz: $S_{m,n} = S_{m-1,n-1} + n \cdot S_{m-1,n}$

Dies liefert eine Möglichkeit der Berechnung der Werte in einem Dreieck (nicht Pascalsches Dreieck!), dem **Stirling-Dreieck zweiter Art**.

Wir legen fest:

$$S_{m,0} := 0 \quad \text{für } m > 0$$

$$S_{0,0} \doteq 1$$

[illegible]

weiter sei $S_{m,n} := 0$ für $n > m$

Wir wissen:

$$\text{card}(\text{Surj}(M,N)) = n! \cdot S_{m,n} \text{ und}$$

$$\text{card}(\text{Inj}(M,N)) = n^m \text{ und}$$

$$\text{card}(\text{Abb}(M, N)) = n^m$$

Frage: Welcher Zusammenhang existiert zwischen diesen kombinatorischen Größen?

Zur Aufklärung der Frage klassifizieren wir die Abbildungen $f: M \mapsto N$:

Für jedes f gibt es eine Teilmenge $A \subseteq \mathbb{N}$, so dass $f: M \mapsto A$.

Dies gilt für $A = f(M)$, $A \in \text{Surj}(M, A)$.

Wir klassifizieren die Abbildungen f nach den Teilmengen $A \subseteq \mathbb{N}$:

$$\text{card}(\text{Abb}(M, N)) = n^m = \sum_{A \subset N} \text{card}(\text{Surj}(M, A))$$

$$= \sum_{k=0}^n \sum_{\substack{A \subseteq N \\ \text{card}(A)=k}} k! \cdot S_{m,k} \quad \left. \vphantom{\sum_{k=0}^n} \right\} \begin{array}{l} \text{die Anzahl hängt nur} \\ \text{ab von der Größe } k \end{array}$$

$$= \sum_{k=0}^n \binom{n}{k} \cdot k! \cdot S_{m,k} = \sum_{k=0}^n \frac{n!}{(n-k)!k!} \cdot k! \cdot S_{m,k}$$

$$= \sum_{k=0}^n \frac{n!}{(n-k)!} \cdot S_{m,k} = \sum_{k=0}^n n^{\underline{k}} \cdot S_{m,k} = n^m$$

Satz:

Zwischen Stirling-Zahlen zweiter Art, fallender Faktoriellen und Potenzen besteht folgende

Beziehung: $n^m = \sum_{k=0}^n n^k \cdot S_{m,k}$

Stirling-Zahlen erster Art

Es sei $M = \{a_1, a_2, \dots, a_m\}$ eine m -Menge. Für Bijektionen $\Pi : M \mapsto M$ (von M auf sich selbst) haben wir folgende Schreibweise:

$$\Pi = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{m-1} & a_m \\ \Pi(a_1) & \Pi(a_2) & \Pi(a_3) & \dots & \Pi(a_{m-1}) & \Pi(a_m) \end{pmatrix}$$

Wir betrachten folgendes Beispiel:

$$\Pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 3 & 7 & 2 & 9 & 1 & 4 & 6 \end{pmatrix}$$

Π ist eindeutig bestimmt durch die Folge seiner Werte: 853729146

Wir betrachten die folgenden Zyklen:

$$\left. \begin{array}{l} 1 \rightarrow 8 \rightarrow 4 \rightarrow 7 \rightarrow 1 : 4 \\ 2 \rightarrow 5 \rightarrow 2 : 2 \\ 3 \rightarrow 3 : 1 \\ 6 \rightarrow 9 \rightarrow 6 : 2 \end{array} \right\} \text{Länge der Zyklen}$$

Summe der Längen ergibt: $4 + 2 + 1 + 2 = \underline{9}$

Die Elemente von M bilden aufgrund von Π Klassen von Zyklen $(1,8,4,7)$, $(2,5)$, (3) , $(6,9)$. Dabei gilt:

- Die Reihenfolge der Zyklen spielt dabei keine Rolle.
- Innerhalb eines Zyklus kann jedes Element das erste sein; die Reihenfolge der übrigen steht dann fest. D.h. die Zykeldarstellung (3) , $(5,2)$, $(9,6)$, $(8,4,7,1)$ beschreibt dieselbe Bijektion Π .

Definition

$s_{m,n}$ (für $0 < n \leq m$) bezeichnet die Anzahl der Zerlegung einer m -Permutation Π in n Zyklen und heißt **Stirling-Zahl erster Art**.

spezielle Werte:

$$\rightarrow s_{m,0} := 0 \text{ für } m > 0$$

$$\rightarrow s_{0,0} := 1$$

$$\rightarrow s_{m,n} := 0 \text{ für } n > m$$

$$\rightarrow s_{m,m} := 1 \} m \text{ Zyklen der Länge } 1, \text{ d.h. } m \text{ Fixpunkte, d.h. identische Abbildung}$$

$$\rightarrow s_{m,m-1} := \binom{m}{2} \} \text{ hierfür ein } 2\text{-er-Zyklus und der Rest } (m-2) \text{ } 1\text{-er-Zyklen (Fixpunkte);}$$
$$\rightarrow s_{m,m-1} := \binom{m}{2} \} \text{ so viele } 2\text{-er-Zyklen, wie } 2\text{-er Mengen}$$

$$\rightarrow s_{m,1} = (m-1)! \} \text{ jedes Element kann vorn stehen, die verbleibenden } (m-1) \text{ Elemente}$$
$$\rightarrow s_{m,1} = (m-1)! \} \text{ sind bzw. können irgendwie angeordnet sein}$$

Frage: Finden wir auch für die Stirling-Zahl erster Art eine Rekursion?

Gegeben sei eine m -Menge M . Wir fixieren ein Element a aus M .

Wir klassifizieren die m -Permutationen mit n Zyklen danach, ob entweder

- (i) a einen Einer-Zyklus bildet oder
- (ii) in einem längeren Zyklus enthalten ist!

zu i) Die verbleibenden $(m-1)$ Elemente sind auf $(n-1)$ Zyklen zu verteilen. Hierfür gibt es $s_{m-1, n-1}$ Möglichkeiten.

