Diskrete Mathematik und Logik 2

Jörg Vogel

SS 2005

Vorwort

Dieses Skript ist im Rahmen des Projekts „Vorlesungsskripte der Fakultät für Mathematik und Informatik“ entstanden und wird im Rahmen dieses Projekts weiter betreut. Das Skript ist nach bestem Wissen und Gewissen entstanden. Denoch garantiert weder der auf der Titelseite genannte Dozent, noch die Mitglieder des Projekts für dessen Fehlerfreiheit. Für etwaige Fehler und dessen Folgen wird von keiner der genannten Personen eine Haftung übernommen. Es steht jeder Person frei, dieses Skript zu lesen, zu verändern oder auf anderen Medien verfügbar zu machen, solange ein Verweis die Internetadresse `http://uni-skripte.lug-jena.de/` *des Projekts enthalten ist.*

Diese Ausgabe trägt die Versionsnummer 2592 und ist vom 4. Dezember 2009. Eine (mögliche) aktuellere Ausgabe ist auf der Webseite des Projekts verfügbar.

Jeder ist dazu aufgerufen, Verbesserungen, Erweiterungen und Fehlerkorrekturen für das Skript einzureichen bzw. zu melden oder diese selbst einzupflegen – einfach eine E-Mail an die Mailingliste `<uni-skripte@lug-jena.de>` *senden. Weitere Informationen sind unter der oben genannten Internetadresse verfügbar.*

Hiermit möchten wir allen Personen, die an diesem Skript mitgewirkt haben, vielmals danken:

- *Matti Bickel* `<kabel@cat0.de>` *(2005)*
- *Jörg Sommer* `<joerg@alea.gnuu.de>` *(2006)*

Inhaltsverzeichnis

1 Aussagenlogik

1.1 Einführung

Prädikatenlogik: unser Schwerpunkt: Sprachen der Prädikatenlogik - als Beschreibungssprachen mathematischer Strukturen (jede Struktur hat ihre Sprache , die durch die Signatur bestimmt wird)

Aussagenlogik: unser Schwerpunkt:

- logische Regeln/ Verknüpfungen und die Regeln des Schlussfolgerns
- Test auf Erfüllbarkeit:

  Beispiel 1.1
  Verifikation von Schaltkreisen

  - Spezifikation S eines Schaltkreises
  - Realisierung R eines Schaltkreises

  S und R lassen sich beschreiben durch 0-1-wertige Funktionen (Boolsche Funktionen) f_s und f_r
  Frage: Stimmen die beiden Funktionen überein?
  Fakt: $f_s = f_r \Leftrightarrow f_s \oplus f_r = 0$
  Test: Ist $f_s \oplus f_r$ unerfüllbar?
  Antwort „ ja“: Realisierung R wie gewünscht.
  Antwort „nein“: Realisierung ändern.

1.2 Syntax und Semantik der Aussagenlogik

Zunächst nicht formal:
Eine Aussage ist ein sprachliches Gebilde, von dem es sinnvoll ist zu sagen, dass es entweder wahr oder falsch ist.

1.2.1 Prinzip der Zweiwertigkeit

Beispiel 1.2

Es gibt unendlich viele Primzahlen	wahr
Es gibt unendlich viele gerade Primzahlen	falsch
Es gibt unendlich viele Primzahlzwillinge	???
Diese Aussage ist falsch.	keine Aussage
Diese Aussage ist keine Aussage	falsch
„Ist dies eine Aussage“	keine Aussage

1.2.2 Schlüsse ziehen

Beispiel 1.3
Im Supermarkt stehen 136 Apfelsinenkisten, jede Kiste enthählt mindestens 140 Apfelsinen und höchstens 166 Apfelsinen.
Dann gibt es min. 6 Kisten mit der gleichen Anzahl Apfelsinen.
(*Schubkastenprinzip*: Existenzbeweis)
Dies ist ein Beispiel für einen korrekten Schluss.

Alle Senatoren sind alt.
Alle Achtziger sind Senatoren.
Also sind alle Achtziger alt.
Korrekter Schluss, obwohl die Prämissen falsch sind und die Konklusion wahr ist.

Einige Senatoren sind alt.
Einige Generäle sind Senatoren.
Einige Generäle sind alt.
Dieser Schluss ist *nicht* korrekt.

1.2.3 Aussagenverknüpfung

In der Aussagenlogik werden Aussageverbindungen durch logische Junktoren beschrieben.

Beispiel 1.4
„Erfurt ist die Hauptstadt Thüringens.“ *und* „$7 =< 3$“

1.2.4 Prinzip der Extensionalität

Der Wahrheitswert einer Aussageverbindung hängt allein von den Wahrheitswerten der (Teil-)Aussagen ab - und nicht von deren Inhalten.

1.2.5 Syntax der Prädikatenlogik

zweifache Reduktion

1. Aussagen werden ersetzt durch Platzhalter: Aussagevariablen;
   Bezeichnung: $A, B, C, D, \ldots$ (eventuell mit Indizes)
   Bemerkung:Feinstruktur der Aussagen geht verloren

2. Aussageverbindungen werden durch logische Junktoren ersetzt.

   Beispiel 1.5
   A und B, sowohl A als auch B, A aber auch $B \Rightarrow$ *Konjunktionen*
   A gdw. B, A dann und nur dann $B \Rightarrow$ *Bijunktionen*
   wenn A, dann B, A hat B zur Folge $\Rightarrow$ *Implikation*

   Bemerkung: Durch diese Reduktionen wird die logische Struktur von zusammengesetzten Aussagen (Formeln) betont.

Zeichenvorrat: Wir brauchen zwei Sorten von Zeichen:

- Aussagevariablen: A,B,C,D
- logische Junktoren: $\wedge, \vee, \rightarrow, \leftrightarrow, \neg$
- Hilfssymbole: (,)

Definition 1.1 (induktive Definition der Syntax der Aussagenlogik)
Induktionsanfang: Jede Aussagenvariable ist eine Aussagenlogische Formel

Induktionsschritt: Falls F und G bereits aussagenlogische Formeln sind, dann sind auch

- $(F \wedge G)$ Konjunktion
- $(F \vee G)$ Disjunktion
- $(F \rightarrow G)$ Implikation
- $(F \leftrightarrow G)$ Bijektion
- $(\neg F)$ Negation

aussagenlogische Formeln

Schluss: Sonst gibt es keine Formeln

Vereinbarungen:

1. $\mathcal{A}$ bezeichnet die Menge aller Aussagenvariablen
2. aussagenlogische Formeln bezeichnen wir durch F, G, H (mit eventuellen Indizes)

3. Mengen von aussagenlogischen Formeln bezeichnen wir durch X, Y, Z (eventuell mit Indizes)

4. Sprechweise: Aussagevariablen heißen **Atome**.

5. Klammereinsparungsregeln:

   - Außenklammern weglassen
   - Bindungsstärke der Junktoren ist von links nach rechts mit abnehmender Priorität: $\neg$, $\{\wedge, \vee\}$, $\rightarrow$, $\leftrightarrow$

6. Sprechweise: F heißt Teilformel von G $\leftrightarrow$

   a) F und G sind Formel

   b) F ist ein Teilwort von G

   Beispiel: Alle Teilformeln von $(A \rightarrow (B \vee \neg B))$ sind: A, B, $\neg B$, $(B \vee \neg B)$, $(A \rightarrow (B \vee \neg B))$

Die Menge der Wahrheitswerte bzw. Boolschen Werte wird bezeichnet durch $B = \{0, 1\}$
Dabei steht 0 für „falsch“ und 1 für „wahr“.

Definition 1.2 (induktive Definition der Semantik)
Eine Belegung β der Variablen aus $\mathcal{A}$ ist eine Abbildung $\beta\colon \mathcal{A} \mapsto B$
(β ordnet jedem Atom einen Wahrheitswert zu)

Eine Interpretation I_β der Formeln ist induktiv wie folgt definiert:

IA $I_\beta(A) = \beta(A)$ für alle $A \in \mathcal{A}$

IS Falls $I_\beta(F)$ und $I_\beta(G)$ bereits gegeben sind, dann ist

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

1.3 Modelle, Äquivalenzen, Normalformen

Definition 1.3
Es sei F eine Formel und β eine Belegung von F.

1. β heißt **Modell** von $F \Leftrightarrow I_\beta(F) = 1$
2. F heißt *erfüllbar* $\Leftrightarrow$ F besitzt ein Modell
3. F heißt gültig oder **Tautologie** $\Leftrightarrow$ jede Belegung ist ein Modell von F
4. F heißt *unerfüllbar* $\Leftrightarrow$ jede Belegung ist kein Modell von F bzw. F besitzt kein Modell.

Bezeichnungen:

$\mathcal{L}_{AL}(\mathcal{A})$	bezeichnet die Menge aller aussagenlogischen Formeln mit der Menge der Atome $\mathcal{A}$.
SAT	Menge aller erfüllbaren Formeln
$TAUT$	Menge aller Tautologien
$\overline{SAT}$	Menge aller unerfüllbaren Formeln

Definition 1.4
Es seien F und G Formeln.
F und G heißen **semantisch äquivalent** $\Leftrightarrow$ für alle Belegungen stimmen die Wahrheitswerte von F und G überein: $I_\beta(F) = I_\beta(G)$

Schreibweise: $(F \models G) \wedge (G \models F)$

Frage: Was hat „semantische Äquivalenz“ mit der Bijunktion „$\leftrightarrow$“ zu tun?
„$\leftrightarrow$“: Formel vs. „$\models\!\!\!\models$“: keine Formel, Aussage über Formel

Satz 1.1
F und G Formeln.
$F \models\!\!\!\models G$ gdw. $(F \leftrightarrow G) \in TAUT$

Beweis:
$F \models\!\!\!\models G$
$\Leftrightarrow$ für alle Belegungen β gilt: $I_\beta(F) = I_\beta(G)$
$\Leftrightarrow$ für alle Belegungen β gilt: $I_\beta(F \leftrightarrow G) = 1$
$\Leftrightarrow (F \leftrightarrow G) \in TAUT$ ∎

Beobachtung: Jede Formel definiert eine Boolsche Funktion f.
Es seien $A_1, \ldots, A_n$ Atome in der Formel F.
Schreibweise: $F(A_1, \ldots, A_n)$
Ein solches F definiert eine n-stellige boolsche Funktion

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

wobei gilt: $f_F(x_1, \ldots, x_n) = y \Leftrightarrow$ für $\beta(A_1) = x_1$ und $\beta(A_2) = x_2$ und ... und $\beta(A_n) = x_n$ gilt:

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

Fakt
F äq. $G \Leftrightarrow f_F = f_G$

Fazit: Die semantische Äquivalenz „$\models\!\!\models$“ ist eine **Äquivalenzrelation** auf der Menge $\mathcal{L}(\mathcal{A})$

Satz 1.2 (Regeln für semantisch äquivalentes umformen)
Für Formeln F, G, H gilt:

$(F \wedge G) \models\!\!\models (G \wedge F)$, Disjunktion und Bijunktion genauso (Kommutivität)

$(F \wedge G) \wedge H) \models\!\!\models F \wedge (G \wedge H)$, Disjunktion genauso (Assozivität)

$$\left.\begin{array}{l} F \wedge (F \vee G) \models\!\!\models F \\ F \vee (F \wedge G) \models\!\!\models F \end{array}\right\} \text{Absorbtion}$$

$\neg\neg F \models\!\!\models F$ (doppelte Negation)

$$\left.\begin{array}{l} \neg(F \wedge G) \models\!\!\models \neg F \vee \neg G \\ \neg(F \vee G) \models\!\!\models \neg F \wedge \neg G \end{array}\right\} \text{de Morgansche Regeln}$$

$$\left.\begin{array}{l} F \wedge (G \vee H) \models\!\!\models (F \wedge G) \vee (F \wedge H) \\ F \vee (G \wedge H) \models\!\!\models (F \vee G) \wedge (F \vee H) \end{array}\right\} \text{Distributiviät}$$

$$\left.\begin{array}{ll} F \in TAUT: & F \wedge G \models\!\!\models G \\ F \in TAUT: & F \vee G \models\!\!\models F \end{array}\right\} \text{Tautologieregeln}$$

$$\left.\begin{array}{ll} F \in \overline{SAT}: & F \wedge G \models\!\!\models F \\ F \in \overline{SAT}: & F \vee G \models\!\!\models G \end{array}\right\} \text{Unerfüllbarkeitsregeln}$$

$F \wedge F \models\!\!\models F$ und $F \vee F \models\!\!\models F$ (Idempotenzregeln)

Satz 1.3 (Ersetzbarkeitstheorem)
Es seien F, E zwei semantisch äquivalente Formeln.
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 ist

$$G \models\!\!\models H$$

BEWEIS:
durch Formelinduktion, wollen zeigen: alle Formeln $G \in \mathcal{L}_{AL}(\mathcal{A})$ besitzen die „Ersetzbarkeitseigenschaft“.

IA : Es sei $G = A$ ein Atom ($A \in \mathcal{A}$).
Dann gilt $F = A$ und damit $F = G$ und deshalb gilt: $G = F \models\!\!\!\mid E = H$

IS : Es sei G eine zusammengesetzte Formel.

1. Fall Es sei $F = G$. Dann gilt wieder $G = F \models\!\!\!\mid E = H$

2. Fall Es sei F eine echte Teilformel von G.

2.1 Es sei $G = (G_1 \wedge G_2)$ eine *Konjunktion*
Nach Induktionsvorraussetzung besitzen $G_{1,2}$ bereits die Ersetzungseigenschaft. Da F eine echte Teilmenge von G ist, ist F eine Teilformel von G_1 oder G_2.

Fall a F sei Teilformel von G_1
H_1 sei eine Formel die durch Ersetzung von F durch E aus G_1 entsteht.
Dann $G_1 \models\!\!\!\mid H_1$. Dann gilt:
$H = (H_1 \wedge G_2)$ und
$I_\beta(H) = \min\{I_\beta(H_1), I_\beta(G_2)\} = \min\{I_\beta(G_1), I_\beta(G_2)\} = I_\beta(G)$
$\Rightarrow H \models\!\!\!\mid G$

Fall b F sei Teilformel von G_2: s. Fall a

2.2 Es sei $G = (G_1 \vee G_2)$ eine Disjunktion. Schluss wie bei 2.1

2.3 Es sei $G = (G_1 \rightarrow G_2)$ eine Implikation.
F ist eine Teilformel von G_1 oder G_2.

Fall a Sei F Teilformel von G_1 und H_1 die Formel, die durch Ersetzung von F durch E aus G_1 entsteht: dann gilt $G_1 \models\!\!\!\mid H_1$.
Weiter ist $H = (H_1 \rightarrow G_2)$ und es gilt:
$I_\beta(H) = 1 \Leftrightarrow I_\beta(H_1) \leq I_\beta(G_2) \Leftrightarrow I_\beta(G_1) \leq I_\beta(G_2) \Leftrightarrow I_\beta(G) = 1$
$\Rightarrow H \models\!\!\!\mid G$

Fall b wie oben mit F Teilformel von G_2

2.4 Es sei $G = (G_1 \leftrightarrow G_2)$: wie 2.3

2.5 Es sei $G = \neg G'$ eine Negation
Dann ist F eine Teilformel von G' und H' sei eine Formel, die durch Ersetzung von F durch E aus G' entsteht.
Nach Induktionsvorraussetzung ist $G' \models\!\!\!\mid H'$ und damit:
$I_\beta(H) = 1 - I_\beta(H') = 1 - I_\beta(G') = I_\beta(G)$ (da $H = \neg H'$)
$\Rightarrow H \models\!\!\!\mid G$ ∎

1.3.1 Disjunktive und konjunktive Normalform

Definition 1.5

1. Jedes Atom $A \in \mathcal{A}$ heißt **positives Literal**
   Jede Negation $\neg A$ heißt **negatives Literal**

2. Eine Formel der Gestalt

   $$(L_{11} \wedge L_{12} \wedge \ldots \wedge L_{1n_1}) \vee (L_{21} \wedge L_{22} \wedge \ldots \wedge L_{2n_2}) \vee \ldots \vee (L_{m1} \wedge L_{m2} \wedge \ldots \wedge L_{mn_m})$$

   oder kurz: $\bigvee_{i=1}^{m}(\bigwedge_{j=1}^{n_i} L_{ij})$, heißt **disjunktive Normalform** (**DNF**)

3. Eine Formel der Gestalt

   $$\bigwedge_{i=1}^{m}(\bigvee_{j=1}^{n_i} L_{ij})$$

   wobei alle L_{ij} Literale sind, heißt **konjunktive Normalform** (**KNF**)

Satz 1.4
Zu jeder Formel F gibt es eine semantisch äquivalente Formel in DNF (F_D) und eine semantisch äquivalente Formel in KNF (F_K)

Beweis: (durch Formelinduktion)
wir beweisen simultan: jede Formel F besitzt „DNF“ und „KNF“

IA : Es sei $F = A$ ein Atom. Dann ist F ein Literal L_{11} und somit in [D|K]NF

IS : Es sei F eine zusammengesetzte Formel.

Fall a Es sei F eine Negation $F = \neg F'$. F' erfüllt die Induktionvorraussetzung und besitzt deshalb [D|K]NF.
Es sei $F'_D = \bigvee_{i=1}^{m}(\bigwedge_{j=1}^{n_i} L_{ij})$.
Dann gilt:

$$\begin{aligned} F = \neg F'_D &= \neg(\bigvee_{i=1}^{m}(\bigwedge_{j=1}^{n_i} L_{ij}) \\ &\models \bigwedge_{i=1}^{m}(\neg(\bigwedge_{j=1}^{n_i} L_{ij}) \\ &\models \bigwedge_{i=1}^{m}(\bigvee_{j=1}^{n_i} \neg L_{ij}) \\ &\models \bigwedge_{i=1}^{m}(\bigvee_{j=1}^{n_i} \overline{L_{ij}}) \end{aligned}$$

wobei $\overline{L_{ij}} = \begin{cases} \neg A, \text{ falls } L_{ij} = A \\ A, \text{ falls } L_{ij} = \neg A \end{cases}$

Dies ist eine Formel in KNF. Ähnlich F'_K: liefert eine zu F semantisch äquivalente Formel in DNF.

Fall b Es seien $F = (F' \wedge F'')$ eine Konjunktion. F' und F'' erfüllen die IV und so gilt $F' \models\!\!\models F'_D$ in DNF und $F' \models\!\!\models F'_K$ in KNF und $F'' \models\!\!\models F''_D$ ind DNF und $F'' \models\!\!\models F''_K$ in KNF.
Zunächst

1. KNF für F: $(F'_K \wedge F''_K)$ ist in KNF und es gilt: $F = (F' \wedge F'') \models\!\!\models (F'_K \wedge F''_K)$
2. semantisch äquivalente DNF für F: wir gehen aus von $F'_D \models\!\!\models F'$ und $F''_D \models\!\!\models F''$ F'_D hat die Gestalt $\bigvee_{i=1}^{m'} G_i$, dabei ist $G_i = \bigwedge_{j=1}^{n_i} L_{ij}$ und F''_D hat die Gestalt $\bigvee_{k=1}^{m''} H_k$, dabei ist $H_k = \bigwedge_{j=1}^{n_k} L_{ij}$ und es gilt (mit Distributivgesetz):

$$\begin{aligned} F = (F' \wedge F'') \models\!\!\models F'_D \wedge F''_D &= (\bigvee_{i=1}^{m'} G_i) \wedge (\bigvee_{k=1}^{m''} H_k) \\ &\models\!\!\models \bigvee_{i=1}^{m'} \Big(G_i \wedge (\bigvee_{k=1}^{m''} H_k) \Big) \\ &\models\!\!\models \bigvee_{i=1}^{m'} \Big(\bigvee_{k=1}^{m''} (\underbrace{G_i \wedge H_k}_{\text{Konjugation von Literalen}}) \Big) \end{aligned}$$

Dies ist eine DNF.

Fall c Disjunktionen: Es sei $F = (G \vee H)$.
Es gilt: $F \models\!\!\models \neg\neg(G \vee H) \models\!\!\models \neg(\neg G \wedge \neg H)$
Weiter wie in Fall a und b.

Fall d Implikation: Es sei $F = (G \to H)$.
Dann ist $F \models\!\!\models \neg G \vee H$. Weiter wie Fall c.

Fall e Bijunktionen: Es sei $F = (G \leftrightarrow H)$.
Dann ist $F \models\!\!\models (G \wedge H) \vee (\neg G \wedge \neg H)$. Weiter wie in Fall a, b, c. ∎

Der Beweis ist zugleich Nachweis der Korrektheit des folgenden Algorithmus.

1. Verfahren zur Bestimmung der Normalform

1. Schritt: Ersetze alle „↔“ gemäß $G \leftrightarrow H \models\!\!\models (G \to H) \wedge (H \to G)$

2. Schritt: Ersetze alle Pfeile „→“ gemäß $(G \to H) \models\!\!\models (\neg G \vee H)$
Nun ergibt sich eine Formel, die nur aus Konjunktionen und Disjunktionen besteht.

3. Schritt: Negation „nach innen“ ziehen, gemäß $\neg(G \wedge H) \models\!\models \neg G \vee \neg H$ und $\neg(G \vee H) \models\!\models \neg G \wedge \neg H$

4. Schritt: **a** für eine KNF:
Disjunktionen nach „innen“ ziehen, gemäß $F \vee (G \wedge H) \models\!\models (F \vee G) \wedge (F \vee H)$

b für eine DNF:
Konjunktionen nach „innen“ ziehen, gemäß $F \wedge (G \vee H) \models\!\models (F \wedge G) \vee (F \wedge H)$

Nach Schritt 4 ergibt sich eine Formel in KNF/DNF

5. Schritt: Kürzen

a für KNF

a.1 $\ldots \wedge (A \vee B \vee \ldots \vee B \vee B \vee A) \wedge \ldots \models\!\models \ldots \wedge (A \vee B) \wedge \ldots$ lasse alle Mehrfachvorkommen in Disjunktionen weg.

a.2 $\ldots \wedge (A \vee \ldots \vee \neg A) \wedge \ldots \models\!\models w$ streiche komplette Klammer, da Tautologie.

b für DNF

b.1 genauso wie 5.a.1 gemäß Idempotenzregel.

b.2 $\ldots \vee (A \wedge \ldots \wedge \neg A) \vee \ldots$ komplette Klammer weglassen, da Konjunktion immer falsch.

Schreibweise: $w := A \vee \neg A$ und $f := A \wedge \neg A$
w und f sind *keine* Formeln, sondern Abkürzungen für Formeln.

2. Verfahren zur Bestimmung der Normalform

Ausgangspunkt für dieses Verfahren ist die Wahrheitswerttabelle.
Es sei $F(A_1, \ldots, A_n)$ eine Formel. Wahrheitswerttabelle für f_F:

	$\beta(A_1)$	$\beta(A_2)$	$\ldots$	$\beta(A_n)$	$I_\beta(F)$
Zeile 0	0	$\ldots$	0		
$\vdots$				$\vdots$	
Zeile j	x_1	x_2	$\ldots$	x_n	y
$\vdots$				$\vdots$	
Zeile $2^n - 1$	1	1	$\ldots$	1	

Wir definieren zwei Mengen:
$E := \big\{(x_1, \ldots, x_n) \in \{0,1\}^n |$ wenn $\beta(A_1) = x_1$ und $\beta(A_2) = x_2$ und $\ldots$ und $\beta(A_n) = x_n$ dann ist $I_\beta(F) = 1\big\}$
$N := \big\{(x_1, \ldots, x_n) \in \{0,1\}^n |$ wenn $\beta(A_1) = x_1$ und $\beta(A_2) = x_2$ und $\ldots$ und $\beta(A_n) = x_n$ dann ist $I_\beta(F) = 0\big\}$
Klar ist: $E \cap N = \varnothing$ und $E \cup N = \{0,1\}^n$

E und N bilden eine Zerlegung der Menge aller 0-1-Tupel.
Für

DNF: für $(x_1, \ldots, x_n) \in \{0,1\}^n$ definieren wir:

$$A_1^{x_1} \wedge A_2^{x_2} \wedge \ldots \wedge A_n^{x_n} \text{ durch}$$
$$A_i^{x_i} := \begin{cases} A_i \text{ falls } x_i = 1 \\ \neg A_i \text{ falls } x_i = 0 \end{cases}$$

Bemerkung: $A_i^{x_i}$ ist stets ein Literal und eine Formel der obigen Gestalt heißt **Elementarkonjunktion**.

Fakt
$I_\beta(A_i^{x_i}) = 1 \Leftrightarrow \beta(A_i) = x_i$ und damit $I(A_1^{x_1} \wedge A_2^{x_2} \wedge \ldots \wedge A_n^{x_n}) \Leftrightarrow \bigwedge_{1 \le i \le n} \beta(A_i) = x_i$
Also: $F \models\!\models \bigvee_{(x_1,\ldots,x_n) \in E} (A_1^{x_1} \wedge \ldots \wedge A_n^{x_n})$.
Eine solche DNF heißt **kanonische DNF (DKNF)**

KNF: für $(x_1, \ldots, x_n) \in \{0,1\}^n$ definieren wir:

$$A_1^{\overline{x_1}} \vee A_2^{\overline{x_2}} \vee \ldots \vee A_n^{\overline{x_n}} \text{ durch}$$
$$A_i^{\overline{x_i}} := \begin{cases} \neg A_i \text{ falls } x_i = 1 \\ A_i \text{ falls } x_i = 0 \end{cases}$$

Bemerkung: $A_i^{\overline{x_i}}$ ist ein Literal und eine Formel der obigen Gestalt heißt Elementarkonjunktion.

Fakt
$I_\beta(A_i^{\overline{x_i}}) = 0 \Leftrightarrow \beta(A_i) = x_i$ und damit $I(A_1^{\overline{x_1}} \vee A_2^{\overline{x_2}} \vee \ldots \vee A_n^{\overline{x_n}}) = 0 \Leftrightarrow \beta(A_1) = x_i$ und $\ldots$ und $\beta(A_n) = x_n$
Also: $F \models\!\models \bigwedge_{(x_1,\ldots,x_n) \in N} (A_1^{\overline{x_1}} \vee \ldots \vee A_n^{\overline{x_n}})$.
Eine solche KNF heißt **kanonische KNF (KKNF)**

Codenummern von Wahrheitswertfunktionen

Es sei $f\colon \{0,1\}^n \mapsto \{0,1\}$ (d. h. f n-stellige Funktion, n fix)

Wahrheitswertabelle:

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

Dann gilt:
$i = x_1^* \cdot 2^{n-1} + x_2^* \cdot 2^{n-2} + \ldots + x_{n-1}^* \cdot 2^1 + x_n^* \cdot 2^0$
$= \sum_{j=1}^{n} (x_j^* \cdot 2^{n-j})$
f ist festgelegt durch die Eintragungen $y_0, y_1, \ldots, y_{2^n-1}$ und wir definieren für dieses n-stellige f

Definition 1.6

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

Beispiel 1.6
$Code(seq) = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 = 11$

x_1	x_2	$f(x_1, x_2) = seq(x_1, x_2)$
0	0	1
0	1	1
1	0	0
1	1	1

Alle Informationen über F bzw. f_F sind in Code(f) gespeichert.

1.3.2 HORN-Formeln

Definition 1.7
Eine Formel F ist eine **HORN-Formel** $\Leftrightarrow$

1. F ist in KNF
2. Jede Disjunktion entält *höchstens* ein positives Literal

Beispiel 1.7
Eine gültige HORN-Formel: $(A \vee \neg B \vee \neg C) \wedge (C \vee \neg D) \wedge (\neg A \vee \neg B)$

Frage: Gibt es für jede KNF eine semantisch äquivalente HORN-Formel?
Anwort: Nein!

HORN-Formeln sind aus zwei Gründen von Bedeutung:

1. Sie lassen sich als PROLOG-Anweisung auffassen
2. Sie besitzen einen effizienten Erfüllbarkeitstest

zu 1: prozedurale Deutung am (obigen) Beispiel:
$(A \vee \neg B \vee \neg C) \models\!\!\!\models (\neg(B \wedge C) \vee A) \models\!\!\!\models (B \wedge C) \rightarrow A$
$(C \vee \neg D) \models\!\!\!\models (\neg D \vee C) \models\!\!\!\models (D \rightarrow C)$
$\neg A \vee \neg B \models\!\!\!\models \neg(A \wedge B) \models\!\!\!\models \neg(A \wedge B) \vee f \models\!\!\!\models A \wedge B \rightarrow f$

zu 2: Algorithmus

1. Schritt: Markiere alle Vorkommen von Atomen, die in Implikationen der Gestalt $(w \rightarrow A)$ auftreten

2. Schritt: while es gibt Teilformeln der Gestalt

i $A_1 \wedge \ldots \wedge A_n \to B$ oder

ii $A_1 \wedge \ldots \wedge A_n \to f$

, wobei alle Atome $A_1, \ldots, A_n$ bereits markiert sind
do if Fall i then markiere alle Vorkommen von B
else return Ausgabe „unerfüllbar“

3. Schritt: return Ausgabe „erfüllbar“

Satz 1.5

1. Der Markierungsalgorithmus ist für HORN-Formeln als Eingabe korrekt.
2. Falls die Ausgabe „erfüllbar“ erreicht wird, dann ist die Belegung $\beta(A) = 1$ für alle markierten Atome A ein Modell für die Formel.
3. Für die Formel F mit n Atomen liefert der Algorithmus nach höchstens n Durchläufen eine Ausgabe. Das heißt der Algorithmus hat linearen Aufwand.

BEWEIS:

zu 3: In jedem Durchlauf wird ein Atom markiert. Nach höchstens n Durchläufen ist nichts mehr zu markieren und eine Ausgabe erscheint.

Lemma 1.1

zu 2: Für alle Belegungen β der Formel F gilt: falls β ein Modell von F ist, dann gilt für alle Atome in F: falls A markiert ist, dann ist $\beta(A) = 1$.

BEWEIS:

a die Behauptung gilt für alle Atome A die in Teilformeln der Gestalt $(w \to A)$ auftreten. Solche Atome werden im ersten Schritt markiert.
Andererseits gilt: eine KNF ist wahr, gdw. jede Disjunktion der KNF ist wahr, insb. diejenigen, die die nur aus einem positiven Literal bestehen, also genau die mit $(w \to A)$.

b Die Behauptung gilt auch für alle Atome B, die im 2. Schritt markiert werden: wir betrachten eine Teilformel der Gestalt $A_1 \wedge \ldots \wedge A_n \to B$
B wird nur markiert, falls alle A_i markiert sind. Dies bedeutet für jedes Modell β: $\beta(A_1) = \ldots = \beta(A_n) = 1$.
Damit gilt: $I_\beta(A_1 \wedge \ldots \wedge A_n \to B) = 1 \Leftrightarrow \beta(B) = 1$ ∎

zu 1: a die Ausgabe „unerfüllbar“ ist korrekt

BEWEIS: (INDIREKT)
Angenommen, diese Aussage sei falsch. Dann hat die Formel F ein Modell β. Die Ausgabe „unerfüllbar“ erfolgt im 2. Schritt für $A_1 \wedge \ldots \wedge A_n \to f$, wobei alle $A_1, \ldots, A_n$ markiert sind.
Wegen des Lemmas gilt $\beta(A_1) = \ldots = \beta(A_n) = 1$. Dann gilt

$$I_\beta(A_1 \wedge \ldots \wedge A_n \to f) = 0$$

im Widerspruch zur Annahme, dass β ein Modell ist.
$\Rightarrow F$ hat kein Modell.

■

b Die Ausgabe „erfüllbar“ ist korrekt.
Es sei G eine beliebige Disjunktion („Klausel“) von F.

1. Fall: $G \models\!\!\!|\; A$ (d. h. $G = w \to A$)
A wird im ersten Schritt markiert und $\beta(A) = 1$ ist ein Modell von G.

2. Fall: Es sei $G = A_1 \wedge \ldots \wedge A_n \to B$ und alle Atome $A_1, \ldots, A_n$ sind markiert
Dann wird im 2. Schritt B markiert und $\beta(A_1) = \ldots = \beta(A_n) = 1 = \beta(B)$ ist ein Modell von G.

3. Fall: Es sei $G = A_1 \wedge \ldots \wedge A_n \to B$ aber nicht alle Atome $A_1, \ldots, A_n$ sind markiert. o. B. d. A. sei A_1 nicht markiert.
Dann ist $\beta(A_1) = 0$ ein Modell von G, denn $I_\beta(A_1 \wedge \ldots \wedge A_n \to B) = 1$

4. Fall: Es sei $G = A_1 \wedge \ldots \wedge A_n \to f$ und die Atwort „unerfüllbar“ sei nicht erfolgt. Dann sind nicht alle Atome $A_1, \ldots, A_n$ markiert. Dann ist wie in Fall 3 $I_\beta(A_1 \wedge \ldots \wedge A_n \to f) = 1$. ■

1.4 Die Folgerungsrelation und der Endlichkeitssatz

wollen formal beschreiben: aus einer Formel F folgt eine Formel G.
inhaltlich: immer wenn F gilt, dann muss auch G gelten.

Definition 1.8
G heißt **Folgerung** aus $F \Leftrightarrow$ jedes Modell von F auch Modell von G.

Schreibweise: $F \models G$

Das heißt für alle Belegungen β gilt:

$$\begin{array}{ccc} I_\beta(F) = 1 & \to & I_\beta(G) = 1 \\ I_\beta(F) & \leq & I_\beta(G) \\ f_F & \leq & f_G \end{array}$$

Beispiel 1.8
1. Möglichkeit: „Argumentation über Wahrheitswerttabelle“
$F := A \wedge (\neg A \vee B)$ und $G := B$

$I_\beta(A)$	$I_\beta(B)$	$I_\beta(\neg A \vee B)$	$I_\beta(F)$	$I_\beta(G)$	
0	0	1	0	0	
0	1	1	0	1	Man sieht: $f_F \leq f_G$.
1	0	0	0	0	
1	1	1	1	1	

2. Möglichkeit: „Argumentation über Modell“
Es sei β ein Modell von F.
Dann gilt: β ist ein Modell von A und Modell von $(\neg A \vee B)$. Da $I_\beta(A) = 1$, ist $I_\beta(\neg A) = 1 - I_\beta(A) = 0$.
Andererseits ist $I_\beta(\neg A \vee B) = 1 = \max\{I_\beta(\neg A), I_\beta(B)\} = \max\{0, I_\beta(B)\} = 1$
Also ist $I_\beta(B) = 1$, β also Modell von G.

Frage: Welche Beziehungen bestehen zwischen der Implikation „$\rightarrow$“ und der Folgerungsrelation „$\models$“?
klar ist: für Formeln F und G ist

i $F \rightarrow G$ wieder eine Formel, aber

ii $F \models G$ ist *keine* Formel, sondern eine Aussage über Formeln.

Fakt

$$\begin{aligned} F \models G &\Leftrightarrow F \rightarrow G \in TAUT \\ F \models G &\Leftrightarrow \bigwedge_\beta (I_\beta(F) \leq I_\beta(G)) \\ &\Leftrightarrow \bigwedge_\beta (I_\beta(F \rightarrow G) = 1) \\ &\Leftrightarrow F \rightarrow G \in TAUT \end{aligned}$$

Fakt

$$\begin{aligned} F \models\!\models G &\Leftrightarrow (F \models G \text{ und } G \models F) \\ F \models\!\models G &\Leftrightarrow \bigwedge_\beta (I_\beta(F) = I_\beta(G)) \\ &\Leftrightarrow \bigwedge_\beta (I_\beta(F) \leq I_\beta(G) \text{ und } I_\beta(G) \leq I_\beta(F)) \\ &\Leftrightarrow F \models G \text{ und } G \models F \end{aligned}$$

Wir werden einen Test auf Unerfüllbarkeit entwickeln.
Es gilt:

a $F \models G \Leftrightarrow (F \rightarrow G) \in TAUT \Leftrightarrow \neg(F \rightarrow G) \in \overline{SAT} \Leftrightarrow (F \wedge \neg G) \in \overline{SAT}$

b $F \models\!\models G \Leftrightarrow (F \leftrightarrow G) \in TAUT \Leftrightarrow \neg(F \leftrightarrow G) \in \overline{SAT}$

c $F \in TAUT \Leftrightarrow \neg F \in \overline{SAT}$

d $F \in SAT \Leftrightarrow \neg F \notin \overline{SAT}$

$F \models G$ formalisiert „aus F lässt sich G beweisen“.

1. Beobachtung: Im allgemeinen werden aus mehreren Vorraussetzungen Schlussfolgerungen gezogen.
2. Beobachtung: Jeder konkrete Beweis ist endlich.

Definition 1.9
Es sei X eine Menge von Formeln und es sei F eine Formel.

1. X besitzt ein Modell $\Leftrightarrow_{df}$ es gibt eine Belegung β, die alle Formeln aus X erfüllt.
2. X ist erfüllbar $\Leftrightarrow_{df}$ X besitzt ein Modell
3. F ist eine Folgerung von X $\Leftrightarrow_{df}$ jedes Modell von X ist auch Modell von F
   Schreibweise: $X \models F$
4. Es sei Y eine Formelmenge.
   Y folgt aus X $\Leftrightarrow_{df}$ jedes Modell von X ist Modell für jede Formel in Y ($X \models Y$)

Bemerkung 1.1
a Es gilt nicht: X ist erfüllbar $\Leftrightarrow$ alle Formeln aus X sind erfüllbar.

Beispiel 1.9
$X = \{A, \neg A\}$
Dann gilt:

i A ist erfüllbar für $\beta(A) = 1$
$\neg A$ ist erfüllbar für $\beta(A) = 0$, aber

ii X besitzt kein Modell! X ist unerfüllbar.

b $X \models Y \Leftrightarrow$ für jede Belegung β gilt: falls β Modell für alle Formeln aus X ist, dann gilt für jede Formel $F \in Y$: β ist Modell von F!

Bemerkung 1.2 (Eigenschaften der Folgerungsrelation)
1. $\models$ ist *reflexiv*, d. h. $X \models X$ (es gilt: $X \supseteq Y$, dann ist $X \models Y$)
2. $\models$ ist *transitiv*, d. h. $X \models Y \wedge Y \models Z \rightarrow X \models Z$
3. $Fl(X) := \{G \mid G \in \mathcal{L}_{Al} \text{ und } X \models G\}$ heißt **Folgerungshülle** von X.

Die Folgerungshülle besitzt folgende Eigenschaften:

1. Einbettung: $X \subseteq Fl(X)$
2. Monotonie: $X \subseteq Y \rightarrow Fl(X) \subseteq Fl(Y)$
3. Abgeschlossenheit: $Fl(Fl(X)) = Fl(X)$

Diese 3 Eigenschaften charakterisieren die Abbildung

$$Fl\colon\ \mathcal{P}(\mathcal{L}_{Al}) \mapsto \mathcal{P}(\mathcal{L}_{Al})$$

als **Hüllenoperator**.

Beispiel 1.10
für eine *unendliche* Formelmenge $X = \{A_1, A_1 \to A_2, A_2 \to A_3, \ldots\}$
Frage: Folgt A_{17} aus X?
Antwort: ja.

Beweis:
help: hier ist ein wenig zuviel platz?

1. Schritt: $\{A_1, A_1 \to A_2\} \models A_2$ $(A_2 \in Fl(X))$
2. Schritt: $\{A_2, A_2 \to A_3\} \models A_3$ $(A_3 \in Fl(X))$

$\vdots$

16. Schritt: $\{A_{16}, A_{16} \to A_{17}\} \models A_{17}$ $(A_{17} \in Fl(X))$

Also $X \models A_{17}$ ∎

1.4.1 Endlichkeitssatz

Satz 1.6
Es seien X eine (beliebige unendliche) Formelmenge und es sei F eine Formel.

$$X \models F \text{ gdw. es gibt eine endliche Teilmenge } X_{FIN} \text{ von } X, \text{ s. d. } X_{FIN} \models F$$

Satz 1.7
Es sei X eine (unendliche) Formelmenge und es sei F eine Formel.

X ist unerfüllbar gdw. es gibt eine Teilmenge $X_{Fin} \subseteq X$ (X_{Fin} endlich), die unerfüllbar ist.

Satz 1.8
Es sei X eine (unendliche) Formelmenge.

Alle endlichen Teilmengen von X sind erfüllbar, gdw. X ist erfüllbar.

Logische Struktur dieser Sätze:
Satz 1.6: $A_1 \leftrightarrow A_2$
Satz 1.7: $B_1 \leftrightarrow B_2$
Satz 1.8: $C_1 \leftrightarrow C_2$

Trivialerweise gilt: $A_2 \to A_1$, $B_2 \to B_1$ und $C_2 \to C_1$.

weitere Beziehungen: $B_2 = \neg C_1$ und $B_1 = \neg C_2$

$$B_1 \to B_2 \models\!\dashv \neg C_2 \to \neg C_1 \models\!\dashv C_1 \to C_2$$

d. h. Satz 1.7 ist äquivalent zu Satz 1.8

Behauptung: Aus Satz 1.6 folgt Satz 1.7!
Es sei X unerfüllbar, d. h. X hat kein Modell. Es sei G irgendeine Formel.