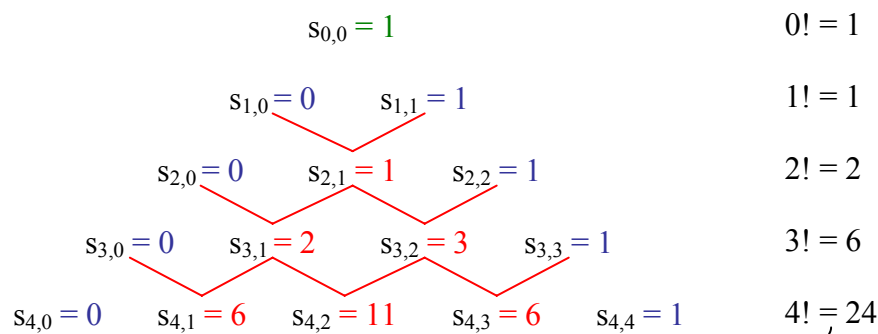
zu ii) Zunächst sind $(m-1)$ Elemente auf n Zyklen zu verteilen. Hierfür gibt es $s_{m-1, n}$ Möglichkeiten. Anschließend gibt es $(m-1)$ Möglichkeiten a in einen bestehenden Zyklus vor eines der $(m-1)$ Elemente zu schreiben. Daraus folgt nach der Produktregel: $(m-1) \cdot s_{m-1, n}$ Möglichkeiten.

Insgesamt erhalten wir folgenden rekursiven Satz:

Satz: (Rekursion der Stirling-Zahlen erster Art)

$$s_{m,n} = s_{m-1, n-1} + (m-1) \cdot s_{m-1, n}$$

Diese Rekursion liefert die Anordnung und Berechnung der Werte im Stirling-Dreieck erster Art:



Fakt: $\sum_{k=0}^m s_{m,k} = m!$ } entspricht der Zeilensumme

§11. Das DIRICHLETsche Schubfachmodell

Formulierung im Schubfachmodell

1. Verteilt man $n = r + 1$ Gegenstände auf r Schubfächer, dann gibt es ein Schubfach das (mindestens) zwei Gegenstände enthält.
2. Verteilt man $n = k \cdot r + 1$ Gegenstände auf r Schubfächer, dann gibt es ein Schubfach das (mindestens) $(k + 1)$ Gegenstände enthält.
3. Verteilt man n Gegenstände auf r Schubfächer, dann gibt es ein Schubfach das (mindestens) $\left(\left\lfloor \frac{n-1}{r} \right\rfloor + 1\right)$ Gegenstände enthält.
4. Verteilt man $n = e_1 + e_2 + \dots + e_r - r + 1$ Gegenstände auf r Schubfächer, dann gibt es ein Schubfach, das (mindestens) e_1 Gegenstände oder e_2 Gegenstände oder ... oder e_r Gegenstände enthält (mindestens in einem sind also $e_i : 1 \leq i \leq r$ Gegenstände).

Beweis von (4):

Annahme: Es gibt eine Verteilung dieser n Gegenstände, so dass für alle Schubfächer gilt:
Anzahl der Gegenstände $< e_i, 1 \leq i \leq r$

d.h. Anzahl der Gegenstände $\leq e_i - 1, 1 \leq i \leq r$

d.h. für die Summe der Anzahlen:

$$\begin{aligned} \sum \text{Anzahl der Gegenstände} &\leq (e_1 - 1) + (e_2 - 1) + \dots + (e_r - 1) \\ &= (e_1 + e_2 + \dots + e_r) - r < e_1 + e_2 + \dots + e_r - r + 1 = n \end{aligned}$$

Formulierung in der Sprache der Abbildungen

Es sei $f: N \mapsto R$, dabei ist N eine n -Menge und R einer r -Menge.

1. Falls $n > r$ ($n \geq r + 1$) dann gibt es ein $b \in R$ mit $\text{card}(f^{-1}(b)) \geq 2$.
2. Falls $n \geq k \cdot r + 1$, dann gibt es ein $b \in R$ mit $\text{card}(f^{-1}(b)) \geq k + 1$.
3. Falls $n \geq r$, dann gibt es ein $b \in R$ mit $\text{card}(f^{-1}(b)) \geq \left(\left\lfloor \frac{n-1}{r} \right\rfloor + 1\right)$.
4. Falls $n \geq e_1 + e_2 + \dots + e_r - r + 1$, dann gibt es ein $b \in R$ mit $\text{card}(f^{-1}(b)) \geq e_i$ mit $1 \leq i \leq r$.

Anwendungen

1. In einem Hörsaal befinden sich mehr als 366 Studenten. Dann gibt es zwei Studenten, die am selben Tag Geburtstag haben. D.h. die Wahrscheinlichkeit dafür, dass zwei am selben Tag Geburtstag haben ist 1.

Frage:

Wie viele Studenten müssen im Hörsaal sein, damit die Wahrscheinlichkeit dafür, dass 2 am selben Tag Geburtstag haben $\geq \frac{1}{2}$ ist?

Antwort: 24

2. Bekannt ist, kein Mensch hat mehr als 100.000 Haare auf dem Kopf. Da Berlin mehr als 3,2 Millionen EW hat, gibt es 33 Berliner mit derselben Haaranzahl!

Bemerkung:

Beweise mit Schubfachprinzip sind typische Existenzbeweise /-aussagen!

3. Eine Urne enthält 5 gelbe, 6 rote und 7 blaue Kugeln!
Bestimmen sie die kleinste Anzahl von Kugeln, die zu Ziehen sind um mit Sicherheit 3 rote oder 4 gelbe oder 5 blaue Kugeln gezogen zu haben!

Ansatz 1: (zur Begründung benutze Fassung (4))

$r = 3 \rightarrow$ verschiedene Sorten

$e_1 = 3, e_2 = 4, e_3 = 5$ liefert: $n = 3 + 4 + 5 - 3 + 1 = 10$

Die gesuchte Anzahl ist 10.

Ansatz 2: (inhaltliche Argumentation)

Sei x die Anzahl der gezogenen roten Kugeln.

Sei y die Anzahl der gezogenen gelben Kugeln.

Sei z die Anzahl der gezogenen blauen Kugeln.