Dann gilt: Jedes Modell von X ist auch Modell von G.
Das heißt $X \models G$ (aus einer unerfüllbaren Formelmenge folgt jede Formel)

Insbesondere gilt: $X \models f$, $f := A \wedge \neg A$
Satz 1.6 impliziert: es gibt eine endliche Teilmenge $X_{Fin} \subseteq X$ mit $X_{Fin} \models f$.

Da jedes Modell von X_{Fin} auch Modell von f ist, aber f kein Modell hat, besitzt auch X_{Fin} kein Modell.

Wir haben gezeigt: $\{A_1 \to A_2\} \models \{B_1 \to B_2\}$

es gilt auch: aus Satz 1.7 folgt Satz 1.6: $\{B_1 \to B_2\} \models \{A_1 \to A_2\}$.

Es gelte: $X \models F$
Wir betrachten $X \cup \{\neg F\}$. Behauptung: $X \cup \{\neg F\}$ ist unerfüllbar.

indirekt: Angenommen es gibt ein Modell β von $X \cup \{\neg F\}$. Dann gilt:

a β ist Modell von X und

b β ist Modell von $\neg F$

b bedeutet: $I_\beta(\neg F) = 1$, d. h. $I_\beta(F) = 0$.
Aus a folgt: (mit $X \models F$) $I_\beta(F) = 1$ (β ist Modell von F ↯)

Satz 1.7 impliziert: es gibt eine endliche Teilmenge $X'_{Fin} \subseteq X \cup \{\neg F\}$, die unerfüllbar ist.

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

1. Fall: auch X_{Fin} ist unerfüllbar. Dann gilt: aus X_{Fin} folgt jede Formel, insb. $X_{Fin} \models F$

2. Fall: X_{Fin} ist erfüllbar. Dann gibt es ein Modell β von X_{Fin}. β ist sicher kein Modell von $\neg F$. Das heißt $I_\beta(\neg F) = 0$, d. h. aber $I_\beta(F) = 1$. Also ist β Modell von von F.

Also gilt: $X_{Fin} \models F$

Damit gilt Satz 1.6 $\models\!\dashv$ Satz 1.7.

BEWEIS: (SATZ 1.8)
Problem: Aus der Fülle der Modelle der endlichen Teilmengen (die zueinander nicht konsistent sein müssen) ein gemeinsames Modell für alle Formeln aus X zu konstruieren.

Es sei X eine unendliche Formelmenge, in der die (unendlich viele) Atome $A_1, A_2, A_3, \ldots$ vorkommen.

Für $n \geq 1$ definieren wir X_n als die Menge aller Formeln aus X, die höchstens $A_1, \ldots, A_n$ enthalten.

Zum Beispiel enthält X_1 alle Formeln aus X, in denen nur A_1 vorkommt. (Selbst diese Menge X_1 kann noch unendlich sein)

Es gilt: $X_1 \subseteq X_2 \subseteq X_3 \subseteq \ldots \subseteq X$ und $\bigcup_{n=1}^{\inf} X_n = X$

Es gilt: für jedes $F \in X$ gibt es einen Index n_F, s. d. $F \in X_{n_F}$

Jede der Mengen X_n kann unendlich sein, *aber* jede dieser Mengen enthält nur endlich viele paarweise nicht-äq. Formeln!

Wir wissen:

i $F \models\!\models G$ gdw. $f_F = f_G$ und

ii für jedes n gilt: es gibt genau 2^{2^n} Wahrheitswertfunktionen über den Atomen $A_1, \ldots, A_n$

Wir legen fest: Y_n sei eine Teilmenge von X_n, die eine max. Menge paarweise nicht-äq. Formeln enthält.

Dann gilt:

***** jedes Modell von Y_n ist endlich und

****** jedes Modell von Y_n ist auch Modell von X_n

Nach Vorraussetzung gilt: für alle $n \geq 1$ ist Y_n erfüllbar!

Für alle $n \geq 1$ sei β_n ein Modell von Y_n.
Damit haben wir eine Familie $(\beta_n)^{n \geq 1}$ von Modellen für die gilt: β_n ist Modell von X_n und damit von $X_{n-1}, \ldots, X_2, X_1$.

Also gilt:

******* für alle $k \geq n$ ist β_k Modell von X_n

Aufgabe: Aus der Familie $(\beta_n)_{n=1}^{\inf}$ *ein* Modell β von X zu konstruieren.

Konstruktion in Stufen: neben der Belegung β auch eine Indexmenge I

Stufe 0 $\beta := \varnothing,\ I := \{1, 2, 3, \ldots\}$ (Initialisierung)

Stufe n+1 if(es gibt unendlich viele Indizes $i \in I$ mit $\beta_i(A_{n+1}) = 1$)
then $\beta(A_{n+1}) := 1$ und $I := I \backslash \{i | \beta_i(A_{n+1}) = 0\}$
else (es gibt nur *endlich* viele Indizes $i \in I$ mit $\beta_i(A_{n+1}) = 1$)
$\beta(A_{n+1}) := 0$ und $I := I \backslash \{i | \beta_i(A_{n+1}) = 1\}$

Fakt

1. Die Zuordnung β ist definiert für die Menge aller Atome $\{A_1, A_2, \ldots\}$ mit Werten aus $\{0,1\}_i$ d. h. β ist eine Belegung

2. Die Indexmenge I ist nach jeder Stufe unendlich. Dies ist offensichtlich nach Stufe 0. Falls die Aussage nach der Stufe n gilt, dann gilt nach Stufe $n+1$:
im if-Zweig bleiben unendlich viele i mit $\beta_i(A_{n+1}) = 1$
im else-Zweig bleiben unendlich viele i mit $\beta_i(A_{n+1}) = 0$

3. β ist ein Modell von X!
Es sei F eine Formel aus X. Müssen zeigen: β ist Modell von F.
Es sei n_F der kleinste Index, s. d. in F höchstens die Atome $A_1, A_2, \ldots, A_{n_F}$ vorkommen.
Nach der Stufe n_F gibt es keinen Index $i_{n_F} \in I$ mit der Eigenschaft $\beta_{i_{n_F}}(A_{n_F}) \neq \beta(A_{n_F})$ und es gibt keinen Index $i_{n_F-1} \in I$ mit $\beta_{i_{n_F-1}}(A_{n_F-1}) \neq \beta(A_{n_F-1})$ usw.
$\vdots$
es gibt keinen Index $i_2 \in I$ mit $\beta_{i_2}(A_2) \neq \beta(A_2)$
es gibt keinen Index $i_1 \in I$ mit $\beta_{i_1}(A_1) \neq \beta(A_1)$

   Das heißt nach der Stufe n_F gilt für *alle* $i \in I$: $\beta_i(A_1) = \beta(A_1)$ und $\beta_i(A_2) = \beta(A_2)$ usw. bis $\beta_i(A_{n_F}) = \beta(A_{n_F})$

wir wissen: (***) für alle $i \geq n_F$ gilt β_i ist Modell von X_{n_F} und $F \in X_{n_F}$

Also gilt für diese i: β_i ist Modell von F und damit β ist Modell von F. ∎

Bemerkung 1.3
Die Konstruktion sichert die Existenz eines Modells β, sie ist kein Algorithmus zur Berechnung von β!

1.5 Das Resolutionskalkül

Ziel: Test auf Unerfüllbarkeit einer Formel F.

Eingabe: help: hier muss ein Bild hin, dass eine Formel F als Eingabe in eine Blackbox „Resolutionskalkül zeigt, die die Ausgaben JA und NEIN hat.

Im Allgemeinen hat jedes Kalkül die Form $K = (Ob.\ ;\ Reg)$. Dabei steht Ob für eine Menge von Objekten (hier: Ob ist die Menge aller Formeln) und Reg steht für eine

Menge von Regeln (hier: *Reg* besteht aus einer syntaktischen Regel: Formelmanipulation)

Jedes Kalkül ist in Bezug auf eine konkrete Aufgabe definiert (hier: Test auf Unerfüllbarkeit).

Jedes Kalkül, dass funktioniert, muss in Bezug auf seine Aufgabe zwei Eigenschaften erfüllen:

1. Korrektheit: keine erfüllbare Formel wird als unerfüllbar berechnet
2. Vollständigkeit: Alle unerfüllbaren Formeln werden als unerfüllbare Formeln erkannt.

Eingabe für den Test: beliebige Formel F.
Frage: in welcher Form ist F gegeben?

Wissen: zu jeder Formel F gibt es eine KNF (die äquivalent ist)

$$\bigwedge_{i=1}^{m}(\bigvee_{j=1}^{n_i} L_{ij})$$

Dies schreiben wir in der Form:

$$\{\{L_{11}, L_{12}, \ldots, L_{1n_1}\}, \{L_{21}, \ldots, L_{2n_2}\}, \ldots, \{L_{m1}, \ldots, L_{mn_m}\}\}$$

Dies ist eine Menge von Mengen von Literalen. Letzteres heißt „**Klausel**“. Also schreiben wir die KNF als **Klauselmenge**.

Beispiel 1.11
Wir betrachten die folgenden Formeln in KNF:

$$(A_1 \vee \neg A_2) \wedge (A_1 \vee A_3 \vee \neg A_4)$$
$$(A_1 \vee A_1 \vee \neg A_2) \wedge (A_1 \vee A_3 \vee \neg A_4) \wedge (A_1 \vee A_3 \vee A_1 \vee \neg A_4)$$
$$(A_1 \vee \neg A_2 \vee \neg A_2) \wedge (A_1 \vee A_3 \vee \neg A_4 \vee A_1) \wedge (A_1 \vee \neg A_2)$$

Diese drei Formeln liefern folgende Klauselmenge:

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

Diese Zuordnung ist nicht umkehrbar eindeutig!
Aber es gilt: falls zwei Formeln F_1 und F_2 die selbe Klauselmenge liefern, dann sind sie semantisch äquivalent. ($F_1 \models\!\models F_2$)

Insbesondere gilt: $F_1 \in \overline{SAT} \leftrightarrow F_2 \in \overline{SAT}$.
Das heißt in Bezug auf den Test „Unerfüllbarkeit“ gehen durch die Reduktion keine Informationen verloren.

Definition 1.10
Es sei F eine Formel gegeben als Klauselmenge. Eine Klausel R heißt **Resolvent** von $F \Leftrightarrow_{df}$ es gibt zwei Klauseln K_1 und K_2 in F und es gibt ein Literal L mit der Eigenschaft $L \in K_1$ und $\overline{L} \in K_2$ und es gilt $R = (K_1 \backslash \{L\}) \cup (K_2 \backslash \{\overline{L}\})$.

Schreibweise: help: das Bild hier zeigt K1 und K2 über und verbunden mit R
Dies symbolisiert die einzige Regel des Kalküls.

Beispiel 1.12
$K_1 = \{A_1, \neg A_2, A_3, A_4\},\ K_2 = \{\neg A_1, A_2, A_3, A_5, A_6\}$
K_1 und K_2 liefern $R' = \{\neg A_2, A_3, A_4, A_2, A_5, A_6\}$ und $R'' = \{A_1, A_3, A_4, \neg A_1, A_5, A_6\}$

Für die Anwendung der Resolutionsregel gibt es eine besondere Situation:
zwei Klauseln der Gestalt: $K_1 = \{L\}$ und $K_2 = \{\overline{L}\}$ liefern $R = \{L \backslash \{L\}\} \cup \{\overline{L} \backslash \{\overline{L}\}\} = \varnothing$

Die leere Resolution ist das Ergebnis eines solchen Resolutionsschrittes und nur in dieser Situation tritt die leere Menge auf.

Eine Belegung β ist Modell von F gdw. β Modell von allen Klauseln von F ist.

Falls in F zwei Klauseln $K_1 = \{L\}$ und $K_2 = \{L\}$ vorkommen, dann ist kein β Modell von K_1 und K_2 und damit kein β Modell von F. (F unerfüllbar)

Dies bedeutet: der leere Resolvent ist ein Indiz für die Unerfüllbarkeit.

Satz 1.9
Es sei F gegeben als Klauselmenge und es sei R ein Resolvent von F. Dann gilt:

$$F \models\!\models F \cup \{R\}$$

Beweis:
es genügt z. z.:

1. $F \models F \cup \{R\}$
2. $F \cup \{R\} \models F$ (klar: $Y \models X$ für jede $X \subseteq Y$)

zu 1: (klar ist: $F \models F$)
es genügt z. z.:

$$F \models R$$

Es seien $K_1, K_2 \in F$ mit $L \in K_1$ und $\overline{L} \in K_2$ und $R = (K_1 \backslash \{L\}) \cup (K_2 \backslash \{\overline{L}\})$

Es sei β ein Modell von F und damit von K_1 und K_2.

1. Fall β ist Modell von L. Dann ist β kein Modell von $\overline{L}$, aber von K_2 und damit auch von $K_2 \backslash \{\overline{L}\}$ und damit von R.

2. Fall β ist kein Modell von L, aber von K_1 und damit von $(K_1 \backslash \{L\})$ und von R. ∎

Definition 1.11
Es sei F eine Klauselmenge.

a Dann ist $Res(F) := F \cup \{R | R \text{ ist Resolvent zweier Klauseln von } F\}$

b Wir definieren induktiv für alle $k \in \mathbb{N}$:

$$Res^0(F) := F$$
$$Res^{k+1}(F) := Res(Res^k(F)$$

c Wir definieren die **Resolutionshülle**

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

Kommentare:

1. $Res^k(F)$ ist für alle K definiert und es gilt
   a) $Res^0 = F$ und
   b) $Res^1(F) = Res(F)$ und
   c) $Res^0(F) \subseteq Res^1(F) \subseteq \ldots \subseteq Res^*(F)$
2. Das Resolutionslemma liefert: $F \models\!\models Res(F)$ und damit $F \models\!\models Res^0(F) \models\!\models Res^1(F) \models\!\models \ldots \models\!\models Res^*(F)$
   Das heißt insbesondere F ist unerfüllbar gdw. die Resolutionshülle $Res^*(F)$ ist unerfüllbar.
3. Die Resolutionshülle $Res^*(F)$ besitzt die char. Eigenschaften eines Hüllenoperators:
   a) $F \subseteq Res^*(F)$ Einbettung
   b) $F \subseteq G \rightarrow Res^*(F) \subseteq Res^*(G)$ Monotonie
   c) $Res^*(Res^*(F)) = Res^*(F)$ Abgeschlossenheit

   Lemma 1.2
4. Falls F eine endliche Klauselmenge ist, dann gibt es ein $k \in \mathbb{N}$, s. d. $Res^{k+1}(F) = Res^k(F)$

   Beweis:
   Es seien $A_1, \ldots, A_n$ die Atome von F.
   Frage: Wieviele Klauseln mit diesen Atomen gibt es höchstens?
   Für eine Klausel K gibt es in Bezug auf ein fixes Atom A_i vier Möglichkeiten:
   a) (nur) A_i kommt in K vor
   b) (nur) $\neg A_i$ kommt in K vor

c) A_i und $\neg A_i$ kommen in K vor

d) weder A_i noch $\neg A_i$ kommen in K vor

Das heißt es gibt höchstens 4^n verschiedene Klauseln mit den Atomen $A_1, \ldots, A_n$.

Der Effekt des Resultierens ist es neue Klauseln zu produzieren. Nach höchstens $k \leq 4^n$ Stufen ist nichts neues mehr zu resultieren.

Das heißt $Res^k(F) = Res^{k+1}(F)$ [Dabei ist $k = 4^n$ eine grobe obere Schranke] ■

5. Folgerung: Für jede endliche Klauselmenge F gilt: es gibt eine stufe k mit $Res^*(F) = Res^k(F)$

   Beweis:
   Es sei $Res^k(F) = Res^{k+1}(F)$.
   Dann gilt:

$$\begin{aligned} Res^{k+2}(F) &= Res(Res^{k+1}(F)) = Res(Res^k(F)) \\ &= Res^{k+1}(F) = Res^k(F) \end{aligned}$$

   Also gilt:

$$Res^0(F) \subseteq \ldots \subseteq Res^k(F) = Res^{k+1}(F) = Res^{k+l}$$

   und damit

$$Res^*(F) = \bigcup_{l=0}^{\infty} Res^l(F) = \bigcup_{l=0}^{k} Res^l(F) = Res^k(F)$$

■

Satz 1.10 (Resolutionssatz der Aussagenlogik)
Es sei F eine beliebige Klauselmenge.

$$F \text{ ist unerfüllbar gdw. } \varnothing \in Res^*(F)$$

Beweis:
wir zeigen I: $\varnothing \in Res^*(F) \rightarrow F$ ist unerfüllbar.

Es sei also $\varnothing \in Res^*(F)$.
Es sei k_0 die kleinste Stufe mit der Eigenschaft $\varnothing \in Res^*(F)$.

Das heißt $\varnothing \notin Res^{k_0-1}(F)$ und beim Übergang von $k_0 - 1$ zu k_0 entstanden.

Also gibt es in $Res^{k_0-1}(F)$ zwei Klauseln K_1 und K_2 der Form $K_1 = \{L\}$ und $K_2 = \{\overline{L}\}$ und help: wieder das Bild der Resolution, das sollte man auch mit Latex bauen können?! K_1 und K_2 sind als Konjunktion unerfüllbar. Dies gilt auch für $Res^{k_0-1}(F)$ und damit auch für $Res^0(F) = F$.

Wir zeigen II: F ist unerfüllbar $\rightarrow \varnothing \in Res^*(F)$

Es sei F eine unerfüllbare Klauselmenge.
o. B. d. A. sei F endlich. (nach Endlichkeitssatz: in jeder unerfüllbaren unendlichen Menge gibt es eine unerfüllbare endliche Menge)

Wir beweisen II durch Induktion über die Anzahl der Atome von F.

Induktionsanfang: $n = 1$: in F kommt (nur) das Atom A_1 vor und F ist unerfüllbar.
Mit A_1 gibt es folgende Klauseln:

$$\{A_1\},\ \{\neg A_1\},\ \{A_1, \neg A_1\}$$

$\{A_1, \neg A_1\}$ kann man nach der Tautologieregel streichen. Also bleiben (höchstens) $\{A_1\}$ und $\{\neg A_1\}$.

Da F unerfüllbar, muss es beide geben. Dann gilt: help: A_1 und $\neg A_1$ resolvieren zu $\varnothing$, also $\varnothing \in Res^*(F)$.

Induktionsschritt:
Induktionsvorraussetzung: Für jede Formel G mit (höchstens) n Atomen $A_1, \ldots, A_n$ gilt: Wenn G unerfüllbar ist, dann ist $\varnothing \in Res^*(G)$.
Induktionsbehauptung: Für jede Formel F mit (höchstens) $n{+}1$ Atomen $A_1, \ldots, A_n, A_{n+1}$ gilt:
Wenn F unerfüllbar ist, dann gilt $\varnothing \in Res^*(F)$.

Induktionsbeweis: Es sei F unerfüllbar und in F kommen (höchstens) $n + 1$ Atome vor. Wir konstruieren zwei neue Klauselmengen:

1. F_1: wir streichen jedes Vorkommen von $\neg A_{n+1}$ in jeder Klausel von F und wir streichen jede Klausel, in der A_{n+1} vorkommt.
   Illustration:

$$(\ldots \vee \neg A_{n+1} \vee \ldots \vee A_3 \vee \ldots) \wedge (\ldots \vee A_{n+1} \vee \ldots \vee A_2 \vee \ldots) \wedge \ldots$$
$$(\ldots \vee 0 \vee \ldots \vee \ldots) \wedge \underbrace{(\ldots \vee 1 \vee \ldots)}_{1} \wedge \ldots$$

2. F_0, dual:

   a) streichen Vorkommen von A_{n+1}

   b) streichen jede Klausel in der $\neg A_{n+1}$ vorkommt

F_1 hat engegengesetzte Streichungen zu F_0.
F_0 und F_1 sind zwei Klauselmengen mit (höchstens) den Atomen $A_1, \ldots, A_n$.

Behauptung: F_0 und F_1 sind unerfüllbar!

Wir zeigen durch indirekten Beweis. Annahme: F_0 hat ein Modell β_0.
Dann definieren wir eine Belegung β_0' für F durch

$$\beta_0(A_i) =_{df} \begin{cases} \beta_0(A_i) & \text{für } i = 1, \ldots, n \\ 0 & \text{für } i = n+1 \end{cases}$$

Alle Klauseln, in denen A_{n+1} vorkommt, werden wahr, da sie in F_0 wahr sind und $w \vee 0 \models\!\!\models w$ gilt.

Alle Klauseln, in denen $\neg A_{n+1}$ vorkommt, werden sofort wahr.

Alle übrigen Klauseln (sehen genauso aus wie in F_0) werden wahr.

Also ist β_0' ein Modell von F.
Nach Vorraussetzung ist aber F unerfüllbar ↯

Also gilt: F_0 ist unerfüllbar. Analog für F_1.