Das Erfolgserlebnis tritt **nicht** ein, falls $x < 3$ und $y < 4$ und $z < 5$; d.h. falls $x \leq 2$ und $y \leq 3$ und $z \leq 4$; d.h. falls $x + y + z = 9$ ist. Das Erfolgserlebnis tritt nicht ein, falls höchstens 9 Kugeln gezogen wurden und damit mindestens 10.

4. Gegeben sei $S \subseteq \{1, 2, 3, \dots, 14\}$ mit der Eigenschaft $\text{card}(S) = 6$.

(Es gibt $\binom{14}{6}$ solcher Mengen!)

Behauptung:

Die Summe der Elemente aller nichtleeren Teilmengen von S sind nicht alle verschieden!

Wir denken uns ein S mit $\text{card}(S) = 6$ fixiert! Wir wissen S hat $2^6 - 1 = 63$ verschiedene nichtleere Teilmengen! Für eine solche Teilmenge $A \subseteq S$ bezeichne S_A die Summe der Elemente von A . Dann gilt: $1 \leq S_A \leq 9 + 10 + 11 + 12 + 13 + 14$ also $1 \leq S_A \leq 69$.

Für das Schubfachprinzip bedeutet dies:

63 Gegenstände (= Teilmengen) sind auf 69 Schubfächer zu verteilen.

Frage: Was können wir daraus schließen?? Bis jetzt nichts!

Wir betrachten weiter nichtleere und echte Teilmengen von A :

Es gibt $2^6 - 2 = 62$ solche Teilmengen ($A = S$ ausgeschlossen).

Für die Teilmengen dieser Teilungen gilt: $1 \leq S_A \leq 10 + 11 + 12 + 13 + 14 = 60$

Das bedeutet nach dem Schubfachprinzip:

62 Gegenstände sind auf 60 Schubfächer (Summen) zu verteilen. Also gibt es 2

Teilmengen $A \subseteq S$ und $B \subseteq S$ mit der Eigenschaft $S_A = S_B$. Somit sind nicht alle Teilmengen von S verschieden!

§12. Erzeugende Funktionen und Rekursionsschemata

Ausgangspunkt: die Gleichung $(1+x)^n = \sum_{r=0}^n \binom{n}{r} x^r$

Die Koeffizienten des Polynoms auf der rechten Seite sind gerade die Zählkoeffizienten des folgenden Abzählproblems: „**Bestimme die Anzahl der r-Kombinationen einer n-Menge.**“ Die Funktion $(1+x)^n$ auf der linken Seite heißt **erzeugende Funktion** dieses konkreten Abzählproblems.

Interpretation:

Wir fassen die Faktoren $(1+x)$ als **Schubfächer** auf und erhalten so n unterschiedliche Schubfächer, auf die r identische Gegenstände zu verteilen sind, wobei gilt: pro Schubfach höchstens ein Gegenstand. „höchstens ein Gegenstand“ bedeutet: entweder 0 Gegenstände oder 1 Gegenstand.

„0“ → interpretiere durch: „wähle aus $(1+x)$ beim ausmultiplizieren die $1 = x^0$ “

„1“ → interpretiere durch: „wähle aus $(1+x)$ beim ausmultiplizieren das x “

Eine r -Kombination ohne Wiederholung entspricht einer Auswahl von r Schubfächern (aus den n Schubfächern) aus denen „ x “ gewählt wurde.

Ansatz:

Wir betrachten neue Abzählprobleme: z.B. „pro Schubfach sind höchstens zwei Gegenstände erlaubt“ ⇒ ein solches Schubfach wird identifiziert mit dem Term $1+x+x^2$ (Dabei steht x^2 für „zwei Gegenstände werden diesem Schubfach zugeordnet“).

Beispiel:

Schubfächer	erlaubte Anzahlen	Term
Fach 1	0,1,3	$1+x+x^2$
Fach 2	1,2	$x+x^2$
Fach 3	1	x
Fach 4	0,4	$1+x^4$

Frage:

Wie viele Möglichkeiten gibt es z.B. 9 Gegenstände auf diese Schubfächer zu verteilen?

Antwort: (durch formales Ausrechnen)

Die erzeugende Funktion für dieses Abzählproblem ist gegeben durch das Produkt: $(1+x+x^2)(x+x^2)x(1+x^4)$. Durch Ausmultiplizieren ergibt sich folgendes Polynom: $1x^2 + 2x^3 + 1x^4 + 1x^5 + 2x^6 + 2x^7 + 1x^8 + 1x^9 + 1x^{10}$.

Dieses Polynom sagt:

- es gibt 0 Möglichkeiten: 0,1,11 oder mehr Gegenstände zu verteilen
- es gibt 1 Möglichkeit: 2,4,5,8,9 oder 10 Gegenstände zu verteilen
- es gibt 2 Möglichkeiten: 3,6 oder 7 Gegenstände zu verteilen

Allgemein:

Gegeben sei ein Abzählproblem bei dem identische Gegenstände auf n unterscheidbare Schubfächer zu verteilen sind.

Dabei seien $0 \leq v_{i_1} < v_{i_2} < \dots < v_{i_{j_i}}$ für $0 \leq i \leq n$, die erlaubten Anzahlen (Vielfachheiten) für dieses Schubfach i .

Ein solches Schubfach identifizieren wir mit dem Term $x^{v_{i_1}} + x^{v_{i_2}} + \dots + x^{v_{i_{j_i}}}$.

Das Produkt $\prod_{i=1}^n (x^{v_{i_1}} + x^{v_{i_2}} + \dots + x^{v_{i_{j_i}}})$ heißt erzeugende Funktion für dieses konkrete Abzählproblem.

Satz:

Die Koeffizienten des ausmultiplizierten Polynoms sind gerade die Zählkoeffizienten für dieses Abzählproblem.

Neue Frage:

★ { Welche Übersetzung existiert für das Abzählproblem „Bestimme die Anzahl der r -Kombinationen mit Wiederholung einer n -Menge.“?

Die erlaubten Vielfachheiten sind hier also $0, 1, 2, 3, \dots$ (je Schubfach)

Ansatz:

Wir identifizieren ein solches Fach mit dem „Term“ $1 + x + x^2 + x^3 + \dots$

Dies ist kein Term im eigentlichen Sinn, sondern eine formale Potenzreihe $\sum_{k=0}^{\infty} x^k$.

Die Analysis sagt uns für $|x| < 1$ konvergiert diese Reihe und es gilt: $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$

Wir untersuchen hier nicht das Konvergenzverhalten, sondern definieren wir formal für das Abzählproblem (★) die erzeugende Funktion $\left(\frac{1}{1-x}\right)^n$.

Satz: (aus Analysis) $\left(\frac{1}{1-x}\right)^n = \sum_{r=0}^{\infty} \binom{n+r-1}{r} \cdot x^r$

D.h. wird die erzeugende Funktion in eine Potenzreihe entwickelt, dann sind die Koeffizienten in dieser Potenzreihe gerade die Zählkoeffizienten des Abzählproblems (★).

Allgemein:

Wir betrachten jetzt Abzählprobleme für n Schubfächer, wobei für jedes Fach eine **unendliche Folge** von Vielfachheiten erlaubt ist.

z.B. auch Folgen der Form $(v_{i_1}, v_{i_2}, \dots, v_{i_{j_i}}, 0, 0, \dots)$

Beispiel:

Wie üblich haben wir n Fächer,

(★★) { wobei hier: jedes Fach soll mindestens ein Gegenstand erhalten.

Ansatz:

Wir identifizieren hier jedes Fach mit der Potenzreihe $x + x^2 + x^3 + \dots$

$$= \sum_{k=1}^{\infty} x^k = \sum_{k=1}^{\infty} x x^{k-1} = \sum_{k'=0}^{\infty} x x^{k'} = x \cdot \sum_{k'=0}^{\infty} x^{k'} = x \cdot \left(\frac{1}{1-x}\right) = \frac{x}{1-x} \quad (\text{pro Fach})$$

Damit ergibt sich folgende erzeugende Funktion für unser (★★)

$$\begin{aligned} \left(\frac{x}{1-x}\right)^n &= x^n \left(\frac{1}{1-x}\right)^n = x^n \cdot \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^r = \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^n x^r \\ &= \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^{n+r} = \sum_{k=n}^{\infty} \binom{k-1}{k-n} x^k = \sum_{k=n}^{\infty} \binom{k-1}{n-1} x^k \end{aligned}$$

Index: $k:=n+r \Rightarrow r=k-n$ $(k-1)-(k-n)=k-1-k+n$

Die so gewonnenen Koeffizienten sind die Zählkoeffizienten, des Abzählproblems (★★).

$$= 0 \cdot x^0 + \dots + 0 \cdot x^{n-1} + \binom{n-1}{n-1} x^n + \binom{n}{n-1} x^{n+1} + \dots$$

Diese entsprechen genau der Anzahl der n-Partitionen der natürlichen Zahlen k

Nachbemerkung:

$$(1+x)^n = \sum_{r=0}^n \binom{n}{r} x^r$$

andere Lesart:

$$(1+x)^n = \sum_{r=0}^n \frac{n!}{(n-r)!r!} x^r = \sum_{r=0}^n \frac{n!}{(n-r)!} \cdot \frac{x^r}{r!} = \sum_{r=0}^n \underbrace{P(n,r)}_{\text{fallende Faktorielle}} \cdot \frac{x^r}{r!}$$

exponentielle erzeugende Funktion

Rekurrenzen, Rekursionsschemata, Rekursionen

Beispiel: FIBONACCI-Zahlen

definierende Rekursion:

$$\begin{array}{l} u_0 := 0 \\ u_1 := 1 \\ \vdots \\ u_n := u_{n-1} + u_{n-2} \end{array} \quad (a)$$

Dieses Schemata definiert für jeden Index n den u_n : kleine Wertetabelle:

n	0	1	2	3	4	5	6	7	...
u_n	0	1	1	2	3	5	8	13	

Dies ist ein Beispiel für eine **homogene lineare** Rekurrenzgleichung mit **konstanten Koeffizienten**:

$$u_n := 1 \cdot u_{n-1}^1 + 1 \cdot u_{n-1}^1 + 0$$

Gesucht ist eine explizite Darstellung der Werte, unabhängig von den Vorgängerwerten: d.h. $u_n = u(n)$. Dies wird durch folgendes Verfahren erreicht:

1. Schritt:

Drücke das gegebene Schema (a) durch eine einzige Gleichung aus!

Setzen: $u_n = 0$ für $n < 0$:

damit gilt:

$$n = 0 : u_n = u_{n-1} + u_{n-2}$$

$$n = 1 : u_n = u_{n-1} + u_{n-2} + 1$$

$$n > 1 : u_n = u_{n-1} + u_{n-2} + 0$$

Damit gilt: für $n > 0$ $u_n = u_{n-1} + u_{n-2} + \text{J-Wert}(n=1)$ (b)

2. Schritt:

Benutze formale Potenzreihen um eine erzeugende Funktion für (b) zu bestimmen!

$$\text{Ansatz: } g(x) := \sum_{n=0}^{\infty} u_n \cdot x^n$$

Wir setzen in diesen Ansatz Gleichung (b) ein:

$$\begin{aligned} g(x) &:= \sum_{n=0}^{\infty} [u_{n-1} + u_{n-2} + \text{J-Wert}(n=1)] \cdot x^n \\ &= \sum_{n=0}^{\infty} u_{n-1} \cdot x^n + \sum_{n=0}^{\infty} u_{n-2} \cdot x^n + \sum_{n=0}^{\infty} \text{J-Wert}(n=1) \cdot x^n \\ &= x \cdot \sum_{n=1}^{\infty} u_{n-1} \cdot x^{n-1} + x^2 \cdot \sum_{n=2}^{\infty} u_{n-2} \cdot x^{n-2} + x \\ &= x \cdot \sum_{n=0}^{\infty} u_n \cdot x^n + x^2 \cdot \sum_{n=0}^{\infty} u_n \cdot x^n + x \end{aligned}$$

$$\text{d.h. } g(x) = x \cdot g(x) + x^2 \cdot g(x) + x$$

$$\text{und damit: } g(x) = \frac{-x}{x^2 + x - 1} \quad (c)$$

Dies ist die erzeugende Funktion für (b).