Die Induktionsvorraussetzung liefert:

1. $\varnothing \in Res^*(F_0)$ und
2. $\varnothing \in Res^*(F_1)$

Punkt 1 bedeutet: es gibt eine Folge von Klauseln $K_1, K_2, \ldots, K_l$, so dass gilt: für alle K_i $(1 \leq i \leq l)$ ist entweder K_i ein Element aus F_0 (Startklauseln) oder es gibt zwei Klauseln K_α und K_β mit $\alpha, \beta < i$ und help: Resolution K_α, K_β zu K_i und $K_l = \varnothing$

Punkt 2 bedeutet: es gibt eine Folge von Klauseln $K_1', K_2', \ldots, K_m'$, so dass gilt: für alle K_j' $(1 \leq j \leq m)$ ist entweder $K_j' \in F$ (Startklauseln) oder es gibt zwei Klauseln K_γ' und K_δ' mit $\gamma, \delta < j$ und help: Resolution K_γ, K_δ zu K_j und $K_m = \varnothing$

1. Fall Alle Startklauseln aus $K_1, \ldots, K_l$ sind Klauseln aus F.
Dann sind alle Klauseln aus $K_1, \ldots, K_l$ Elemente aus $Res^*(F)$ und damit $\varnothing \in Res^*(F)$

2. Fall Alle Startklauseln aus $K_1', \ldots, K_m'$ sind Klauseln aus F.
Dann sind alle Klauseln aus $K_1', \ldots, K_m' \in Res^*(F)$ und damit $\varnothing \in Res^*(F)$

3. Fall „Sonst-Fall“ (d. h. Fall 1/2 gelten nicht)
Die Startklauseln aus F_0 sind entstanden durch Streichen aller Vorkommen von A_{n+1}.
Wir betrachten die Folge $\widetilde{K}_1, \widetilde{K}_2, \ldots, \widetilde{K}_l$, die entsteht, wenn zunächst in allen Startklauseln von F_0 dort, wo A_{n+1} gestrichen wurde, A_{n+1} wieder hinzugefügt wird und dann resolviert wird. (z. B. $\widetilde{K}_1 = K_1 \cup \{A_{n+1}\}$ falls A_{n+1} dort gestrichen wurde)
Der Effekt dieses Hinzufügens ist:

$$\widetilde{K}_i = K_i \text{ oder } \widetilde{K}_i = K_i \cup \{A_{n+1}\}$$

Insbesondere gilt: $\widetilde{K}_l = K_l \cup \{A_{n+1}\} = \{A_{n+1}\}$

Analog: Die Startklauseln aus F_1 sind entstanden durch Streichen der Vorkommen von $\neg A_{n+1}$. Wir betrachten die Folge $\widetilde{K}'_1, \ldots, \widetilde{K}'_m$, die entsteht, wenn zunächst in den Startklauseln, in denen $\neg A_{n+1}$ gestrichen wurde, $\neg A_{n+1}$ wieder hinzugefügt wird un danach resolviert wird.
Dies liefert $\widetilde{K}'_m = \{\neg A_{n+1}\}$.
Ein weiterer Resolutionsschritt help: Resolution $\widetilde{K_l}, \widetilde{K}'_m$ zu $\varnothing$ liefert $\varnothing \in Res^*(F)$ ■

Definition 1.12
Es sei F eine endliche (unerfüllbare) Klauselmenge.

Eine **Ableitung** oder **Deduktion** der leeren Klausel $\varnothing$ ist eine Folge $K_1, \ldots, K_l$ von Klauseln, für die gilt: entweder ist $K_i \in F$ (Startklausel) oder es gibt $\alpha, \beta < i$ und help: Resolution K_α, K_β zu K_i

Beispiel 1.13
help: Resolutionsbaum $F = \{\{A, B, C, D\}, \{A, B, C, \neg D\}, \{A, B, \neg C\}, \{A, \neg B\}, \{\neg A\}\}$
jeweils resolviert: $\{A, B, C\},\ \{A, B\},\ \{A\},\ \{\varnothing\}$
Ableitungen: $K_1 = \{A, B, C, D\},\ K_2 = \{A, B, C, \neg D\},\ K_3 = \{A, B, \neg C\},\ K_4 = \{A, \neg B\},\ K_5 = \{\neg A\},\ K_6 = \{A, B, C\},\ K_7 = \{A, B\},\ K_8 = \{A\},\ K_9 = \{\varnothing\}$

Beispiele dieser Art benötigen etwa soviele Schritte wie Atome (linearer Aufwand)
ABER: Es gibt Beispiele, die erfordern expotentiellen Aufwand.

Der Induktionsbeweis liefert folgenden Algorithmus:

Algorithmus von Gilmore

```
n:=0
Res[n]:=F
repeat n:=n+1
   Res[n]:= Res(Res[n-1])
until (∅ ∈ Res[n]) or (Res[n] = Res[n-1])

if (∅ ∈ Res[n])
then return unerfüllbar
else return erfüllbar
```

2 Einführung in die Kombinatorik

Frage: Wie viele Elemente enthält eine gegebene Menge?
Die „*Kunst des Zählens*“

2.1 Elementare Abzählregeln

2.1.1 Summenregel

Gegeben seien a_1 Elemente vom Typ A_1 und a_2 Elemente vom Typ A_2.
Dabei schließen sich diese Typen gegenseitig aus.

Frage: Auf wie viele Weisen lässt sich ein Element vom Typ A_1 oder A_2 wählen?

Antwort: $a_1 + a_2$

Begründung: Bilden

$$M_1 \Leftrightarrow_{df} \{x \mid x \text{ vom Typ } A_1\}$$
$$M_2 \Leftrightarrow_{df} \{y \mid y \text{ vom Typ } A_2\}$$

Dann gilt: $M_1 \cap M_2 = \varnothing$ und es gilt: $\text{card}(M_1 \cup M_2) = \text{card}M_1 + \text{card}M_2$.

Sprechweise: Falls gilt $\text{card}M = n$ für $n \in \mathbb{N}$ dann heißt M n-Menge.

Verallgemeinerung: Die Summenregel gilt für jede endliche Anzahl $k \geq 2$ von Typen.

2.1.2 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 mit der ersten Komponente von A_1 und mit der zweiten Komponente vom Typ A_2 bilden?

Antwort: $a_1 \cdot a_2$

Begründung: Wir betrachten

$$M_1 \times M_2 \Leftrightarrow_{df} \{(x, y) \mid x \in M_1 \text{ und } y \in M_2\}$$

und es gilt: $\operatorname{card} M_1 \times M_2 = \operatorname{card} M_1 \cdot \operatorname{card} M_2 = a_1 \cdot a_2$

Verallgemeinerung: Die Produktregel gilt für jede endliche Anzahl $k \geq 2$ von Typen.

Beispiel 2.1
Wie viele Schriften erlaubt ein gegebener PC?

„Schrift " hat folgende Komponenten:

1. „Schriftart": Arial,...Dies seien 20.
2. „Schriftgröße: ...,12 Pkt,...Dies seien 27.
3. "Schriftsatz„: fett, kursiv, unterstrichen
   Dies sind 3 Komponenten, die unabhänig voneinander gewählt werden können.
   Für jede Komp. gibt es zwei Möglichkeiten: (an/aus) $2 \cdot 2 \cdot 2 \cdot = 8$

Also insgesamt: $20 \cdot 27 \cdot 8$ Möglichkeiten.

Ein zweiter Blick auf die Produktregel als „Entscheidungsbaum".
Wir haben einen k-stufigen Entscheidungsprozess:

1. Stufe: a_1 verschiedene Alternativen
$\vdots$
k. Stufe: a_k verschiedene Alternativen

2.1.3 Gleichheitsregel

Gegeben seien zwei verschiedene Mengen X und Y. Falls es eine Bijektion zwischen diesen beiden Mengen gibt, dann gilt: $\operatorname{card} X = \operatorname{card} Y$.

Beispiel 2.2
Gegeben sei die Menge $M = \{x_1, \ldots, x_m\}$ (also ist M eine m-Menge) und wir definieren

$$X =_{df} \left\{ f \mid f \colon M \mapsto \{0,1\} \right\} = \{0,1\}^M$$

Es gilt:

$$\operatorname{card} M = \operatorname{card}\{0,1\}^M = (\operatorname{card}\{0,1\})^{\operatorname{card} M} = 2^m$$

Wir betrachten nun $Y =_{df} \{N \mid N \subseteq M\} = \mathcal{P}(M)$.

Behauptung: Es gibt eine Bijektion φ von X und Y.

Folgerung: $\operatorname{card}(\mathcal{P}) = \operatorname{card}(\{0,1\}^M) = 2^{\operatorname{card} M} = 2^m$

Wir definieren: $\varphi(N) =_{df} \psi_N \quad (N \subseteq M)$
Dabei ist $\psi_N(x) =_{df} \begin{cases} 1 & \text{falls } x \in N \\ 0 & \text{falls } x \notin N \end{cases}$ die **charakteristische Funktion** von N.

Es gilt: Definitionsbereich $D_\varphi = \mathcal{P}(M)$, $\psi_N \in \{0,1\}^M$

Bleibt zu zeigen: φ inj. und surj.

1. φ injektiv: $\varphi(N_1) = \varphi(N_2) \Rightarrow N_1 = N_2$

   Es sei also $\varphi(N_1) = \varphi(N_2)$. Dann gilt:

   $$x \in N_1 \leftrightarrow \psi_{N_1}(x) = 1 \leftrightarrow \psi_{N_2}(x) = 1 \leftrightarrow x \in N_2$$

2. φ surjektiv: für jedes $f \in \{0,1\}^M$ gibt es ein $N \in \mathcal{P}(M)$ mit $\varphi(N) = f$.

   Es sei also $f \in \{0,1\}^M$.
   Wir definieren $N := \{x \mid x \in M \text{ und } f(x) = 1\} =: f^{-1}(1)$

   Damit gilt: $f(x) = 1 \leftrightarrow x \in f^{-1}(1) \leftrightarrow x \in N \leftrightarrow \psi_N(x) = 1$

   Also gilt: $\varphi(N) = \psi_N = f$

2.1.4 Regel vom zweifachen Abzählen

Gegeben seien eine n-Menge $A = \{a_1, \ldots, a_n\}$ und eine m-Menge $B = \{b_1, \ldots, b_m\}$ und eine binäre Relation $R \subseteq A \times B$ zwischen A und B.

Ferner sei $r(a_i)$ die Anzahl der Elemente aus B, die mit a_i in Relation stehen; und es sei $r(b_j)$ die Anzahl der Elemente aus A, die mit b_j in Relation stehen.

$$\begin{aligned} r(a_j) &= \text{card}\{(a_i, b) \mid (a_i, b) \in R\} \\ &= \text{card}\{b \mid b \in B \wedge (a_i, b) \in R\} \\ r(b_j) &= \text{card}\{a \mid a \in A \wedge (a, b_j) \in R\} \end{aligned}$$

Begründung: Darstellung als Rechteckschema:

	b_1	b_2	$\ldots$	b_j	$\ldots$	b_m
a_1	1	0	$\ldots$	1	$\ldots$	0
$\vdots$			$\vdots$		$\vdots$	
a_i	0	0	$\ldots$	1	$\ldots$	0
$\vdots$			$\vdots$		$\vdots$	
a_n	1	1	$\ldots$	0	$\ldots$	0

$r(a_1)$: Anzahl Einsen in der ersten Zeile,
$r(a_i)$: Anzahl Einsen in Zeile i,
$r(b_j)$ analog.

Einträge:

$$m_{ij} = 1 \leftrightarrow (a_i, b_j) \in R$$
$$m_{ij} = 0 \leftrightarrow (a_i, b_j) \notin R$$

Dann gilt: $\sum_{i=1}^{n} r(a_i) = \sum_{j=1}^{m} r(b_j)$

Beispiel 2.3
$A = B = \{1, 2, \ldots, 10\}$ und R als R als Teilerrelation.

$$(i, j) \in R \leftrightarrow i \setminus j$$

Frage: Wie sieht dann das Rechteckschema aus?
Frage: Wie viele Teiler hat eine nat. Zahl im Mittel?

	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2		1		1		1		1		1
3			1			1			1	
4				1				1		
5					1					1
6						1				
7							1			
8								1		
9									1	
10										10

$\underline{t(j)}$	1	2	2	3	2	4	2	4	3	4
$\overline{t(j)}$	1	3/2	5/3	8/4	10/5	14/6	16/7	20/8	23/9	27/10

$\underline{t(j)}$ - Anzahl der Teiler von j
$\overline{t(j)}$ - Anzahl der Teiler von j im Mittel

$$\overline{t(n)} = 1/n \sum_{j=1}^{n} t(j)$$

$t(j)$ ist völlig unregelmäßig.
$t(prim) = 2$,
$t(2^k) = k + 1$

Blick auf die Zeilen:
in Zeile i stehen an den Stellen $1 \cdot i, 2 \cdot i, 3 \cdot i, \ldots$ solange bis $k \cdot i \leq n$: das größte k ist $k = \frac{n}{\lfloor i \rfloor}$
d. h. $r(i) = \frac{n}{\lfloor i \rfloor}$ und es gilt:

$$\overline{t(n)} = 1/n \cdot \sum_{j=1}^{n} t(j) = 1/n \cdot \sum_{i=1}^{n} r(i) = 1/n \cdot \sum_{i=1}^{n} \frac{n}{\lfloor i \rfloor}$$

für das größte ganze $\lfloor x \rfloor$ gilt:

$$x - 1 < \lfloor x \rfloor \leq x$$

also gilt $\lfloor x \rfloor \sim x$ und der Fehler ist kleiner als 1.

Also:

$$1/n \cdot \sum_{i=1}^{n} n/\lfloor i \rfloor = 1/n \cdot \sum_{i=1}^{n} n/i = 1 \cdot \sum_{i=1}^{n} 1/i := \ H_n$$

H_n wird als n-te harmonische Zahl bezeichnet und es gilt $H_n \sim \ln n$

2.1.5 Kominatorische Grundaufgaben

Wiederholung	Reihenfolge wird berücksichtigt	Reihenfolge wird n. b.
Elemente einfach	Permutation ohne Wiederholung	Kombination o. W.
Elemente mehrfach	Permutation mit Wiederholung	Kombination m. W.

„Denkmodelle“ erweisen sich als hilfreich in der Kombinatorik.

Wir untersuchen:

Urnenmodell aus einem Gefäß werden Kugeln gezogen

Schubfachmodell auf vorhandene Schubfächer werden Gegenstände verteilt

2.1.6 Ermittlung der Zahlenwerte

Permutation ohne Wiederholung (o. W.)

Gegeben sei eine n-Menge N.

Eine r-Permutation o. W. der n-Menge N ist $\Leftrightarrow_{df}$ ein r-Tupel ($\rightarrow$ Reihenfolge) verschiedener Elemente ($\rightarrow$ o. W.) aus N.

$P(n, r)$ bezeichnet die Anzahl der r-Permutationen einer n-Menge ($1 \leq r \leq n$)

Satz 2.1

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

Beweis: (Anwendung der Produktregel, r-stufiger Entscheidungsprozess)
1. Stufe: Wähle ein Element aus N: n-Möglichkeiten
2. Stufe: Wähle ein Element aus N: $(n-1)$-Möglichkeiten
$\vdots$
r. Stufe: Wähle ein Element aus N: $(n-r+1)$-Möglichkeiten ∎

Speziell gilt: $P(n,n) = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n!$

Damit gilt:

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

Außerdem legen wir fest:

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

heißt **fallende Faktorielle**.

Permutation mit Wiederholung (m. W.)

Eine r-Permutation m. W. einer n-Menge ist $\Leftrightarrow_{df}$ ein r-Tupel ($\rightarrow$ Reihenfolge) von (beliebigen, $\rightarrow$ m. W.) Elementen aus N (d. h. ein Element von $\underbrace{N \times \ldots \times N}_{r\text{-Mal}} =: N^r$.

Satz 2.2
Die Anzahl der r-Permutationen m. W. einer n-Menge beträgt n^r.

Beweis:
Wieder Produktregel mit r-stufigem Entscheidungsprozess. Auf jeder Stufe hat man n Möglichkeiten. ∎

Kombination ohne Wiederholung (o. W.)

Gegeben sei eine n-Menge N.

Eine r-Kombination o. W. von N ist $\Leftrightarrow_{df}$ r-Teilmenge ($\rightarrow$ Reihenfolge) von N.

$C(n,r)$ bezeichnet die Anzahl der r-Kombinationen o. W. einer n-Menge $(1 \leq r \leq n)$!

Satz 2.3

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

Beweis:
Zusammenhang zw. $C(n,r)$ und $P(n,r)$: Jede r-Teilmenge liefert $P(r,r) = r!$ verschiedene r-Tupel verschiedener Elemente aus N.

Also gilt: $C(n,r) \cdot r! = P(n,r)$

Also: $C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{(n-r)!\,r!}$ ∎

Wir legen fest:

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

heißt **Binomialkoeffizient**.

Kombination mit Wiederholung (m. W.)

In jeder Menge spielt weder die Reihenfolge noch die Vielfachheit ihrer Elemente eine Rolle.

z. B.: $\{1,2,3\} = \{3,2,1\} = \{1,2,2,3,3,3\}$

In einer sog. **Multi-Menge** spielt die Vielfachheit eine Rolle:
$\{1,2,3\} \neq \{1,2,2,3,3,3\} \neq \{1,1,2,2,3,3\}$

Das heißt in einer Multi-Menge wird die Vielfachheit der Elemente gezählt (aber nicht die Reihenfolge berücksichtigt)

Eine r-Kombination m. W. einer n-Menge $N \Leftrightarrow_{df}$ eine r-Multiteilmenge der Menge N.

Satz 2.4
Die Anzahl der r-Kombinationen m. W. einer n-Menge ist

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

Beweis: (Gleichheitsregel)
1. Variante

Es sei X die Menge aller r-Kombinationen m. W. einer gegebenen n-Menge $N = \{1,2,\ldots,n\}$

Ferner sei Y die Menge aller r-Teilmengen der Menge $\{1,2,\ldots,n,n+1,\ldots,n+r-1\}$

Damit ist klar: $\operatorname{card} Y = \binom{n+r-1}{r}$
(gemäß obiger Abschnitt, Kombination o. W.)

Behauptung: Es gibt eine Bijektion zwischen X und Y!

Schreibweise: Es sei $\{a_1, a_2, \ldots, a_r\} \in X$

o. B. d. A. sei $1 \leq a_1 \leq a_2 \leq \ldots \leq a_r \leq n$
Dies beschreiben wir durch

$$\{a_1 \leq a_2 \leq \ldots \leq a_r\}$$

Wir definieren eine Abbildung, die als Elemente des Definitionsbereiches solche Objekte hat.

Die Elemente des Wertebereiches sind gewöhnliche r-Teilmengen von $\{1,2,\ldots,n+r-1\}$

Es sei $\varphi(\{a_1 \leq a_2 \leq \ldots \leq a_r\}) =_{df} \{a_1 < a_2 + 1 < a_3 + 2 < \ldots < a_r + (r-1)\}$, definiert für $\{a_1 \leq \ldots \leq a_r\} \in X$.

Wir halten fest:

- dies ist eine (Multi)Menge mit r Elementen für die gilt $1 \leq a_1$ und $a_r \leq n + (r-1)$
- da $a_i \leq a_{i+1}$, folgt $a_i + (i-1) < a_{i+1} + i$

Also ist $\{a_1 < a_2 + 1 < \ldots < a_r + (r-1)\} \in Y$

Es bleibt zu zeigen, dass die Abbildung φ zwischen X und Y bijektiv ist.

Dies realisieren wir durch die Angabe einer Umkehrabbildung γ Y nach X.

Es sei $\gamma(\{b_1 < b_2 < \ldots < b_r\}) =_{df} \{b_1 \leq (b_2 - 1) \leq (b_3 - 2) \leq \ldots \leq (b_r - (r-1))\}$, definiert für $\{b_1 < b_2 < \ldots < b_r\} \in Y$.

Wir halten fest:

- $1 \leq b_1$ und $b_r - (r-1) \leq n + r - 1 - (r-1) \leq n$
- da $b_i < b_{i+1}$ folgt $b_i - (i-1) \leq b_{i+1} - i$

Und es gilt: $\varphi \circ \gamma = Id_x$ und $\gamma \circ \varphi = Id_y$

2. Variante: Wir beschreiben die r-Multimenge von N durch eine geeignete Codierung. Dazu benötigen wir ein Alphabet mit zwei Buchstaben

$$\Sigma = \{|,\ *\}$$

Dabei ist $*$ein Platzhalter für die Vielfachheiten der Elemente und | codiert die Elemente von N auf folgende Weise:
vor dem i-ten Strich steht das Element n. Beispiel:

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

Dies sind 3 verschiedene 6-Multimengen von N.

Zur Codierung benötigen wir: 6-mal $*$als Platzhalter und $(5-1)$-mal | als Trennungssymbol.

$$*|**|***|,\ **|**|**||,\ |||******$$

Diese codierung ist eindeutig, d. h. wir haben eine bij. Zuordnung zwischen den r-Multimengen und diesen Codewörtern.

Wie viele derartige Codewörter gibt es?
r-mal $*$ und $(m-1)$-mal | bedeutet: $n + r - 1$ Buchstaben.

Es gibt genauso viele Codewörter, wie es Möglichkeiten gibt, r-mal $*$ auf $n + r - 1$ Plätze zu verteilen.

Hierfür gilt gerade: $\binom{n+r-1}{r}$ Möglichkeiten. ∎

2.2 Binominalkoeffizienten

Satz 2.5 (Elementare Eigenschafte)

$$\binom{n}{r} = \binom{n}{n-r} \qquad \text{(Symetrie)} \tag{2.1}$$

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r} \qquad \text{(Rekursion)} \tag{2.2}$$

Beweis:
zu Gleichung 2.1 zwei Varianten:

1. Variante: per Rechnung

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

2. Variante: per Gleichheitsregel

Es gibt eine bijektive Zuordnung zwischen den r-Teilmengen A von N und den $(n-r)$-Teilmengen B von N durch $B = N - A = \overline{A}$
und deshalb gilt: $\binom{n}{r} = \binom{n}{n-r}$ (ohne Rechnen)

zu Gleichung 2.2 zwei Varianten:

1. Variante: per Rechnung - durch vollständige Induktion

2. Variante: mit Gleichheitsregel

Ausgangspunkt sei eine n-Menge N.

Wir fixieren ein Element $a_0 \in N$ und wir klassifizieren die r-Teilmengen von N danach, ob sie a_0 enthalten oder nicht.

1. Frage: Wie viele r-Teilmengen gibt es, die a_0 enthalten?
So viele, wie es $(r-1)$-Teilmengen einer $(n-1)$-Menge gibt, also $\binom{n-1}{r-1}$

2. Frage: Wie viele gibt es, die a_0 nicht enthalten?
So viele, wie es r-Teilmengen einer $(n-1)$-Menge gibt, also $\binom{n-1}{r}$.

Die Summenregel liefert:
es gibt $\binom{n-1}{r-1} + \binom{n-1}{r}$ r-Teilmengen von N. ∎

Diese Eigenschaften liefern die Darstellung der Binomialkoeffizienten im **PASCALschen Dreieck**. help: Bild mit pascaldreieck bis 3 fehlt

Beobachtung:

- $\binom{n}{n} = \binom{n}{0} = 1$
- $\binom{n}{1} = \binom{n}{n-1} = n$

Frage: Woher kommt die Bezeichnung „Binominalkoeffizient“?

Satz 2.6 (Binomischer Satz)

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} \underbrace{x^{n-r} y^r}_{\text{Binom}}$$

Beweis:
zwei Varianten:

1. Variante: per Rechnung - vollständige Induktion

2. Variante: mit Gleichheitsregel - Übersetzung in ein Schubfachmodell

linke Seite: Produkt aus Summen: n-mal den Term $(x+y)$ ($\rightarrow$ n Schubfächer).

Das Distributivgesetz liefert durch Ausmultiplizieren eine Summe von Produkten der Form $x^a y^b,\ a+b=n$. Dies schreiben wir als $x^{n-r}y^r$. (Dies sind die Summanden der rechten Seite)

Frage: Wie oft kommt der Summand $x^{n-r}y^r$ vor?
So oft, wie es Möglichkeiten gibt, sich in n Schubfächern r-mal für y zu entscheiden (und damit $(n-r)$-mal für x in den restlichen Fächern). Diese Anzahl ist $\binom{n}{r}$. ∎

2.2.1 Spezialfälle

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

   Dies ist gerade die Zeilensumme im Pascalschen Dreieck. Sie besagt: die Anzahl der Teilmengen einer n-Menge klassifiziert nach der Kardinalität der Teilmengen ist gemäß Summenregel 2^n.

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

   Dies entspricht:

   $$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots$$

   Dies bedeutet: für jede n-Menge gibt es genau so viele Teilmengen mit gerader Kardinalität, wie mit ungerader, also jeweils 2^{n-1}.

3.

$$x = 1,\ y = x \qquad \to (1+x)^n = \underbrace{\sum_{r=0}^{n} \binom{n}{r} x^r}_{\text{Polynom aus Binominialkoeff.}}$$

Also sind in diesem Term alle Informationen über diese Binominialkoeffizienten „codiert“.
Deshalb heißt die Funktion $f(x) = (1+x)^n$ **erzeugende Funktion** für die Binominialkoeffizienten.

Spaltensummen des PASCALschen Dreiecks:
eine Möglichkeit: wir betrachten

$$\binom{r}{r}, \binom{r+1}{r}, \ldots, \binom{m}{r}$$

Dies sind die Spalten „von rechts oben nach links unten“ bis zu einer vorgegebenen Zeile m.
Kurz:

$$\sum_{i=r}^{m} \binom{i}{r}$$

Vereinbarung: $\binom{i}{r} := 0,$ falls $i < r$

Damit ist $\sum_{i=0}^{m} \binom{i}{r}$ sinnvoll.

Satz 2.7 (Spaltensumme - obere Summation)

$$\sum_{i=0}^{m} \binom{i}{r} = \binom{m+1}{r+1}$$

Beweis:

$$\begin{aligned}
\sum_{i=0}^{m} \binom{i}{r} &= \underbrace{\binom{0}{r} + \ldots + \binom{r-1}{r}}_{0} + \binom{r}{r} + \binom{r+1}{r} + \ldots + \binom{m}{r} \\
&= \binom{r+1}{r+1} + \binom{r+1}{r} + \ldots + \binom{m}{r} \\
&= \binom{r+2}{r+1} + \binom{r+2}{r} + \ldots + \binom{m}{r} \\
&\vdots \\
&= \binom{m}{r+1} + \binom{m}{r} \\
&= \binom{m+1}{r+1}
\end{aligned}$$

■

eine zweite Möglichkeit:
sind die Spalten „von links oben nach rechts unten“:

$$\binom{r}{0}, \binom{r+1}{1}, \ldots, \binom{r+i}{i}, \ldots, \binom{r+m}{m}$$

bis zur Zeile $(r+m)$.

Satz 2.8 (Spaltensumme - paralelle Summation)

$$\sum_{i=0}^{m} \binom{r+i}{i} = \binom{r+m+1}{m}$$

Beweis:

1. benutzt Symmetrie
2. Rekursion analog zur oberen Summation

■

2.2.2 Produkte der Binominialkoeffizienten

Als Beispiel der folgende

Satz 2.9 (Vandermonsche Identität)

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k} \binom{n}{r-k}$$

Beweis: (ohne Rechnung - wir suchen ein passendes Modell)
Wir betrachten eine m-Menge M und eine n-Menge N, mit $M \cap N = \varnothing$ (M, N disjunkt)

z. B.: $M = \{a_1, \ldots, a_m\},\ N = \{b_1, \ldots, b_n\}$

linke Seite: $\binom{m+n}{r}$ ist die Anzahl der r-Teilmengen von $M \cup N$,card$(M \cup N) = m + n$

rechte Seite: wir klassifizieren die r-Teilmengen von $M \cup N$ nach der Anzahl k der Elemente in M.

0. Stufe kein Element aus M: $\binom{m}{0}$
diese werden durch die fehlenden $(r-0)$ Elemente aus N ergänzt: $\binom{n}{r}$.
Die Produktregel liefert: $\binom{m}{0}\binom{n}{r}$ Möglichkeiten eine r-Teilmenge von $M \cup N$ auszuwählen, die 0 Elemente aus M beinhaltet.

k. Stufe k Elemente aus M: $\binom{m}{k}$
dazu $r-k$ Elemente aus N: $\binom{n}{r-k}$
Produktregel: $\binom{m}{k}\binom{n}{r-k}$ Möglichkeiten

Summenregel:

$$\sum_{k=0}^{r} \binom{m}{n} \binom{n}{r-k}$$

als Anzahl der r-Teilmengen von $M \cup N$. ∎

2.2.3 Multinomialkoeffizienten

haben: Symmetrie $\binom{n}{r} = \binom{n}{n-r}$.

Dies läßt sich auch so schreiben:

$$\binom{a+b}{a} = \binom{a+b}{b}$$

Dies rechtfertigt die folgende Schreibweise:

$$\binom{a+b}{a,b} := \frac{(a+b)!}{a! \cdot b!} = \binom{a+b}{a} = \binom{a+b}{b}$$

Eine formale Analogie liefert folgende

Definition 2.1 (Trinominalkoeff.)

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

Satz 2.10 (Trinomialsatz)

$$(x+y+z)^n = \sum_{a+b+c+n} \binom{a+b+c}{a,b,c} x^a y^b z^c$$

Definition 2.2 (Multinomialkoeff.)

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

Satz 2.11 (Multinomialsatz)

$$(x_1+x_2+\ldots+x_k)^n = \sum_{a_1+a_2+\ldots+a_k=n} \binom{a_1+a_2+\ldots+a_k}{a_1,\ldots,a_k} x_1^{a_1} \cdot \ldots \cdot x_k^{a_k}$$

Beweis:

$$\begin{aligned}
\binom{a_1+a_2+\ldots+a_k}{a_1,a_2,\ldots,a_k} &= \frac{(a_1+a_2+\ldots+a_k)!\,(a_1+a_2+\ldots+a_k)!}{a_1! \cdot a_2! \ldots a_k!\,(a_1+a_2+\ldots+a_k)!} \\
&= \frac{(a_1+a_2+\ldots+a_k)!}{a_1!\,(a_2+\ldots+a_k)} \cdot \frac{(a_2+\ldots+a_k)!}{a_2! \ldots a_k!} \\
&= \underbrace{\binom{a_1+a_2+\ldots+a_k}{a_2+\ldots+a_k}}_{(1)} \cdot \underbrace{\binom{a_2+\ldots+a_k}{a_2,\ldots,a_k}}_{(2)}
\end{aligned}$$

(1): Anzahl der Möglichkeiten aus n Termen der Form $(x_1+\ldots+x_n)$ genau a_1 -mal x_1 auszuwählen
(2): Anzahl der Möglichkeiten aus den restlichen $(n-a_1)$ Termen irgendwie $x_1, x_2, \ldots, x_k$ auszuwählen, aber insgesamt genau $(a_2+\ldots+a_n)$-mal

Eine Rekursion liefert:

$$= \binom{a_1+a_2+\ldots+a_k}{a_2+\ldots+a_k} \cdot \binom{a_2+a_3+\ldots+a_k}{a_3+\ldots+a_k} \cdot \binom{a_3+\ldots+a_k}{a_4+\ldots+a_k} \ldots \binom{a_{k-1}+a_k}{a_k} \quad \blacksquare$$

eine weitere Anwendung des Binominialkoeff.:

2.2.4 geordnete Zahlpartitionen

z. B. ist $1+1+1+2+2+3 = 10$ eine geordnete 6-Partition von 10.

Schreibweise: Für positive nat. Zahlen $a_1, \ldots, a_r$ und n ist

$$a_1 + a_2 + \ldots + a_r = n$$

eine geordnete r-Partition von n. Also ist $3+2+2+1+1+1 = 10$ eine weitere r-Partition von 10.

Frage: Wie viele r-Partitionen von n gibt es?

Satz 2.12
Die Anzahl der geordneten r-Partitionen von n beträgt $\binom{n-1}{r-1}$.

Beweis: (Mithilfe der Gleichheitsregel)
X sei die Menge der geordneten r-Partitionen von n (die Elemente von X schreiben wir als $a_1 + a_2 + \ldots + a_r = n$)

Y sei die Menge der $(r-1)$-Teilmengen der Menge $\{1, \ldots, n-1\}$

wissen: $\operatorname{card} Y = \binom{n-1}{r-1}$

wir definieren folgende Abbildung:

$$\varphi(a_1 + a_2 + \ldots + a_r = n) =_{df} \{a_1, a_1 + a_2, a_1 + a_2 + a_3, \ldots, a_1 + a_2 + \ldots + a_r\}$$

Hierfür gilt:

1. X ist der Definitionsbereich von φ
2. φ bildet nach Y ab, denn es gilt:
   $\underbrace{1 \leq a_1 < a_1 + a_2 < a_1 + a_2 + a_3 < \ldots < a_1 + \ldots + a_{r-1} \leq n-1}_{(r-1)\text{-Teilmenge von } Y}$

es bleibt zu zeigen: φ ist bijektiv.

Dies zeigen wir durch Angabe einer Umkehrabbildung σ:

$$\sigma(\{b_1, \ldots, b_{r-1}\}) =_{df} b_1 + (b_2 - b_1) + \ldots + (b_{r-1} - b_{r-2}) + (n - b_{r-1})$$
$$\varphi \circ \sigma = Id_X, \qquad \sigma \circ \varphi = Id_Y$$

■

2.3 Das Prinzip der Inklusion und Exklusion

Aufgabe: Bekannt ist, dass die PIN-Codes von EC-Karten aus 4 Ziffern $\{0, 1, \ldots, 9\}$ bestehen. Wie viele Codes gibt es, die eine Ziffer (1) und eine Ziffer (2) und eine Ziffer (3) enthalten?

Es sei $Z = \{0, 1, \ldots, 9\}$

Z^r bezeichnet die Menge aller Wörter der Länge r mit Buchstaben aus Z. Dabei ist Z das zugrundeliegende Alphabet

$$Z^r = \{z_1 z_2 \ldots z_r \mid 1 \leq i \leq r : z_i \in Z\}$$

am Beispiel: $Z^4 = \{z_1 z_2 z_3 z_4 \mid z_1, z_2, z_3, z_4 \in Z\}$

$$D_1^r = \{z_1 \ldots z_r \in Z^r \mid \text{ für ein } i \in \{1, \ldots, r\} \text{ gilt } : z_i = 1\}$$

entsprechend D_2^r und

$$D_3^r = \{z_1 \ldots z_r \in Z^r \mid \text{ für ein } i \in \{1, \ldots, r\} \text{ gilt } : z_i = 3\}$$

Bemerkung: „es gibt eine Ziffer“ wird stets gebraucht wie in $\exists z_1$ (also „es gibt min. eine Ziffer. . .“)

Gesucht ist also folgende Anzahl: $\text{card}(D_1^r \cap D_2^r \cap D_3^r)$

Der nächste Schritt:

$$M_1^r =_{df} \{z_1 \ldots z_r \in Z^r \mid \text{ für alle } i \in \{1, \ldots, r\} \text{ gilt: } z_i \neq 1\}$$

gilt: $M_1^r = Z^r \backslash D_1^r$. Entsprechend werden M_2^r und M_3^r definiert.

Für diese Mengen gilt:

$$\begin{aligned} D_1^r \cap D_2^r \cap D_3^r &= (Z^r \backslash M_1^r) \cap (Z^r \backslash M_2^r) \cap (Z^r \backslash M_3^r) \\ &= Z^r \backslash (M_1^r \cup M_2^r \cup M_3^r) \end{aligned}$$

Es genügt also $\text{card}(M_1^r \cup M_2^r \cup M_3^r)$ zu bestimmen. (card Z^r bekannt)

1. Versuch:

$$\text{card}(M_1^r \cup M_2^r \cup M_3^r) = \text{card}\, M_1^r + \text{card}\, M_2^r + \text{card}\, M_3^r$$

wäre korrekt, wenn $M_{1|2|3}^r$ disjunkt wären. (Was nicht der Fall ist)

2. Versuch:

$$\begin{aligned} \text{card}(M_1^r \cup M_2^r \cup M_3^r) = &\text{card}\, M_1^r + \text{card}\, M_2^r + \text{card}\, M_3^r \\ &- \text{card}(M_1^r \cap M_2^r) - \text{card}(M_1^r \cap M_3^r) - \text{card}(M_2^r \cap M_3^r) \end{aligned}$$

Fehlerhaft für alle $z_1z_2z_3z_4$ mit $\forall i\ z_i \neq \{1,2,3\}$

3. Versuch:

$$\begin{aligned}\operatorname{card}(M_1^r \cup M_2^r \cup M_3^r) = &\operatorname{card} M_1 + \operatorname{card} M_2^r + \operatorname{card} M_3^r \\ &- \operatorname{card}(M_1^r \cap M_2^r) - \operatorname{card}(M_1^r \cap M_3^r) - \operatorname{card}(M_2^r \cap M_3^r) \\ &+ \operatorname{card}(M_1^r \cap M_2^r \cap M_3^r)\end{aligned}$$

Behauptung: Antwort 3 ist korrekt!

Begründung mit Fallunterscheidung nach der Zugehörigkeit zur Menge:

1. Fall: Codewort gehört zu genau einer der Mengen M_1^r, M_2^r, M_3^r (z. B. $z_1z_2 \ldots z_r \in M_1^r$, aber $z_1 \ldots z_r \notin M_2^r$ und $z_1 \ldots z_r \notin M_3^r$)
links (LGS): einmal gezählt
rechts (RGS): einmal gezählt

2. Fall: Codewort gehört zu genau zwei der Mengen
LGS: einmal gezählt
RGS: zweimal addiert, einmal subtrahiert

3. Fall: Codewort gehört zu allen Mengen
LGS: einmal gezählt
RGS: dreimal addiert, dreimal subtrahiert, einmal addiert

Für unser Beispiel gilt:

$$\begin{aligned}\operatorname{card} M_k^r &= 9^r \qquad k = 1,2,3 \\ \operatorname{card}(M_k^r \cap M_j^r) &= 8^r \qquad k \neq j,\ j \in 1,2,3 \\ \operatorname{card}(M_k^r \cap M_j^r \cap M_i^r) &= 7^r\end{aligned}$$

Damit ist:

$$\operatorname{card}(M_1^r \cup M_2^r \cup M_3^r) = 3 \cdot 9^r - 3 \cdot 8^r + 7^r$$

und damit

$$\operatorname{card}(D_1^r \cap D_2^r \cap D_3^r) = 10^r - 3 \cdot 9^r + 3 \cdot 8^r - 7^r$$

Verallgemeinerung der Aufgabenstellung:

Gegeben seien n Mengen $M_1, \ldots, M_n$ über dem Grundbereich U (jede Menge M_i ist durch eine Eigenschaft E_i definiert)

Aufgabe: Bestimme $\operatorname{card}(M_1 \cup \ldots \cup M_n)$!

Wir definieren folgende Größen:

$$
\begin{aligned}
S_1 &=_{df} \operatorname{card} M_1 + \operatorname{card} M_2 + \ldots + \operatorname{card} M_n = \sum_{i=1}^{n} \operatorname{card} M_i \\
S_2 &=_{df} \operatorname{card}(M_1 \cap M_2) + \operatorname{card}(M_1 \cap M_3) + \ldots + \operatorname{card}(M_1 \cap M_n) \\
&\qquad + \operatorname{card}(M_2 \cap M_3) + \ldots + \operatorname{card}(M_2 \cap M_n) \\
&\qquad\quad \ddots \\
&\qquad\qquad + \operatorname{card}(M_{n-1} \cap M_n) \\
&= \sum_{1 \le i_1 < i_2 \le n} \operatorname{card}(M_{i_1} \cap M_{i_2}) \\
S_3 &=_{df} \sum_{1 \le i_1 < i_2 < i_3 \le n} \operatorname{card}(M_{i_1} \cap M_{i_2} \cap M_{i_3}) \\
S_j &=_{df} \sum_{1 \le i_1 < \ldots < i_j \le n} \operatorname{card}(M_{i_1} \cap \ldots \cap M_{i_j}) \\
S_n &=_{df} \operatorname{card}(M_1 \cap \ldots \cap M_n) \\
S_{Gesamt} &=_{df} \operatorname{card} U \\
S_* &=_{df} \operatorname{card}(M_1 \cup M_2 \cup \ldots \cup M_n) \\
S_0 &=_{df} \operatorname{card}(\overline{M_1} \cap \overline{M_2} \cap \ldots \cap \overline{M_n}) \qquad (\overline{M_i} = U \backslash M_i)
\end{aligned}
$$

Satz 2.13 (Inklusions-Exklusions-Prinzip (IEP))

$$
\begin{aligned}
S_* &= S_1 - S_2 + S_3 - S_4 + \ldots + (-1)^{j-1} S_j + \ldots + (-1)^{n-1} S_n \\
&= \sum_{i=1}^{n} (-1)^{i-1} S_i \\
S_0 &= S_{Gesamt} - S_* = S_{Gesamt} + \sum_{i=1}^{n} (-1)^i S_i
\end{aligned}
$$

Beweis:
Wir zählen die Vielfachheiten, mit denen Elemente aus U in dieser Formel gezählt werden.

Dazu klassifizieren wir die Elemente nach der Anzahl der Mengen, zu denen sie gehören.