3. Schritt:

Entwickle die rechte Seite von (c) in eine formale Potenzreihe, deren Koeffizienten sind dann gerade die gesuchten Zählkoeffizienten u_n . Dies geschieht durch folgenden Ansatz:

Ansatz: Wir betrachten g als gebrochene rationale Funktion:

$$g(x) = \frac{\text{Zählerpolynom}}{\text{Nennerpolynom}} = \frac{p(x)}{q(x)}$$

Bei uns: $p(x) = -x$, $q(x) = x^2 + x - 1$

3.1. Bestimme die Nullstellen des Nennerpolynoms $q(x)$.

$$0 = x^2 + x - 1$$

$$\Rightarrow x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q} = -\frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = -\frac{1}{2} \pm \frac{\sqrt{5}}{2}$$

$$\Rightarrow x_1 = -\frac{1+\sqrt{5}}{2}, x_2 = -\frac{1-\sqrt{5}}{2} \quad (d)$$

$$\text{haben: } \alpha = -\frac{1+\sqrt{5}}{2}, \beta = -\frac{1-\sqrt{5}}{2}$$

$$\text{einsetzen: } q(x) = (x - \alpha)(x - \beta) = \left(x + \frac{1+\sqrt{5}}{2}\right)\left(x + \frac{1-\sqrt{5}}{2}\right) \quad (e)$$

3.2. Realisiere für die gebrochene rationale Funktion $g = \frac{p}{q}$ ein Partialbruchzerlegung:

$$g(x) = \frac{p(x)}{q(x)} = \frac{p(x)}{(x-\alpha)(x-\beta)}$$

$$g(x) = \frac{A}{x-\alpha} + \frac{B}{x-\beta} \quad (f)$$

3.3. Bestimme die Koeffizienten A und B und

3.4. Bestimme die gesuchten Zählkoeffizienten u_n durch Einsatzen der Werte aus (f) in den Ansatz 1 (Schritt 2).

$$\text{Es gilt: } g(x) = \frac{A}{x-\alpha} + \frac{B}{x-\beta}$$

Erweitern den ersten Bruch mit $-\frac{1}{\alpha}$ und den zweiten Bruch mit $-\frac{1}{\beta}$. Dies liefert:

$$g(x) = \frac{\left(-\frac{1}{\alpha}\right)A}{\left(-\frac{1}{\alpha}\right)(x-\alpha)} + \frac{\left(-\frac{1}{\beta}\right)B}{\left(-\frac{1}{\beta}\right)(x-\beta)} = \left(-\frac{A}{\alpha}\right) \cdot \frac{1}{1-\frac{1}{\alpha}x} + \left(-\frac{B}{\beta}\right) \cdot \frac{1}{1-\frac{1}{\beta}x}$$

$$= \left(-\frac{A}{\alpha}\right) \cdot \sum_{n=0}^{\infty} x^n \cdot \left(\frac{1}{\alpha}\right)^n + \left(-\frac{B}{\beta}\right) \cdot \sum_{n=0}^{\infty} x^n \cdot \left(\frac{1}{\beta}\right)^n$$

$$= \sum_{n=0}^{\infty} -\frac{A}{\alpha^{n+1}} \cdot x^n + \sum_{n=0}^{\infty} -\frac{B}{\beta^{n+1}} \cdot x^n$$

$$g(x) = \sum_{n=0}^{\infty} \left(-\frac{A}{\alpha^{n+1}} - \frac{B}{\beta^{n+1}} \right) \cdot x^n$$

Damit erhalten wir durch Koeffizientenvergleich:

$$u_n = -\frac{A}{\alpha^{n+1}} - \frac{B}{\beta^{n+1}} \quad (g)$$

Dies ist die gewünschte Darstellung $u_n = u(n)$.

Für unser Beispiel:

Starten mit (e):

$$\begin{aligned} g(x) &= \frac{p(x)}{\left(x + \frac{1+\sqrt{5}}{2}\right)\left(x + \frac{1-\sqrt{5}}{2}\right)} = \frac{A}{\left(x + \frac{1-\sqrt{5}}{2}\right)} + \frac{B}{\left(x + \frac{1+\sqrt{5}}{2}\right)} \\ &= \frac{A\left(x + \frac{1+\sqrt{5}}{2}\right) + B\left(x + \frac{1-\sqrt{5}}{2}\right)}{\left(x + \frac{1+\sqrt{5}}{2}\right)\left(x + \frac{1-\sqrt{5}}{2}\right)} = \frac{(A+B)x + A \cdot \frac{1+\sqrt{5}}{2} + B \cdot \frac{1-\sqrt{5}}{2}}{\left(x + \frac{1+\sqrt{5}}{2}\right)\left(x + \frac{1-\sqrt{5}}{2}\right)} \end{aligned}$$

Koeffizientenvergleich liefert:

$$(A+B)x = -x \Rightarrow A+B = -1 \quad : I$$

sowie:

$$A \cdot \frac{1+\sqrt{5}}{2} + B \cdot \frac{1-\sqrt{5}}{2} = 0 \quad : II$$

$I' : A = -1 - B$ in II liefert:

$$0 = (-1 - B) \cdot \frac{1 + \sqrt{5}}{2} + B \cdot \frac{1 - \sqrt{5}}{2} = -\frac{1 + \sqrt{5}}{2} - B \cdot \frac{1 + \sqrt{5}}{2} + B \cdot \frac{1 - \sqrt{5}}{2}$$

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

$$\frac{1 + \sqrt{5}}{2} = -\sqrt{5} \cdot B$$

$$\Rightarrow B = -\frac{1}{\sqrt{5}} \cdot \frac{1 + \sqrt{5}}{2} \quad \text{und} \quad A = \frac{1}{\sqrt{5}} \cdot \frac{1 - \sqrt{5}}{2}$$

um (g) darzustellen:

$$\alpha = -\frac{1 - \sqrt{5}}{2}, \text{ also } \frac{1}{\alpha} = -\frac{2}{1 - \sqrt{5}} = -\frac{2(1 + \sqrt{5})}{-4} = \frac{1 + \sqrt{5}}{2} = -\beta$$

und

$$\beta = -\frac{1 + \sqrt{5}}{2}, \text{ also } \frac{1}{\beta} = -\frac{2}{1 + \sqrt{5}} = -\frac{2(1 - \sqrt{5})}{-4} = \frac{1 - \sqrt{5}}{2} = -\alpha$$

einsetzen in (g):

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

Daraus folgt das **gesuchte Ergebnis**:
$$u_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right]$$

3. Kapitel: Einstieg in die Zahlentheorie

§13. Natürliche Zahlen

Beschreibung durch Mengen:

$$\left. \begin{array}{l} 0 := \emptyset \\ n+1 := n \cup \{n\} \end{array} \right\} \text{Rekursionsschema für Mengen}$$

somit gilt:

$$0 = \emptyset$$

$$1 = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$$

$$2 = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$$

Allgemein liefert dieser Ansatz $n = \{0, 1, 2, 3, \dots, n-1\}$.