Wir unterscheiden n Fälle:

Fall j: $(1 \le j \le n)$
Wir betrachten solche Elemente, die zu genau j der gegebenen n Mengen gehören.

links: es wird (in S_*) einmal gezählt
rechts:

- in S_1: es wird j-mal gezählt
- in S_2: es wird $\binom{j}{2}$-mal gezählt (in jeder 2-Menge von Indizes von Mengen zu denen es gehört)
- in S_3: es wird $\binom{j}{3}$-mal gezählt

  $\vdots$
- in S_j: es wird $\binom{j}{j}$-mal gezählt

Damit ergibt sich für die Vielfachheit:

$$\begin{aligned}
&\binom{j}{1} - \binom{j}{2} + \binom{j}{3} - \ldots + (-1)^{j-1}\binom{j}{j} \\
=&\Big[\binom{j}{0} - \binom{j}{0}\Big] + \binom{j}{1} - \binom{j}{2} + \binom{j}{3} - \ldots + (-1)^{j-1}\binom{j}{j} \\
=&\binom{j}{0} - \Big[\binom{j}{0} - \binom{j}{1} + \binom{j}{2} - \ldots + (-1)^{j}\binom{j}{j}\Big] \\
=&\binom{j}{0} - [1-1]^j = 1
\end{aligned}$$

■

2.3.1 Anwendungen des IEP

Unordnungen

Aufgabe: Gegeben seien n Briefe und n adressierte Kuverts.

Frage: Wie viele Möglichkeiten gibt es, die Briefe den Umschlägen so zuzuordnen, dass kein Brief richtig adressiert ist?

Formalisierung: Ausgangspunkt ist eine n-Menge $N = \{1, 2, \ldots, n\}$. Jede Zuordnung läßt sich beschreiben als eine Abbildung von N auf N (bijektiv).

Schreibweise:

$$\pi = \begin{pmatrix} 1\ 2\ 3\ \ldots\ n \\ \pi(1)\ \pi(2)\ \pi(3)\ \ldots\ \pi(n) \end{pmatrix}$$

ist eine (n, n)-Permutation.

$i \in N$ heißt **Fixpunkt** von $\pi \Leftrightarrow_{df} \pi(i) = i$

Mathematische Aufgabe: bestimme die Anzahl der Permutationen ohne Fixpunkte.

Um IEP anwenden zu können, definieren wir n Eigenschaften.

Für $i \in N$: Eine Permutation π besitzt die Eigenschaft

$$E_i \Leftrightarrow_{df} \pi(i) = i$$

S_1 ist die Anzahl der Permutationen mit einem Fixpunkt:

$$S_1 = n \cdot (n-1)!$$

Wobei n die Anzahl der Möglichkeiten darstellt, den Fixpunkt zu verteilen und $(n-1)!$ die Anzahl der Mögl. die verbleibenden Elemente anzuordnen.

S_2 ist die Anzahl der Permutationen mit zwei Fixpunkten:

$$\begin{aligned} S_2 &= \binom{n}{2} \cdot (n-2)! \\ &\vdots \\ S_j &= \binom{n}{j} \cdot (n-j)! \\ S_n &= 1 = \binom{n}{n} \cdot 0! \\ S_{Gesamt} &= n! \end{aligned}$$

Bestimme S_0!

$$\begin{aligned} S_0 &= S_{Gesamt} - S_1 + S_2 - S_3 + \ldots + (-1)^n S_n \\ &= n! - \binom{n}{1}(n-1)! + \ldots + (-1)^j \binom{n}{j}(n-j)! + \ldots + (-1)^n \binom{n}{n}(n-n)! \end{aligned}$$

Exkurs in die Analysis:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} \qquad \text{(Potenzreihe)} \tag{2.3}$$

$$\sum_{k=n+1}^{\infty} \frac{x^k}{k!} \leq \frac{1}{(n+1)!} \tag{2.4}$$

Spezialfall: $x = -1$

$$e^{-1} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!} \qquad \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \leq \frac{1}{(n+1)!}$$

$$\begin{aligned} S_0 &= n! - \frac{n!}{1!(n-1)!} \cdot (n-1)! + \ldots + (-1)^j \cdot \frac{n!}{j!(n-j)!} \cdot (n-j)! + \ldots + (-1)^n \cdot \frac{n!}{n!\,0!} \cdot 0! \\ &= n! \Big[\sum_{n=0}^{\infty} \frac{(-1)^n}{n!} - \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!} \Big] \end{aligned}$$

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

Also gilt: $|S_0 + \frac{n!}{e}| \leq \frac{1}{n+1}$

S_0 ist diejenige nat. Zahl, die am „dichtesten“ an $\frac{n!}{e}$ liegt:

$$S_0 \sim \frac{n!}{e}$$

Frage: Wie groß ist die Wahrscheinlichkeit dafür, dass bei einer willkürlichen Zuordnung eine solche Unordnung entsteht?

$$\begin{aligned} \text{relative Häufigkeit} &= \frac{\text{Anzahl der günstigen Fälle}}{\text{Anzahl der möglichen Fälle}} \\ &= \frac{\text{Anzahl der Unordnungen von } n \text{ Elementen}}{\text{Anzahl der Permutationen von } n \text{ Elementen}} \\ &= \frac{S_0}{n!} \sim \frac{\frac{n!}{e}}{n!} = \frac{1}{e} \sim 0.36\ldots \end{aligned}$$

Dies ist unabhänig von n.

Die Eulersche φ-Funktion

In der Zahlentheorie spielt die folgende Funktion eine wesentliche Rolle:

$$\varphi(n) =_{df} \text{card}\{m \mid 1 \leq m \leq n \text{ und (m und n sind teilerfremd)}\}$$

$D_\varphi \colon [1, \infty)$

m und n sind teilerfremd $\Leftrightarrow_{df}$ $\text{ggT}(m, n) = 1$

Beispiel 2.4
$n = 360$ $\varphi(n)$? Es gilt: $n = 2^3 \cdot 3^2 \cdot 5$

m ist teilerfremd zu n gdw. m ist weder durch 2,3 oder 5 teilbar.

Wir definieren folgende drei Eigenschaften: für $p \in \{2, 3, 5\}$; m besitzt die Eigenschaft

$$E_p =_{df} p \text{ ist Teiler von } m \quad (p \setminus m)$$

entsprechend

$$M_p = \{m \mid 1 \leq m \leq n \text{ und } p \setminus m\}$$

Nach IEP gilt: $\varphi(360) = S_0 = S_{Gesamt} - S_1 + S_2 - S_3$

$$\begin{aligned} S_{Gesamt} &= \text{card}\{m \mid 1 \leq m \leq 360\} = 360 \\ S_1 &= \text{card}\, M_2 + \text{card}\, M_3 + \text{card}\, M_5 \\ &= \text{card}\{m \mid 1 \leq m \leq 360 \wedge 2 \setminus m\} + \text{card}\{m \mid 1 \leq m \leq 360 \wedge 3 \setminus m\} \\ &\quad + \text{card}\{m \mid 1 \leq m \leq 360 \wedge 5 \setminus m\} \\ &= 360/2 + 360/3 + 360/5 = 180 + 120 + 72 = 372 \end{aligned}$$

Für Primziffern $p_1 \neq p_2$ gilt: $p_1 \setminus m$ und $p_2 \setminus m$ gdw. $p_1 \cdot p_2 \setminus m$

$$\begin{aligned} S_2 &= \text{card}(M_2 \cap M_3) + \text{card}(M_2 \cap M_5) + \text{card}(M_3 \cap M_5) \\ &= \text{card}\{m \mid 1 \leq m \leq 360 \wedge 6 \setminus m\} + \text{card}\{m \mid 1 \leq m \leq 360 \wedge 10 \setminus m\} \\ &\quad + \text{card}\{m \mid 1 \leq m \leq 360 \wedge 15 \setminus m\} \\ &= 360/6 + 360/10 + 360/15 = 60 + 36 + 24 = 120 \\ S_3 &= \text{card}(M_2 \cap M_3 \cap M_5) = \text{card}\{m \mid 1 \leq m \leq 360 \wedge 30 \setminus m\} \\ &= 360/30 = 12 \end{aligned}$$

$$\varphi(360) = 360 - 372 + 120 - 12 = 96$$

Exkurs in die Zahlentheorie

Fundamentalsatz der Arithmetik

Jede nat. Zahl $n > 1$ besitzt eine eindeutig bestimmte geordnete Zerlegung in Potenzen von Primzahlen:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \text{ , wobei } p_1 < p_2 < p_3 < \ldots < p_k \tag{2.5}$$

Aufgabe: Es sei n wie in Gleichung 2.5 mit $n \in \mathbb{N}$ und $n > 1$. Bestimme $\varphi(n)$!

Das Beispiel liefert:

Fakt
m ist teilerfremd zu n gdw weder p_1 noch p_2 noch … noch p_n sind Teiler von n.

Wir definieren für $1 \leq j \leq k$

$$M_{p_j} = \{m \mid 1 \leq m \leq n \wedge p_j \setminus m\}$$

und

$$M_{p_{i_1}} \cap M_{p_{i_2}} = \{m \mid 1 \leq m \leq n \wedge p_{i_1} \cdot p_{i_2} \setminus m\}, \quad 1 \leq i_1 < i_2 \leq k$$

usw.

$$\begin{aligned}
\varphi(n) =& S_0 = S_{Gesamt} - S_1 + S_2 \pm \ldots + (-1)^k \cdot S_k \\
S_{Gesamt} =& n = \text{card}\{1 \leq m \leq n\} \\
S_1 =& \sum_{1 \leq i_1 \leq k} \text{card}\, M_{p_{i_1}} = n/p_1 + n/p_2 + \ldots + n/p_k && \binom{k}{1} \text{ Summanden} \\
S_2 =& \sum_{1 \leq i_1 < i_2 \leq k} \text{card}(M_{p_{i_1}} \cap M_{p_{i_2}}) = \frac{n}{p_1 \cdot p_2} + \frac{n}{p_1 \cdot p_3} + \ldots + \frac{n}{p_{n-1} \cdot p_n} && \binom{k}{2} \text{ Summanden} \\
& \vdots \\
S_k =& \frac{n}{p_1 \cdot p_2 \cdot \ldots \cdot p_k} && \binom{k}{k} \text{ Summanden}
\end{aligned}$$

$$\begin{aligned}
\varphi(n) = S_0 = n \Big[1 &- \frac{1}{p_1} - \frac{1}{p_2} - \ldots - \frac{1}{p_k} \\
&+ \frac{1}{p_1 \cdot p_2} + \frac{1}{p_1 \cdot p_3} + \ldots + \frac{1}{p_{k-1} \cdot p_k} \\
&- \frac{1}{p_1 \cdot p_2 \cdot p_3} - \ldots - \frac{1}{p_{k-2} \cdot p_{k-1} \cdot p_k} \\
&\vdots \\
&+ (-1)^k \frac{1}{p_1 \cdot p_2 \cdot \ldots \cdot p_k} \Big]
\end{aligned}$$

Also:

$$\varphi(n) = n\,(1 - \frac{1}{p_1})\,(1 - \frac{1}{p_2})\,(1 - \frac{1}{p_3}) \ldots (1 - \frac{1}{p_k})$$

Satz 2.14

$$\varphi(n) = n \cdot \prod_{p \backslash n} (1 - \frac{1}{p})$$

unser Beispiel: $\varphi(360) = 360 \cdot 1/2 \cdot 2/3 \cdot 4/5 = 96$

weitere Eigenschaften:

$$\varphi(p) = p \cdot (1 - \frac{1}{p})$$
$$\varphi(p^e) = p^e \cdot (1 - \frac{1}{p})$$

Damit: (unter der Vor. $p \neq q$)

$$\begin{aligned}\varphi(p^e \cdot q^f) =& p^e \cdot q^f \,(1-\frac{1}{p})\,(1-\frac{1}{q})\\ =& p^e\,(1-\frac{1}{p}) \cdot q^f\,(1-\frac{1}{q})\\ =& \varphi(p^e) \cdot \varphi(q^f)\end{aligned}$$

Satz 2.15
Die φ-Funktion ist multiplikativ.

Das heißt für nat. Zahlen m und n, die Teilerfremd sind, gilt:

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

Ein anderer Blick auf $\varphi(n)$: $\varphi(n)$ ist die Anzahl der nicht mehr kürzbaren Brüche von $1/n, \ldots, n/n$

Beispiel 2.5
n=12

	1/12	2/12	3/12	4/12	5/12	6/12	7/12	8/12	9/12	10/12	11/12	12/12
$\varphi(12) = 4$	1/12				5/12		7/12				11/12	
$\varphi(6) = 2$		1/6								5/6		
$\varphi(4) = 2$			1/4						3/4			
$\varphi(3) = 2$				1/3					2/3			
$\varphi(2) = 1$						1/2						
$\varphi(1) = 1$												1/1

$12 = \varphi(12) + \varphi(6) + \varphi(4) + \varphi(3) + \varphi(2) + \varphi(1)$

Das heißt $12 = \sum_{t \backslash 12} \varphi(t)$

Satz 2.16

$$n = \sum_{t \backslash n} \varphi(t)$$

Surjektionen

Gegeben seien zwei Mengen

$$M = \{a_1, a_2, \ldots, a_m\} \text{ und } N = \{b_1, \ldots, b_n\} \text{ mit } n \leq m$$

Aufgabe: Bestimme die Anzahl der Surjektionen von M auf N.

Wir halten fest:

$$Abb(M,N) = \{f \mid f\colon M \mapsto N\} =: N^M$$

bezeichnet die Menge aller Abbildungen von M nach N.

Dann gilt:

$$\operatorname{card} Abb(M,N) = \operatorname{card} N^M = n^m \qquad \text{(Produktregel)}$$

$Surj(M,N) =_{df} \{f \mid f\colon M \mapsto N\}$ bezeichnet die Menge aller Abbildungen von M auf N ($D_f = M$, $W_f = N$).

Ansatz:

Für $1 \leq i \leq n$ definieren wir:

Eine Abbildung $f \in Abb(M,N)$ besitzt die Eigenschaft $E_i \Leftrightarrow_{df} b_i \notin W_f$

Dann gilt: $f \in Surj(M,N)$ gdw f besitzt weder E_1 noch E_2 noch ... noch E_n.

Das heißt $\operatorname{card} Surj(M,N) = S_0 = S_{Gesamt} - S_1 + S_2 - S_3 \pm \ldots$

Für $1 \leq j \leq n$ betrachten wir j-Tupel $1 \leq i_1 < i_2 < \ldots < i_j \leq n$

Hierfür sei $S_{i_1 i_2 \ldots i_j}$ die Anzahl der Abb. die die j Eigenschaften E_{i_1}, E_{i_2} usw. erfüllen.

$f \in Abb(M,N)$ erfüllt die Eigenschaften E_{i_1} und E_{i_2} und ... und E_{i_j}
gdw. $f\colon\ M \mapsto N \backslash \{b_{i_1}, b_{i_2}, \ldots, b_{i_j}\}$

Es gibt genau $(n-j)^m$ solche Abb.

Es gibt $\binom{n}{j}$ Möglichkeiten zur Auswahl eines j-Tupels $1 \leq i_1 < i_2 < \ldots < i_j \leq n$.
Damit ergibt sich:

$$S_j = \sum_{1 \leq i_1 < i_2 < \ldots < i_j \leq n} S_{i_1 i_2 \ldots i_j} = \sum_{1 \leq i_1 < i_2 < \ldots < i_j \leq} (n-j)^m = \binom{n}{j}(n-j)^m$$

Also: $S_0 = n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m \pm \ldots + (-1)^n \binom{n}{n}(n-n)^m$

Satz 2.17
Für die Anzahl der Surjektionen gilt:

$$\operatorname{card} Surj(M,N) = \sum_{k=0}^{n} (-1)^k \binom{n}{k}(n-k)^m$$

2.4 STIRLING-Zahlen

andere Deutung von $\sum_{k=0}^{n}(-1)^k \binom{n}{k} (n-k)^m$:

Anzahl der Mögl. m verschiedene Kugeln auf n numerierte aber sonst gleiche Fächer zu verteilen, so dass keines der Fächer leer bleibt.

Aufgabe: Bestimme die Anzahl der Mögl. m Kugeln auf n ununterscheidbare Fächer zu verteilen, s. d. keines der Fächer leer bleibt. $(m \geq n)$

Jede solche Verteilung gibt Anlass zu $n!$ Numerierungen der Fächer.

Definition 2.3
Für $m \geq n$ heißt

$$S_{m,n} := \frac{1}{n!} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m$$

STIRLING-Zahl 2. Art.

Satz 2.18
Die Anzahl der Mögl. m verschiedene Kugeln auf n ident. Fächer zu verteilen beträgt $S_{m,n}$.

Folgerung: $\operatorname{card} Surj(M,N) = n! \cdot S_{m,n}$

Wir betrachten ein Beispiel einer Surj.

$m = 6,\ n = 3, \qquad M = \{1,2,3,4,5,6\},\ N = \{a,b,c\}$ help: hier muss das Bild der Surj. hin Jede solche Surj. wird vollständig beschrieben durch $\big(f^{-1}(a);\ f^{-1}(b);\ f^{-1}(c)\big) = \big(\{1,2\};\ \{3\};\ \{4,5,6\}\big)$
geordnete Zerlegung der Menge M in n Teilmengen.

Definition 2.4
Es sei M eine m-Menge. $\mathfrak{j} \subseteq \mathfrak{P}(M)$ heißt n-Zerlegung von $M \ \Leftrightarrow_{df}$

1. $\mathfrak{j} = \{z_1, \ldots, z_n\} \qquad (\operatorname{card} \mathfrak{j} = n,\ z_i \subseteq M)$
2. $\bigcup_{\mathfrak{j}} = M$
3. $i \neq j \qquad z_i \cap z_j = \varnothing$
4. $z_i \neq \varnothing$

Satz 2.19
Die Anzahl der n-Zerlegungen einer m-Menge M ist gegeben durch $S_{m,n}$.

Spezielle Werte für $S_{m,n}$:

$$S_{m,m} = 1 \qquad S_{m,1} = 1$$
$$S_{m,m-1} = \binom{m}{2} \qquad S_{m,2} = 2^{m-1} - 1$$
$$m < n : \quad S_{m,n} := 0$$

Frage: Gibt es zur Berechnung der STIRLING-Zahlen in Analogie zu den Binomialkoeff. eine Rekursionsbeziehung?

Ansatz: Wir klassifizieren die n-Zerlegungen von M nach einem fixierten Element $a \in M$ (in Analogie zu den Binomialkoeff.)

1. Sorte: Die Zerlegungen von M, bei denen a eine eigene Klasse bildet, d. h. $\{a\} \in \mathfrak{j}$. Die restlichen $(m-1)$ Elemente sind auf $(n-1)$ Klassen zu verteilen: hierfür gibt es $S_{m-1,n-1}$ Möglichkeiten!

2. Sorte: Die n-Zerlegungen von M, bei denen a in einer größeren Klasse enthalten ist. Die verbleibenden $(m-1)$ Elemente sind auf n Klassen zu verteilen: hierfür gibt es $n \cdot S_{m-1,n}$ Mögl. (der Faktor n resultiert daraus, dass das a jeder der n Klassen hinzugefügt werden kann).

Satz 2.20
Für die Stirling-Zahlen zweiter Art gilt die folgende Rekursionsbeziehung:

$$m \geq n \geq 1 \ : \ S_{m,n} := S_{m-1,n-1} + n \cdot S_{m-1,n}$$

Diese Rekursion liefert ein Dreieck der Stirling-Zahlen 2. Art: help: hier ein Image der Rekursionsbeziehung

2.5 Dirichletsches Schubfachprinzip

Formulierung im Schubfachmodell:

1. Verteilt man $n = r + 1$ Gegenstände in r Schubfächer, dann gibt es ein Schubfach, das (min.) 2 Gegenstände enthählt.
2. Verteilt man $n = k \cdot r + 1$ Gegenstände auf r Schubfächer, dann gibt es ein Fach, das (min.) $r + 1$ Gegenstände enthählt.
3. Verteilt man n Gegenstände auf r Fächer, dann gibt es ein Fach, das $\lfloor \frac{n-1}{r} \rfloor + 1$ Gegenstände enthält.
4. Verteilt man $n = l_1 + l_2 + l_3 + \ldots + l_r - r + 1$ Gegenstände auf r Fächer, dann enthählt das 1. Fach l_1 Gegenstände oder das 2. Fach l_2 oder ... oder das r-te Fach l_r Gegenstände.

Formulierungen als Abbildungen:

$\varphi : N \to R$, dabei ist N eine n-Menge und $R = \{b_1, b_2, \ldots, b_r\}$

1. Falls $n \geq r + 1$, dann existiert ein $i \in \{1, \ldots, r\}$ mit $\operatorname{card} \varphi^{-1}(b_i) \geq 2$
2. Falls $n \geq k \cdot r + 1$, dann existiert ein $i \in \{1, \ldots, r\}$ mit $\operatorname{card} \varphi^{-1}(b_i) \geq k + i$
3. Falls $n \geq r$, dann existiert ein $i \in \{1, \ldots, r\}$ mit $\operatorname{card} \varphi^{-1}(b) \geq \lfloor \frac{n-1}{r} \rfloor + 1$
4. Falls $n \geq l_1 + l_2 + \ldots + l_r - r + 1$, dann gilt: $\operatorname{card} \varphi^{-1}(b_1) \geq l_1$ oder $\operatorname{card} \varphi^{-1}(b_2) \geq l_2$ oder $\ldots$ oder $\operatorname{card} \varphi^{-1}(b_r) \geq l_r$

2.5.1 Anwendungen

Studenten

Unter 367 Studenten befinden sich mindestens 2, die am selben Tag Geburtstag haben.

Haare

Kein Mensch hat mehr als 100.000 Haare auf dem Kopf.

Berlin hat 3,2 Mio. Einwohner. Dann gibt es X Einwohner, die haargenau dieselbe Haarzahl auf dem Kopf haben.

$$\lfloor \frac{3.199.999}{100.001} \rfloor = 31$$

Aussagen, die mit dem Schubfachschluss begründet werden, sind Existenzaussagen.

Kugeln

Eine Urne enthählt 5 gelbe, 6 rote und 7 blaue Kugeln. Bestimmen Sie die kleinste Anzahl von Kugeln, die gezogen werden müssen, um mit Sicherheit 3 rote oder 4 gelbe oder 5 blaue Kugeln zu haben.

$$r = 3 \; l_1 = 3 \; l_2 = 4 \; l_3 = 5$$

Dann gilt

$$n = l_1 + l_2 + l_3 - r + 1 = 10$$

9 Züge reichen nicht: 2 rote + 3 gelbe + 4 blaue

Mengen

$$S \subseteq \{1, \ldots, 14\} \text{ mit } \operatorname{card}(S) = 6$$

Beweisen Sie, dass die Summen der Elemente aller nicht leeren Teilmengen von S nicht alle verschieden sein können.

$$S = 1, \ldots, 4, 5, \ldots, 9, 12, 13$$

help: hier ist die Kopie undeutlich, hat jemand was anderes?

1. Versuch: S besitzt $2^6 - 1 = 63$ nicht leere Teilmengen A

S_A sei die Summe der Elemente aus A

Dann gilt $1 \leq S_A \leq 9 + 10 + 11 + 12 + 13 + 14 = 69$

Damit haben wir 69 mögliche Werte (Schubfächer) auf 63 Teilmengen (Gegenstände) zu verteilen. Daraus folgt: der Schubfachschluss sagt nichts aus.

2. Versuch:

Wir betrachten echte nicht leere Teilmengen von S, was 62 Teilmengen ergibt.

Mögliche Summen: $1 \leq S_A \leq 10 + 11 + 12 + 13 + 14 = 60$

Wir verteilen 62 Teilmengen (Gegenstände) auf 60 Fächer (Summen)

Damit gibt es 2 (echte) nichtleere Teilmengen von S, deren Summe gleich ist.

Quadrate

Unter je 5 Punkten eines Einheitsquadrates gibt es stets zwei Punkte deren Abstand nicht größ er als $\frac{1}{\sqrt{2}}$ ist. help: Bild eines Einheitsquadrates mit radius $\frac{1}{\sqrt{2}}$ und Einteilung mit Quadranten

Zwischen einem der 4 Quadrate mit Seitenlänge 1/2 müssen 2 Punkte liegen, die nicht weiter als $\frac{1}{\sqrt{2}}$ entfernt liegen können.

Bekannte

Unter je sechs Personen gibt es stets drei Personen, die entweder paarweise untereinander bekannt sind oder paarweise nicht miteinander bekannt sind.

Seien A, B, C, D, E, F die 6 Personen.

Wir unterscheiden sie dadurch, ob sie A kennen.

Zimmer 1: alle Personen, die A kennen.
Zimmer 2: alle Personen, die A nicht kennen.

(A wird keinem Zimmer zugeordnet)

Das heißt 5 Personen werden auf 2 Zimmer verteilt. Dann gibt es ein Zimmer, das 3 Personen enthählt.

1. Fall: B, C, D sind in Zimmer 1

1.1: B, C, D kennen sich paarweise nicht. Das ist die Behauptung.

1.2: sonst: es gibt 2 die sich kennen $o.B.d.A.$ seien das B und C. Dann sind A, B, C 3 Personen, die sich paarweise kennen.

2. Fall: B, C, D sind in Zimmer 2

2.1: B, C, D kennen sich paarweise. Das ist die Behauptung.

2.2: sonst: es gibt zwei ($o.B.d.A.B$ und C) die sich nicht kennen. Dann bilden A, B, C eine Menge von 3 Personen, die sich paarweise nicht kennen.

Frage: gilt die Aussage auch für 5 Personen?

Nein: help: Pentagram mit roten Kanten (Personen kennen sich) zw. AB,AC,ED,EC,BD und blaue Kanten (Personen kennen sich nicht) zwischen AE,DC,BC,BE,AD

Frage: Welches ist die kleinste Zahl $R(n)$, so dass die folgende Aussage wahr ist: Zu jeder Gruppe von $R(n)$ Personen gibt es stets eine Gruppe von n Personen, die sich entweder paarweise kennen oder sich paarweise nicht kennen.

$R(n)$ bezeichnet die sogenannte **Ramsay-Zahl**, das Beispiel zeigt $R(3) = 6$.

Umformulierung: In jedem vollständigen Graphen mit $R(n)$ Knoten dessen Kanten rot und blau gefärbt sind, gibt es stets eine „einfarbige Clique“.

help: vollständiger Graph mit den Knoten A,B,C,D,E,F rot und blau gefärbten Kanten (rot=AB,AC,AD,AE,BD,CD,CE,DF) (blau=AF,BC,BE,BF,CF,DE,EF)

Beweisen Sie: Bei jeder Verteilung von 1600 Bananen an 100 Affen gibt es 4 Affen, die dieselbe Anzahl von Bananen erhalten.

Wir betrachten folgende Verteilung:

$$
\begin{aligned}
a_1^{'} = a_2^{'} = a_3^{'} &= 0 \\
a_4^{'} = a_5^{'} = a_6^{'} &= 1 \\
&\vdots \\
a_{3\,i+1}^{'} = a_{3\,i+2} = a_{3\,i+3} &= i \\
&\vdots \\
a_{97} = a_{98} = a_{99} &= 32 \\
a_{100} &= 33
\end{aligned}
$$

indirekt: Angenommen $(a_1, \ldots, a_{100})$ ist eine Verteilung bei der keine 4 Affen die gleiche Bananenanzahl bekommen.

Dann gilt $\sum a_i \leq \sum a_i^{'} = 3(\sum_{i=1}^{32} i + 33 = 1617$

Widerspruch zur Annahme, dass 1600 Bananen zur Verfügung stehen.

help: jetzt gibt es einen Bruch, wer helfen kann, bitte hier einfügen. Irgendwie fehlt mir das Bindeglied zwischen 21.06. und 23.06. denn so ergibt das einfach keinen Sinn

Jede Folge von $n^2 + 1$ positiven, verschiedenen Zahlen enthählt eine Teilfolge der Länge $n + 1$ die entweder monoton fallend oder steigend ist.

Die Folge sei gegeben durch:

$$a_1, a_2, \ldots, a_{n^2+1}$$

Es gibt Indizes $i_1, i_2, \ldots, i_{n+1}$, wobei $1 \leq i_1 < i_2 < \ldots < i_{n+1} \leq n^2 + 1$ mit $a_{i_1} < a_{i_2} < \ldots < a_{i_{n+1}}$ oder $a_{i_1} > a_{i_2} > \ldots > a_{i_{n+1}}$

Für jedes a_i sei w_i die maximale Länge einer bei a_i startenden Folge monoton wachsender Zahlen.

Fallunterscheidung:

1. Fall: Es gibt ein i mit $w_i \geq n+1$, d. h. es gibt eine monton wachsende Folge der Länge $n + 1$

2. Fall: Für alle i ist $w_i < n + 1$
Wir definieren „Schubfächer“:

$$S_K =_{df} \{i \mid w_i = k\} \qquad \text{für } k = 1, \ldots, n$$

Also gibt es ein Schubfach, dass (min) $\lfloor \frac{(n^2+1)-1}{n} \rfloor + 1 = n+1$ Indizes enthält.

Diese seien $1 \leq i_1 < i_2 < \ldots < i_j \leq n^2 + 1$ wobei $j \geq n + 1$

Behauptung: Für die zugehörige Folge der Zahlen gilt:

$$a_{i_1} > a_{i_2} > \ldots > a_{i_j}$$

warum ist $a_{i_k} < a_{i_{k+1}}$?

Angenommen es gilt: $a_{i_k} < a_{i_{k+1}}$!

Wissen: es gibt eine maximale Folge monoton wachsender Zahlen der Länge l, die bei $a_{i_{k+1}}$ beginnt und ebenso für a_{i_k}

Das heißt es gibt für a_{i_k} sogar eine monton wachsende Folge der Länge $(l+1)$!

2.5.2 STIRLING-Zahlen 1. Ordnung

$M = \{a_1, a_2, \ldots, a_m\}$ sei eine m-Menge.

Für **bijektive Abbildungen** $\pi\colon M \twoheadleftarrow\!\!\!\rightarrow M$ haben wir folgende Schreibweise:

$$p = \begin{pmatrix} 1 & 2 & \ldots & m \\ \pi(1) & \pi(2) & \ldots & \pi(m) \end{pmatrix}$$

Beispiel 2.6
$\pi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{smallmatrix}\right)$ ist durch das Wort: 4 5 3 1 2 eindeutig festgelegt.

Wir betrachten die Abbildung im Einzelnen:

$$\begin{gathered} 1 \to 4 \to 1 \to \ldots \\ 2 \to 5 \to \ldots \\ 3 \to 3 \to 3 \to \ldots \end{gathered}$$

Alle Elemente lassen sch in Klassen von Zyklen zerlegen:

$$(1\,4)(2\,5)(3)$$

mit der Gesamtlänge von m: $\quad 2 + 2 + 1 = 5.$

Wir halten fest:

1. Für die Charakterisierung von π ist die Reihenfolge der Zyklen unwesentlich
2. In jedem Zyklus kann jedes Element an erster Position stehen (damit ist der Rest festgelegt)

Definition 2.5
$S_{m,n}$ $(1 \leq n \leq m)$ bezeichnet die die Anzahl der Zerlegungen von Permutationen von m Elementen (m-Permutationen) in n Zyklen und heißt **Stirling-Zahl, erster Art**.

wir ergänzen:

$$S_{m,0} =_{df} 0 \qquad \text{für } m > 0$$
$$S_{0,0} =_{df} 1$$

spezielle Werte:

$$S_{m,m} = 1$$
$$S_{m,m-1} = \binom{m}{2}$$
$$S_{m,1} = (m-1)!$$

Außerdem gilt:

$$\sum_{n=0}^{m} S_{m,n} = m!$$

Aufgabe: Suche eine Rekursionsbeziehung!

Ansatz: wir klassifizieren nach einem fixierten Element $a \in M$: danach ob a einem Zyklus für sich allein bildet oder nicht.

1. Sorte: a ist Fixpunkt: die verbleibenden $m-1$ Elemente müssen auf $(n-1)$ Zyklen verteilt werden; dafür gibt es $S_{m-1,n-1}$ Möglichkeiten

2. Sorte: a ist kein Fixpunkt: die verbleibenden $m-1$ Elemente müssen auf n Zyklen verteilt werden ($S_{m-1,n}$ Mögl.)
Hieraus wird eine m-Permutation, indem a innerhalb der vorhandenen Zyklen vor eines der $(m-1)$ Elemente geschrieben wird: also $m-1$ Mögl. für a, insgesamt also

$$(m-1)\, S_{m-1,n}$$

Möglichkeiten.

Dann gilt:

Satz 2.21 (Rekursion für Stirlingzahlen 1. Art)

$$S_{m,n} = S_{m-1,n-1} + (m-1)\, S_{m-1,n}$$

Dies liefert ein Dreieck der Stirlingzahlen 1. Art.

help: ein typisches Pascaldreieck mit Stirlingzahlen halt...

2.6 Erzeugende Funktionen und Rekurrenzen

Ausgangspunkt: Spezialfall des Binomischen Satzes

$$(1+X)^n = \sum_{r=0}^{n} \binom{n}{r} \cdot x^r$$

rechte Seite: Polynom dessen Koeffizienten gerade die Binomialkoeffizienten sind:

$$C(n,r) = \binom{n}{r}$$

linke Seite: $(1+x)^n$ enthält kombinatorische Informationen für das Abzählproblem: Bestimme die r-Kombinationen einer n-Menge (ohne Wiederholung).

Definition 2.6
Eine Funktion

$$f(x) = \sum_{r=0}^{k} a_r \, x^r$$

heißt erzeugende Funktion für die Koeff. a_r. Falls die Zahlen a_r Zählkoeff. eines Abzählproblems sind, dann heißt f erzeugende Funktion dieses Problems.

Beispiel 2.7
$f(x) = (1+x)^n$ ist also erzeugende Funktion des Abzählproblems „r-Kombinationen (ohne Wiederholung) aus n-Menge“.

Interpretation: Jeder Term $(1+x)$ wird aufgefasst als ein Schubfach; wir haben n unterscheidbare Schubfächer, auf die r identische Gegenstände zu verteilen sind. (wobei jedes Fach höchstens einen Gegenstand enthält)

Dabei entspricht die Zuordnung

- 1 Gegenstand für das Fach - der Auswahl von x beim Ausmultiplizieren und
- 0 Gegenstände für das Fach - der Auswahl von 1 beim Ausmultiplizieren

Ansatz: Die Erweiterung „höchstens zwei Gegenstände pro Fach“ wird durch den Term

$$x^2 + x + 1$$

repräsentiert:
„2 Gegenstände“ bedeutet: „wähle x^2 beim Ausmultiplizieren“

Beispiel 2.8
Ein konkretes Problem sei gegeben durch:

Fach	erlaubte Anzahlen	Term
Fach 1	0, 1, 3	$x^3 + x + 1$
Fach 2	1, 2	$x^2 + x$
Fach 3	1	x
Fach 4	0, 4	$x^4 + 1$

Die erzeugende Funktion für dieses spezielle Abzählproblem ist gegeben durch:

$$f(x) = (x^3 + x + 1)\,(x^2 + x)\,(x)\,(x^4 + 1)$$

Durch Ausmultiplizieren ergibt sich folgendes Polynom:

$$f(x) = 1 \cdot x^2 + 2 \cdot x^3 + 1 \cdot x^5 + 2 \cdot x^6 + 2 \cdot x^7 + x^8 + 2 \cdot x^9 + 1 \cdot x^8$$

Das heißt es gibt

- 0 Möglichkeiten 0, 1, 11 oder mehr Gegenstände zu verteilen
- 1 Möglichkeit 2, 4, 5, 8, 10 Gegenstände zu verteilen
- 2 Möglichkeiten 3, 6, 7 oder 9 Gegenstände zu verteilen

Die Lösung dieses Zählproblems ergibt sich durch „rein mechanisches“ Ausmultiplizieren.

Verallgemeinerung: Gegeben sei ein Abzählproblem bei dem identische Gegenstände auf n unterscheidbare Schubfächer zu verteilen sind.

Die zulässigen Anzahlen für das Schubfach i sei gegeben durch $0 \leq V_{i_1} < V_{i_2} < \ldots < V_{i_{j_i}}$

Wir identifizieren dieses Fach i mit dem Term

$$(x^{V_{i_1}} + x^{V_{i_2}} + \ldots + x^{V_{i_{j_i}}})$$

und erhalten die erzeugende Funktion

$$\prod_{i=1}^{n} (x^{V_{i_1}} + \ldots + x^{V_{i_{j_i}}})$$

Satz 2.22
Die Koeffizienten des ausmultiplizierten Polynoms sind gerade die Zählkoeffizienten dieses Abzählproblems.

Frage: Gibt es einen Ansatz für das Abzählproblem r-Kombinationen einer n-Menge mit Wiederholung?

Das heißt die erlaubten Anzahlen pro Fach sind:

$$0, 1, 2, 3, \ldots$$

Ansatz: Wir identifizieren ein solches Fach mit dem „Term“ $1+x+x^2+\ldots$

Dies ist kein Term im eigentlichen Sinn, sondern eine **Potenzreihe** $\sum_{k=0}^{\infty} x^k$.

Die Analysis sagt: Die Reihe konvergiert für $|x| < 1$ und es gilt für solche x:

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$$

Wir ignorieren das Konvergenzverhalten und definieren formal: $(\frac{1}{1-x})^n$ ist die erzeugende Funktion für das Abzählproblem „Bestimme die r-Kombination einer n-Menge mit Wiederholung.“

Definition 2.7

$$f(x) = \sum_{k=0}^{\infty} a_k \, x^k$$

heißt erzeugende Funktion für die Koeff. $(a_k)_{k=0}^{\infty}$;

Falls die Zahlen a_k Zählkoeff. sind, dann heißt f erzeugende Funktion für dieses Abzählproblem.

Satz 2.23 (aus der Analysis)

$$\left(\frac{1}{1-x}\right)^n = \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^r$$

Dies liefert: Die Zählkoeff. für das gegebene Abzählproblem sind $\binom{n+r-1}{r}$.

2.6.1 Exkurs: Rechnen mit Potenzreihen

Rechenregeln

$$a \cdot \sum_{k=0}^{\infty} u_k\, x^k + b \cdot \sum_{k=0}^{\infty} v_k\, x^k = \sum_{k=0}^{\infty} (a \cdot u_k + b \cdot v_k) \cdot x^k \tag{2.6}$$

$$\left(\sum_{k=0}^{\infty} u_k \cdot x^k\right) \cdot \left(\sum_{k=0}^{\infty} v_k \cdot x^k\right) = \sum_{k=0}^{\infty} w_k \cdot x^k \qquad w_k = \sum_{i=0}^{k} u_i \cdot v_{k-i} \tag{2.7}$$

$$n(x) = \sum_{k=0}^{\infty} 0 \cdot x^k = 0 \text{ ist neutrales Element bez. Addition} \tag{2.8}$$

$$e(x) = \sum_{k=1}^{\infty} 0 \cdot x^k + 1 = 1 \text{ ist neutrales Element bez. Multiplikation} \tag{2.9}$$

und

Für eine Reihe

$$g(x) = \sum_{k=0}^{\infty} u_k \cdot x^k$$

existiert ein Inverses

$$h(x) = \sum_{k=0}^{\infty} v_k \cdot x^k$$

so dass

$$g(x) \cdot h(x) = 1, \text{ falls } u_o \neq 1$$

Eine Verallgemeinerung wird dadurch erreicht, in dem für jedes Fach eine bel. Folge $(n_0, n_1, n_2, \ldots)$ von erlaubten Anzahlen zugelassen wird.

Dann ist z. B. auch $(v_{i_1}, v_{i_2}, \ldots, v_{i_{j_i}}, 0, 0, \ldots)$ eine solche unendliche Folge.

Beispiel 2.9 („Jedes Fach soll min. einen Gegenstand enthalten“)
Ansatz: „Term“ $x + x^2 + \ldots$

Potenzreihe:

$$\sum_{k=1}^{\infty} x^k = \sum_{k'=0}^{\infty} x^{k'+1} = \sum_{k=0}^{\infty} x^{k+1}$$

mit dem Index $k' = k - 1$ $(k = k' + 1)$, also

$$
\begin{aligned}
&= x \cdot \sum_{k=0}^{\infty} x^k = x \left(\frac{1}{1-x} \right) = \frac{x}{1-x} \\
&= \sum_{k-n=0}^{\infty} \binom{k-1}{k-n} x^k \\
&= \sum_{k=n}^{\infty} \binom{k-1}{k-n} x^k \qquad \text{(Symetrie)} \\
&= \sum_{k=n}^{\infty} \binom{k-1}{n-1} x^k
\end{aligned}
$$

Die Koeff. $\binom{k-1}{n-1}$ sind gerade die Zählkoeff. für unser Abzählproblem und es gilt: dies entspricht der n-Partition von k.

2.6.2 Rekurrenzen - am Beispiel der FIBONACCI-Zahlen

Rekursionsschema

(2.10) $\qquad u_0 = 0\,,\ u_1 = 1$

(2.11) $\qquad u_n = u_{n-1} + u_{n-2} \qquad (n \geq 2)$

Dieses Schema liefert folgende Werte:

n	0	1	2	3	4	5	6	7	8	9	10
u_n	0	1	1	2	3	5	8	13	21	34	55

Anliegen: Bestimme eine explizite Formel für die Werte u_n, d. h. u_n bekommt eine Darstellung von n (aber *nicht* von den Vorgängerwerten).