Damit ist jede natürliche Zahl eine spezielle Menge, die gerade n Elemente enthält.

Logische Beschreibung:

\mathbb{N} ... für die Menge aller natürlichen Zahlen

0 ... Null (dies ist die Bezeichnung für eine Konstante)

$n+1$... für die Bezeichnung des Nachfolgers (dies ist eine einstellige Funktion)

PEANO-Axiome

$$(P1) \bigwedge_n (n+1 \neq 0)$$

Null ist kein Nachfolger einer natürlichen Zahl.

$$(P2) \bigwedge_n \bigwedge_m (n+1 = m+1 \rightarrow n = m)$$

Also die Nachfolgerfunktion ist injektiv.

$$(P3) \bigwedge_{A \subseteq \mathbb{N}} (0 \in A \wedge \bigwedge_n (n \in A \rightarrow n+1 \in A) \rightarrow A = \mathbb{N})$$

Induktionsaxiom

Wir definieren die **Relation \leq für \mathbb{N}** :

$$n \leq m \leftrightarrow_{\text{df}} \underbrace{n = m \vee n \in m}_{\text{Quasielementbeziehung}}$$

Eigenschaften dieser Relation:

1. $n \leq n$
2. $n \leq m \wedge m \leq k \Rightarrow n \leq k$
3. $n \leq m \wedge m \leq n \Rightarrow n = m$
4. $n \leq m \vee m \leq n$
5. Jede nichtleere Teilmenge $A \subseteq \mathbb{N}$ besitzt ein Minimum.

- i. Eigenschaften 1.-3. beschreiben die Menge der natürlichen Zahlen $[\mathbb{N}, \leq]$ als halbgeordnete Menge.
- ii. Eigenschaften 1.-4. beschreiben $[\mathbb{N}, \leq]$ als Ordnung.
- iii. Eigenschaften 1.-3. und 5. beschreiben $[\mathbb{N}, \leq]$ als eine wohlgeordnete Menge (Wohlordnung).

Rechenoperationen

Addition:

rekursiv: $m + 0 := m$
 $m + (n + 1) := (m + n) + 1$

Multiplikation:

rekursiv: $m \cdot 0 := 0$
 $m(n + 1) := (m \cdot n) + m$

Diese Schemata definieren Addition und Multiplikation als zweistellige Operationen für **alle Paare** natürlicher Zahlen.

Insbesondere folgt: $n \leq m \leftrightarrow \bigvee_{k \in \mathbb{N}} (n + k = m)$

Wir definieren eine neue Relation als

multiplikatives Analogon: $n \setminus m \leftrightarrow_{\text{df}} \bigvee_{k \in \mathbb{N}} (n \cdot k = m)$

Eigenschaften dieser Relation:

\setminus ist eine Halbordnungsrelation und damit ist $[\mathbb{N}, \setminus]$ eine halbgeordnete Menge.

weitere Eigenschaften:

1. $1 \setminus n$: 1 ist das Minimum in dieser Struktur $[\mathbb{N}, \setminus]$.
2. $n \setminus 0$: 0 ist das Maximum in $[\mathbb{N}, \setminus]$.
3. $n \setminus x \wedge n \setminus y \Rightarrow n \setminus ax + by$
 n ist Teiler jeder Linearkombination
4. $n \setminus x \wedge m \setminus y \Rightarrow n \cdot m \setminus x \cdot y$
5. $m \setminus n \wedge n \neq 0 \Rightarrow m \leq n$

Eingeschränkte Differenz:

Falls $m \leq n$ existiert eine natürliche Zahl k mit $m + k = n$. In diesem Fall liefert k die **Differenz** zwischen m und n und wir schreiben: $m - n := k$

z.B. gilt: $(3') n \setminus x \wedge n \setminus y \wedge ax \geq by \Rightarrow n \setminus ax - by$

Frage: Was ist die „eingeschränkte Division“?

Lemma 1:

Für je zwei natürliche Zahlen m, n mit $m \leq n$ existieren eindeutig bestimmte Zahlen q und r mit $n = qm + r$ und $0 \leq r < m$.

Wir definieren: $n \text{ div } m := q$
 $n \text{ mod } m := r$

als zweistellige Operation:

Falls für $m \leq n$, $n \bmod m = r = 0$ ist, gilt: $n = qm$ und damit $m \mid n$. Dann heißt q der Quotient

zwischen n und m und wir schreiben: $\frac{n}{m} := q = n \operatorname{div} m$

falls $r \neq 0$: schreiben wir: $\left\lfloor \frac{n}{m} \right\rfloor := n \operatorname{div} m$

und nennen es den ganzen Teil des Quotienten $\frac{n}{m}$.

Beweis von Lemma 1: mit Hilfe des Wohlordnungsprinzips

1. Teil: Existenzbeweis für die Existenz der Zahlen q und r

Dazu definieren wir: $A =_{\text{df}} \{n - k \cdot m \mid k \in \mathbb{N} \wedge n - k \cdot m \geq 0\}$

Es gilt: $A \subseteq \mathbb{N}$, $A \neq \emptyset$, da $n \in A$

Das Wohlordnungsprinzip (Eigenschaft (5) von \leq) sagt, dass A ein Minimum besitzt!