Das obige Schema ist ein lineares und homogenes Rekursionsschema mit konstanten Koeffizienten. Zur Realisierung des Anliegens geben wir ein prinzipielles Verfahren, dass sich auf weitere Bsp. übertragen lässt.

Das Verfahren vollzieht sich in den folgenden Schritten:

1. Schritt: Stelle das Schema 2.10 durch eine einzige Gleichung dar!

Dazu setzen wir: $u_n := 0$ für $n < 0$

Damit gilt auch für $n = 0:\ u_n = u_{n-1} + u_{n-2}$
aber für $n = 1:\ u_n = u_{n-1} + u_{n-2} + 1$
und für $n > 1:\ u_n = u_{n-1} + u_{n-2}$

Dies schreiben als:

$$u_n = u_{n-1} + u_{n-2} + \text{Wert-I}_a^n(„n = 1“) \tag{2.12}$$

2. Schritt: Bestimme mit Hilfe formaler Potenzreihen eine erzeugende Funktion für Schema 2.12!

1. Ansatz:

$$g(x) := \sum_{n=0}^{\infty} u_n \, x^n$$

Wegen Gleichung 2.12 gilt:

$$\begin{aligned}
g(x) &= \sum_{n=0}^{\infty} u_n \, x^n = \sum_{n=0}^{\infty} (u_{n-1} + u_{n-2} + \text{Wert-I}_a^n(„n = 1“)) \; x^n \\
&= \sum_{n=0}^{\infty} u_{n-1} \, x^n + \sum_{n=0}^{\infty} u_{n-2} \, x^n + \sum \text{Wert-I}_a^n(„n = 1“) \cdot x^n \\
&= x \cdot \sum_{n=1}^{\infty} u_{n-1} \cdot x^{n-1} + x^2 \cdot \sum_{n=2}^{\infty} u_{n-2} \, x^{n-2} + x \\
&= x \cdot \sum_{n'=0}^{\infty} u_{n'} \cdot x^{n'=0} + x^2 \cdot \sum_{n''=0}^{\infty} u_{n''} \, x^{n''} + x \\
&= x \cdot g(x) + x^2 \cdot g(x) + x
\end{aligned}$$

wir haben:

$$\begin{aligned}
g(x) &= x \cdot g(x) + x^2 \cdot g(x) + x \\
x &= g(x)[x + x^2 - 1]
\end{aligned}$$

und damit:

$$g(x) = \frac{-x}{x^2 + x - 1} \tag{2.13}$$

$g(x)$ ist die erzeugende Funktion für das Schema 2.12

3. Schritt: Entwickle die rechte Seite von Gleichung 2.13 in eine formale Potenzreihe und bestimme deren Koeff.! (Aufgrund des 1. Ansatzes sind die gerade die gesuchten u_n!)

Dies geschieht in mehreren Teilschritten:
$g(x)$ besitzt die Darstellung als rationale Funktion, d. h. ist von der Form

2. Ansatz: $g(x) = \frac{p(x)}{q(x)}$, dabei ist $p(x)$ das *Zählerpolynom* und $q(x)$ das *Nennerpolynom*.

Schritt 3.1: Bestimme die Nullstellen des Nennerpolynoms:

$$q(x) = x^2 + x - 1$$

Die Lsg. sind

$$\alpha = -1/2 + \sqrt{(1/2)^2 + 1} = \frac{-1 + \sqrt{5}}{2} \tag{2.14}$$

$$\beta = -1/2 - \sqrt{(1/2)^2 + 1} = \frac{-1 - \sqrt{5}}{2} \tag{2.15}$$

und es gilt:

$$q(x) = (x - \alpha)\,(x - \beta) = (x + \frac{1 - \sqrt{5}}{2})\,(x + \frac{1 + \sqrt{5}}{2}) \tag{2.16}$$

Schritt 3.2: Realisiere gemäß des 2. Ansatzes eine Darstellung von $g(x)$ durch Partialbruchzerlegung.

$$g(x) = \frac{p(x)}{q(x)} = \frac{p(x)}{(x - \alpha)\,(x - \beta)} \stackrel{!}{=} \frac{A}{(x - \alpha)} + \frac{B}{(x - \beta)} \tag{2.17}$$

3. Ansatz:
Schritt 3.3: Bestimme die Koeff. A und B!

Schritt 3.4: Bestimme die gesuchten Koeff. u_n (gemäß Ansatz 1) durch Einsetzen in die formale Potenzreihe.

Denn es gilt: $g(x) = \frac{A}{x-\alpha} + \frac{B}{x-\beta}$
Erweitern wir den 1. Bruch mit $-1/\alpha$, den 2. Bruch mit $-1/\beta$

Damit gilt:

$$\begin{aligned} g(x) &= \frac{(-1/\alpha) \cdot A}{(-1/\alpha) \cdot (x - \alpha)} + \frac{(-1/\beta) \cdot B}{(-1/\beta) \cdot (x - \beta)} \\ &= (-1/\alpha)\ A \cdot \frac{1}{1 - (1/\alpha) \cdot x} + (-1/\beta) \cdot B \cdot \frac{1}{1 - (1/\beta) \cdot x} \\ &= -A/\alpha \cdot \sum_{n=0}^{\infty} \left(\frac{1}{\alpha}\right)^n x^n - B/\beta \cdot \sum_{n=0}^{\infty} \left(\frac{1}{\beta}\right)^n x^n \\ &= \sum_{n=0}^{\infty} \left[-\frac{A}{\alpha^{n+1}} - \frac{B}{\beta^{n+1}}\right] x^n \end{aligned}$$

Damit gilt:

$$u_n = -\frac{A}{\alpha^{n+1}} - \frac{B}{\beta^{n+1}} \tag{2.18}$$

Nun Schritt 3.3 (wir starten mit Gleichung 2.17)

$$\begin{aligned} g(x) = \frac{p(x)}{(x-\alpha)(x-\beta)} &= \frac{-x}{\left(x+\frac{1-\sqrt{5}}{2}\right)\left(x+\frac{1+\sqrt{5}}{2}\right)} \stackrel{!}{=} \frac{A}{\left(x+\frac{1-\sqrt{5}}{2}\right)} + \frac{B}{\left(x+\frac{1-\sqrt{5}}{2}\right)} \\ &= \frac{A\left(x+\frac{1+\sqrt{5}}{2}\right) + B\left(x+\frac{1-\sqrt{5}}{2}\right)}{\left(x+\frac{1-\sqrt{5}}{2}\right)\left(x+\frac{1+\sqrt{5}}{2}\right)} \\ &= \frac{(A+B)\,x + A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right)}{\left(x+\frac{1-\sqrt{5}}{2}\right)\left(x+\frac{1+\sqrt{5}}{2}\right)} \end{aligned}$$

Ein Koeff.vergleich liefert:

$$A + B = -1 \tag{2.19}$$

$$A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right) = 0 \tag{2.20}$$

Gleichung 2.19 ergibt: $A = -1 - B$, einsetzen in Gleichung 2.20:

$$\begin{aligned} (-1-B)\,(\frac{1+\sqrt{5}}{2}) + B(\frac{1-\sqrt{5}}{2}) &= 0 \\ -\frac{1+\sqrt{5}}{2} - B\cdot\frac{1+\sqrt{5}}{2} + B\,\frac{1-\sqrt{5}}{2} &= 0 \\ B\left[-1/2-\sqrt{5}/2+1/2-\sqrt{5}/2\right] &= 1/2+\sqrt{5}/2 \\ B\,(-\sqrt{5}) &= \frac{1+\sqrt{5}}{2} \\ B &= -1/\sqrt{5}\cdot\frac{1+\sqrt{5}}{2} \end{aligned}$$

haben: $B = -1/\sqrt{5}\cdot\frac{1+\sqrt{5}}{2}$ in Gleichung 2.19 liefert:

$$A = \frac{1}{\sqrt{5}}\cdot\frac{1-\sqrt{5}}{2} \tag{2.21}$$

Um Gleichung 2.18 darstellen zu können, benutzen wir noch folgende Beziehungen:

haben: $\alpha = \frac{-1+\sqrt{5}}{2} = -\frac{1-\sqrt{5}}{2}$. Dann ist

$$\frac{1}{\alpha} = \frac{-2}{1-\sqrt{5}} = \frac{-2\,(1+\sqrt{5}}{(1+\sqrt{5})\,(1-\sqrt{5})} = \frac{-2\,(1+\sqrt{5})}{-4} = \frac{1+\sqrt{5}}{2} = -\beta$$

entsprechend liefert

$$\beta = \frac{-1-\sqrt{5}}{2} = -\frac{1+\sqrt{5}}{2} \text{ für } \frac{1}{\beta} = -\alpha$$

Dies setzen wir in Gleichung 2.18 ein:

$$\begin{aligned} u_n = &-\left(\frac{1}{\sqrt{5}} \cdot \frac{1-\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n \\ &+\left(\frac{1}{\sqrt{5}} \cdot \frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n \end{aligned}$$

$$u_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n \tag{2.22}$$

3 Einblicke in die Zahlentheorie

3.1 Natürliche Zahlen

Beschreibung als Mengen:

Rekursionsschema:

$$0 := \varnothing$$
$$n + 1 := n \cup \{n\}$$

Beispiel 3.1

$$1 = \varnothing \cup \{\varnothing\} = \{\varnothing\} = \{0\}$$
$$2 = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} = \{0, 1\}$$

Prädikatenlogische Beschreibung

3.1.1 PEANA-Axiome

Struktur:	$\mathbb{N}$	sei die Menge der natürlichen Zahlen
	0	Null
	$n + 1$	Nachfolger

(3.1) $$\forall_{n \in \mathbb{N}}(n + 1 \neq 0)$$

(3.2) $$\forall_{n \in \mathbb{N}} \forall_{min \mathbb{N}}(n + 1 = m + 1 \rightarrow n = m) \qquad \text{Eindeutigkeit}$$

(3.3) $$\forall_{M \in \mathbb{N}} (0 \in M \wedge \forall_{n \in N} (n \in M \rightarrow n + 1 \in M) \rightarrow M = \mathbb{N})$$

Frage: Wieso gilt in der Struktur $[\mathbb{N}, 0, +1]$ das Induktionsprinzip?

Dazu definieren wir:

$$n \leq m \Leftrightarrow_{df} n = m \vee n \in m \qquad \text{Quasielementbeziehung}$$

Eigenschaften:

1. ist reflexiv
2. ist transitiv
3. ist antisymetrisch
4. ist linear
5. jede nichtleere Teilmenge besitzt ein kleinstes Element

1) bis 3) charakterisieren $\leq$ als Halbordnungsrelation.
1) bis 4) charakterisieren $\leq$ als Ordnungsrelation.
1) bis 3) + 5) charakterisieren $\leq$ als Wohlordnungsrelation.

Für die wohlgeordnete Menge $[\mathbb{N}, \leq]$ gilt folgendes Induktionsprinzip:

$$\forall_{M \in N} \left(\min N \in M \wedge \forall_{K \in N} \left(\min K \in M \rightarrow \min(K \backslash \{\min K\} \in M) \rightarrow M = N\right)\right.$$

Rechenoperationen - mit Hilfe des Induktionsprinzips

Satz 3.1 (Rekursionsschema für die Addition)

$$\begin{aligned} m + 0 &:= m \\ m + (n + 1) &:= (m + n) + 1 \end{aligned}$$

Satz 3.2 (Rekursionsschema für die Multiplikation)

$$\begin{aligned} m \cdot 0 &:= 0 \\ m \cdot (n + 1) &:= m \cdot n + m \end{aligned}$$

Damit gilt: $n \leq m \leftrightarrow \exists_{k \in \mathbb{N}}(n + k = m)$

$\leq$ ist damit durch die Addition charakterisiert!

Frage: Was ist das multiplikative Analogon?

$$n \backslash m \Leftrightarrow_{df} \forall_{k \in \mathbb{N}} (n \cdot k = m) \qquad \text{Teilerrelation}$$

Eigenschaften:

- $\backslash$ ist eine Halbordnungsrelation, d. h. $[\mathbb{N}, \backslash]$ ist eine halbgeordnete Menge
- $1 \backslash n$ für alle $n \in \mathbb{N}$, d. h. $1 = \min_{\backslash} \mathbb{N}$
- $n \backslash 0$ für alle $n \in \mathbb{N}$, d. h. $0 = \max_{\backslash} \mathbb{N}$ $(0 = \min_{\leq} \mathbb{N})$
- $n \backslash x \wedge n \backslash y \rightarrow n \backslash a\, x + b\, y$: n ist gemeinsamer Teiler von x und y
- $n \backslash x \wedge m \backslash y \rightarrow n \cdot m \backslash x\, y$
- $n \backslash m \wedge m + 0 \rightarrow n \leq m$

Eigenschaften der Differenz

Falls $m \leq n$, dann ex. $k \in \mathbb{N}$ mit $m + k = n$. k heißt **Differenz** zwischen m und n.

Schreibweise: $n - m := k$

Rechenregeln: z. B.

- $a \cdot (n - m) = a\,n - a\,m$
- falls $n \backslash x$ und $n \backslash y$ und $b\,y \leq a\,x$, dann $n \backslash (a\,x - b\,y)$

Frage: Was ist eine „eingeschränkte Division“?

Lemma 3.1
Für je zwei natürliche Zahlen n und m mit $m \leq n$ gibt es zwei eindeutig bestimmte Zahlen q und r, so dass gilt:

$$n = q \cdot m + r \qquad \text{und} \qquad 0 \leq r < m$$

Schreibweise:

$$n \text{ div } m := q$$
$$n \mod m := r$$

Dies ist die Definition zweier zweistelliger Funktionen „div“ und „mod“.

Falls $n \mod m = 0$, dann $m \backslash n$ und wir setzen den (eingeschränkten) Quotienten $\frac{n}{m} := q$

Verallgemeinerung:

$$\lfloor \frac{n}{m} \rfloor := n \text{ div } m \text{ heißt ganzer Teil der Division}$$

Beweis: (mithilfe des Wohlordnungsprinzips)
Wir definieren folgende Menge:

$$N := \{n - k \cdot m \mid k \in \mathbb{N} \text{ und } k \cdot m \leq n\}$$

Da $n \cdot m \in \mathbb{N}$, gilt $N \neq \varnothing$
Also ex. ein Minimum in N. Es sei $r = \min_{\leq} N$.

1. Fall $r < m$, $r \in \mathbb{N}$ bedeutet: es gibt ein $k \in \mathbb{N}$ mit $r = n - k \cdot m$, d. h. $n = k \cdot m + r$ und $0 \leq r < m$

2. Fall $r \geq m$, d. h. es gibt $k \in \mathbb{N}$, s. d. $r = n - k \cdot m$. Damit $r - m = (n - k \cdot m) - m = n - (k + 1) \cdot m \geq 0$
Das heißt $r - m \in \mathbb{N}$ und $r - m < r$ $\lightning (r = \min N)$
Der 2. Fall tritt nicht ein.

Dies beweist die Existenz von q und r!
Es bleibt zu zeigen: Eindeutigkeit:

Es sei $n = q_1 m + r_1 \qquad 0 \leq r_1 < m$
und $n = q_2 m + r_2 \qquad 0 \leq r_2 < m$
Also gilt:

$$\begin{aligned} 0 &= q_1 m + r_1 - (q_2 m + r_2) \\ &= (q_1 - q_2)m + (r_1 - r_2) \\ (r_2 - r_1) &= (q_1 - q_2)m \end{aligned}$$

Also $m \backslash (r_2 - r_1)$, andererseits $0 \leq r_2 - r_1 < m$.
Also $r_2 - r_1 = 0 \ \rightarrow r_2 = r_1$
Das heißt $(q_1 - q_2) \cdot m = 0 \ \rightarrow q_1 - q_2 = 0 \ \rightarrow q_1 = q_2$ ∎

m-adische Darstellung der natürlichen Zahlen

Definition 3.1
Für ein finites $m \geq 2$ ist die m-adische Darstellung einer nat. Zahl n gegeben durch

$$\begin{aligned} n &= (a_{k-1} a_{k-2} \ldots a_1 a_0)_m \\ n &= a_{k-1} m^{k-1} + a_{k-2} m^{k-2} + \ldots + a_1 m + a_0 \\ n &= (\ldots ((a_{k-1} m + a_{k-2})\, m + a_{k-3}) \ldots + a_1)\, m + a_0 \qquad \text{HORNER-Schema} \end{aligned}$$

und $0 \leq a_0, a_1, a_2, \ldots, a_{k-2}, a_{k-1} < m$. a_i sind die **Ziffern** im m-adischen System.

Satz 3.3 (Rechtfertigung der m-adischen Darstellung)
Jede nat. Zahl n besitzt eine eindeutig bestimmte Darstellung der obigen Form.

Beweis:
mit Hilfe von Lemma 1 ∎

3.1.2 Größter gemeinsamer Teiler

Wir betrachten: $[\mathbb{N}, \backslash]$ ist eine halbgeordnete Menge mit den Eigenschaften

$$\begin{aligned} 1 \backslash n, \quad n \backslash 0 \\ 1 = \min_{\backslash} \mathbb{N}, \quad 0 = \max_{\backslash} \mathbb{N} \end{aligned}$$

wissen: $d \backslash n$ und $d \backslash m \ \rightarrow d \backslash (an + bm)$ und $d \backslash (an + bm)$, falls $an \geq bm$

Definition 3.2
Es seien $m, n \in \mathbb{N}$. g heißt größter gemeinsamer Teiler von n und $m \Leftrightarrow_{df}$

1. $g \backslash n$ und $g \backslash m$

2. $\forall d\,((d\backslash n \wedge d\backslash m) \to d\backslash g)$

Eigenschaft 1 bedeutet: g ist untere Schranke von $\{n, m\}$.
Eigenschaft 1 mit 2 bedeutet: g ist größte untere Schranke von $\{n, m\}$

Schreibweise:

$$g = \mathrm{ggT}(n, m)$$

Satz 3.4
Für je zwei natürliche Zahlen ex. der größte gemeinsame Teiler (und ist eindeutig bestimmt)

Beweis:
$\mathrm{ggT}(0,0) = 0,\ \mathrm{ggT}(n,0) = n,\ \mathrm{ggT}(0,m) = m$
Es seien $n \geq m > 0$. Wir definieren

$$\begin{aligned} D =& \{an - bm \mid a, b \in \mathbb{N} \wedge an \geq bm\} \\ & \cup \{am - bn \mid a, b \in \mathbb{N} \wedge am \geq bn\} \end{aligned}$$

Eigenschaften:

1. $o, n, m \in D$
2. Falls $d\backslash n$ und $d\backslash m$, dann gilt $d\backslash c$ für alle $c \in D$

Daraus folgt: $D\backslash\{0\} \neq \varnothing$
Also ex. ein Minimum in $D\backslash\{0\}$
Es sei $g = \min_{\leq}(D\backslash\{0\})$

Behauptung: $g \stackrel{!}{=} \mathrm{ggT}(n, m)$
zunächst: g ist Teiler von n! Da $g \in D\backslash\{0\}$, also gilt entweder $g = an - bm$ oder $g = am - bn$.
Außerdem gilt: $g \leq n$ (wegen Eigenschaft 1)

Wegen Lemma 1 gibt es q, r mit $n = q \cdot g + r$ und $0 \leq r < g$.
Also gilt: $r = n - q \cdot g$.

Angenommen es gilt $g = an - bm$:
Dann ist

$$\begin{aligned} r &= n - q(an - bm) \geq 0 \\ &= qbm - (qa - 1)n \end{aligned}$$

Das heißt $r \in D$, da $r < g$ und $g = \min_{\leq}(D\backslash\{0\})$.
Hieraus folgt: $r = 0$!

Also gilt (in Lemma 1): $n = qg$, d. h. $g\backslash n$

Angenommen es gilt $g = am - bn$:
Damit ist $r = n - q(am - bn) = (qb + 1)n - (qa)m$
Also wieder $r \in D$ und damit $r = 0$! Also auch $g \backslash n$.

Analog: g ist ein Teiler von m!

Bleibt zu zeigen: g ist ein Infimum von $\{n, m\}$ bezüglich $\backslash$.
Dies folgt sofort aus Eigenschaft 2 von D. ■

Folgerung: Der $\mathrm{ggT}(n, m)$ lässt sich schreiben als Linearkombination $g = a \cdot n - b \cdot m$ oder $g = a \cdot m - b \cdot n$.

Dies lässt sich für *ganze* Zahlen A und B schreiben als

$$g = An + Bm$$

wobei $\mathrm{sgn}(A) \neq \mathrm{sgn}(B)$

Index