Es sei das Minimum von A : $r := \min A$

Es gilt: $r \geq 0$

1. Fall: $r < m$

Dann gilt: $r = n - km$

und damit $n = km + r$, $0 \leq r < m$

2. Fall: $r \geq m$

Dann gilt: $r - m \geq 0$

und außerdem gilt: $r = n - km$

und damit: $r - m = n - km - m = n - (k + 1)m$

dies heißt $r - m \in A$ und klar ist $r - m < r$. **Widerspruch!!!**

Das ist ein Widerspruch zur Tatsache, dass $r = \min A$.

2. Teil: Eindeutigkeitsbeweis - Unität

Angenommen wir haben $m \leq n$

$n = q_1 m + r_1$, $0 \leq q_1 < m$ und

$n = q_2 m + r_2$, $0 \leq q_2 < m$

Hieraus folgt ($r_2 - r_1$ ist eine ganze Zahl).

1. Fall: $r_1 \leq r_2$ und 2. Fall: $r_2 \leq r_1$:

Falls Fall (1) eintritt, gilt: $0 \leq r_2 - r_1 < m$ (a)

Wir betrachten:

$n - m = 0 = q_2 m + r_2 - q_1 m - r_1 = (q_2 - q_1)m + (r_2 - r_1) \Rightarrow (q_2 - q_1)m = (r_2 - r_1)$

Da $m \nmid (q_2 - q_1)m$ gilt: $m \nmid r_2 - r_1$ (b)

Aus (a) und (b) folgt mit (5) $r_2 - r_1 = 0$. Also ist $r_1 = r_2$ und damit $q_1 m = q_2 m$ und damit auch $q_1 = q_2$.

m – adische Darstellung

Für $m \geq 2$ ist die m – adische Darstellung einer natürlichen Zahl n gegeben durch:

$n = (a_{k-1} a_{k-2} \dots a_2 a_1 a_0)_m$ wobei gilt:

$$\star \left\{ \begin{array}{l} n = (a_{k-1} m^{k-1} + a_{k-2} m^{k-2} + \dots + a_2 m^2 + a_1 m^1 + a_0 \\ \text{Dabei gilt: } a_{k-1}, \dots, a_1, a_0 \in \{0, 1, 2, \dots, m-1\} \text{ (Ziffern)} \\ \text{und } a_{k-1} \neq 0 \dots n \text{ hat } k\text{-stellige Darstellung} \end{array} \right.$$

Satz 1: Rechtfertigungssatz

Jede natürliche Zahl n besitzt für fixiertes $m \geq 2$ eine eindeutig bestimmte Darstellung der Form (\star) .

Beweis: mit Hilfe von Lemma 1!

Größter gemeinsamer Teiler / kleinstes gemeinsames Vielfaches

Wir wissen für alle $n, m \in \mathbb{N}$ gilt: $1 \mid n \wedge 1 \mid m$

Falls: $d \mid n \wedge d \mid m$ heißt d gemeinsamer Teiler von n und m .

Lemma 2:

Für beliebige natürliche Zahlen a, b gilt: Falls $d \mid n \wedge d \mid m$, dann ist auch $d \mid an + bm$ (d.h. falls d also gemeinsamer Teiler ist, so ist d auch Teiler der Linearkombination).

Definition

g heißt größter gemeinsamer Teiler (ggT) von n und $m \leftrightarrow_{df}$

1. $g \mid n$ und $g \mid m$
2. für alle c gilt: $c \mid n$ und $c \mid m \Rightarrow c \mid g$

Schreibweise: $g := \text{ggT}(n, m)$ und es gilt: $g = \sup\{n, m\}$

Bemerkung:

- a. (1.) bedeutet in $[\mathbb{N}, \mid]$: g ist untere Schranke von $\{n, m\}$
(2.) bedeutet in $[\mathbb{N}, \mid]$: g ist größte untere Schranke von $\{n, m\}$
- b. da aus $c \mid g$ und $g \neq 0$ folgt $c \leq g$ gilt: g ist größter gemeinsamer Teiler bezüglich \leq !
- c. stets gilt $1 \mid n$ und $1 \mid m$

Lemma 2:

Falls $c \mid n$ und $c \mid m$ dann ist c auch Teiler jeder Linearkombination, d.h. $c \mid an + bm$ für alle $a, b \in \mathbb{N}$.

Beweis:

$c \mid n$, d.h. $\bigvee_{k \in \mathbb{N}} (ck = n)$

$c \mid m$, d.h. $\bigvee_{l \in \mathbb{N}} (cl = m)$

und damit gilt: $an + bm = ack + bcl = (ak + bl)c \Rightarrow c \mid ak + bl$.

Satz 2:

Für jede natürliche Zahl n und m existiert $\text{ggT}(n, m)$ und ist eindeutig bestimmt. Dabei bezeichnet $\text{ggT}(n, m)$ den größten gemeinsamen Teiler.

Beweis: mit Hilfe des Wohlordnungsprinzips)

speziell gilt: $\text{ggT}(0, 0) = 0$; $\text{ggT}(n, 0) = n$ und $\text{ggT}(0, m) = m$

Wir betrachten im Folgenden: O.B.d.A sei $n \geq m > 0$

Wir definieren:

$$D =_{\text{df}} \{an - bm \mid a, b \in \mathbb{N}_0 \text{ mit } an \geq bm\} \cup \{am - bn \mid a, b \in \mathbb{N}_0 \text{ mit } am \geq bn\}$$

Es gilt:

$$(I) \quad 0 \in D, n \in D, m \in D$$

$$(II) \quad c \setminus n \text{ und } c \setminus m \Rightarrow c \setminus d \text{ für alle } d \in D \text{ (wegen Lemma 2)}$$

Dann gilt: $D \setminus \{0\} \neq \emptyset$

Also existiert ein Minimum bezüglich \leq in $D \setminus \{0\}$ (und ist eindeutig bestimmt).

Es sei $g := \min_{\leq}(D \setminus \{0\})$.

Behauptung: $g = \text{ggT}(n, m)$

Dazu zeigen wir:

1. $g \setminus n$ und $g \setminus m$ und

$$2. \bigwedge_c (c \setminus n \wedge c \setminus m \Rightarrow c \setminus g)$$

Dies ist aufgrund von (II) sofort klar, da $g \in D$

Da $g \in D$ gilt:

a) $g = an - bm$ oder

b) $g = am - bn$

Nach Lemma 1 existiert q und r mit $n = gq + r$ und $0 \leq r < g$, denn es gilt $g \leq n$, $n \in D$ und $n \neq 0$ und $g = \min_{\leq}(D \setminus \{0\})$.

Es sei a) $g = an - bm$.

Damit gilt: $r = n - gq = n - q(an - bm) = (qb)m - (qa - 1)n \geq 0$

Also gilt $r \in D$ gemäß b). Da $r \in D$ und $r < g$ und $g = \min_{\leq}(D \setminus \{0\})$ folgt: $r = 0$

Also gilt: $n = gq \Rightarrow g \setminus n$.

Falls b) $g = am - bn$ gilt, folgt: $r = n - gq = n - q(am - bn) = (qb + 1)n - (qa)m$

Damit gilt: $r \in D$ gemäß a).

Auch hier folgt $r = 0$ und $g \setminus n$.

Da auch $g \leq m$ folgt nach Lemma 1: $m = q'g + r'$ und analog: $g \setminus m$.

Folgerung aus diesem Beweis:

Der $\text{ggT}(n, m)$ lässt sich als **Linearkombination** von n und m schreiben:

Also entweder: $g = an - bm$ oder $g = am - bn$.

Bemerkung:

Es gibt also ganze Zahlen A und B mit der Eigenschaft $\text{ggT}(n, m) = An + Bm$ mit $\text{sgn}(A) \neq \text{sgn}(B)$.

Lemma 3:

Es sei g' ein gemeinsamer Teiler von n und m (Eigenschaft 1 nach Definition) und g' lässt sich schreiben als Linearkombination a) $g' = an - bm$ oder b) $g' = am - bn$.

Dann ist g' der ggT .

Beweis:

$g' \in D$, da $g = \min_{\leq}(D \setminus \{0\})$ und $g' \neq 0$ folgt $g \leq g'$.

umgekehrt gilt: (Eigenschaft 2) $g' \setminus g$ (da $g' \mid gT$) und $g \neq 0$ ergibt $g' \leq g$.

Also gilt: $g' = g$.

Ziel: Darstellung des ggT als Linearkombination

Hierfür zunächst:

Euklidischer Algorithmus

(Dies ist ein weiterer Beweis von Satz 2 – mit Hilfe von Lemma 1)

O.B.d.A. sei $n \geq m > 0$. Dann liefert die fortgesetzte Anwendung von Lemma 1:

$$\star \left\{ \begin{array}{l} n = q_0 m + r_0 \quad (0 \leq r_0 < m) \\ m = q_1 m + r_1 \quad (0 \leq r_1 < r_0) \\ r_0 = q_2 r_1 + r_2 \quad (0 \leq r_2 < r_1) \\ \vdots \\ r_{k-2} = q_k r_{k-1} + r_k \quad (0 \leq r_k < r_{k-1}) \\ r_{k-1} = q_{k+1} r_k + r_{k+1} \quad (r_{k+1} = 0) \end{array} \right.$$

Es gilt: $m > r_0 > r_1 > r_2 > \dots$ ist streng monoton fallend, also gibt es eine Stelle $(k+1)$ mit $r_{k+1} = 0$!

Weiter gilt: $r_k = \text{ggT}(n, m)$

Lemma 4: Es seien $n \geq m > 0$ und $n = qm + r$ mit $0 \leq r < m$. Dann gilt: $\text{ggT}(n, m) = \text{ggT}(m, r)$

Beweis:

zu Zeigen: $\{n, m\}$ und $\{m, r\}$ haben dieselben gemeinsamen Teiler.

a) Es sei d ein gemeinsamer Teiler von $\{m, n\}$, d.h. $d \mid n$ und $d \mid m$

Dann gilt: $r = n - qm$ ist eine Linearkombination, folgt nach Lemma 2: $d \mid r$

b) Es sei c ein gemeinsamer Teiler von $\{m, r\}$; da $n = qm + r$ eine Linearkombination ist, folgt analog: $c \mid n$

Mit Lemma 4 folgt:

$$\text{ggT}(n, m) = \text{ggT}(m, r_0) = \text{ggT}(r_0, r_1) = \text{ggT}(r_1, r_2) = \dots = \text{ggT}(r_{k-1}, r_k) = \text{ggT}(r_k, 0) = r_k$$

Satz 3:

Es gilt: $\text{ggT}(n, m) = g = A_{k+2}n + B_{k+2}m$ für ganze Zahlen A_{k+2}, B_{k+2} mit $\text{sgn}(A_{k+2}) \neq \text{sgn}(B_{k+2})$

Dabei gilt:

$$\star \left\{ \begin{array}{l} \text{IA) } A_0 = 1 \text{ und } B_0 = 0 \text{ und } A_1 = 0 \text{ und } B_1 = 1 \\ \text{IS) } A_i := A_{i-2} - q_{i-2}A_{i-1} \text{ und } B_i := B_{i-2} - q_{i-2}B_{i-1} \\ \text{Dabei sei } q_0, \dots, q_k \text{ gemäß } (\star) \text{ definiert!} \end{array} \right.$$

Dies ist ein Rekursionsschema zur Bestimmung der Koeffizienten der Linearkombination des größten gemeinsamen Teilers.

Illustration dieser Rekursionsgleichungen:

Es gilt: $n = 1 \cdot n + 0 \cdot m = A_0 n + B_0 m$

weiter: $m = 0 \cdot n + 1 \cdot m = A_1 n + B_1 m$

weiter: $r_0 = n - q_0 m = A_2 n + B_2 m$

und: $A_2 = A_0 - q_0 A_1 = 1 - q_0 \cdot 0 = 1$

$$B_2 = B_0 - q_0 B_1 = 0 - q_0 \cdot 1 = -q_0$$

weiter: $r_1 = m - q_1 r_0 = m - q_1(n - q_0 m) = (-q_0)n + (q_0 + 1)m = A_3 n + B_3 m$

und: $A_3 = A_1 - q_1 A_2 = 0 - q_1 \cdot 1 = (-q_1)$

$$B_3 = q_0 + 1$$