Übersichtsfolien zur Übung

Diskrete Strukturen im Wintersemester 2013/2014

Markus Kaiser

8. Januar 2014

Organisatorisches

- Markus Kaiser
  - Mail: tutor@zfix.org
  - Web: ds.zfix.org
- Vorlesung
  - Dienstag 13:45-15:15 in MI HS1
  - Donnerstag 10:15-11:45 in MI HS1
- Meine Tutorübungen
  - Dienstag 12:00-14:00 in 03.09.014
  - Dienstag 16:15-17:45 in 03.11.018
  - Offiziell müsst ihr in die angemeldete Übung!

Übungsablauf

- Hausaufgaben
  - Abgabedatum auf Übungsblatt
  - Abgabe in Briefkästen, Rückgabe in Tutorübung
  - Geheftet, Handschriftlich, Deckblatt
  - Teams aus 3 oder 4 Stundenten
  - Teams nicht änderbar, nicht gruppenübergreifend
  - Üblicherweise schwerer als Klausurstoff
- Notenbonus
  - „Bepunktung“ mit Ampelfarben
  - Bei $\frac{2}{3}$ mindestens gelb
  - 0.3 Notenstufen Bonus auf bestandene Klausur
- Tutoraufgaben
  - Lösen wir zusammen in den Übungen
  - Üblicherweise schwerer als Klausurstoff

Was machen wir hier?

- Mathematische Grundlagen
  - Mengen, Relationen, Funktionen
  - Logik
  - Beweise
- Kombinatorik
  - Zählkoeffizienten
  - Spaß mit Urnen
- Graphentheorie
  - Definition
  - Ein paar Algorithmen
- Algebra
  - Modulo
  - Algebren
  - Gruppen, vielleicht Körper

Definition (Menge)

Eine Menge ist eine ungeordnete Sammlung unterscheidbarer Objekte.
Mit Mengenklammern werden Objekte zusammengefasst.

$$A := \{a, b, \ldots, z\}$$

Man nennt a ein Element von A, es gilt $a \in A$.

- Reihenfolge ist egal
- Elemente kommen nicht mehrfach vor

Beispiel

- $\{a, b, c, a, c\} = \{a, b, c\} = \{c, a, b\}$
- $\mathbb{N} := \{1, 2, 3, \ldots\}$
- $\emptyset := \{\}$

Definition (Extensionale Schreibweise)

Die extensionale Schreibweise einer Menge zählt ihre Elemente auf.

$$M := \{x_1, x_2, x_3, \ldots\}$$

Beispiel

- $A := \{2, 4, 6, \ldots\}$
- $B := \{1, 2, 3, 4\} = [4]$
- $C := \{2, 3, 5, 7, 11, \ldots\}$
- $D := \{\alpha, a, ☺, 8, \{1, 2\}, \mathbb{N}\}$

Definition (Intensionale Schreibweise)

Die intensionale Schreibweise beschreibt eine Menge durch charakteristische Eigenschaften.

$$M := \{x \in \Omega \mid P(x)\}$$

M enthält alle Elemente im Universum Ω mit der Eigenschaft P.

Beispiel

- $A := \{2, 4, 6, \ldots\} = \{x \in \mathbb{N} \mid x \text{ gerade}\} = \{2x : x \in \mathbb{N}\}$
- $B := \{1, 2, 3, 4\} = \{x \in \mathbb{N} \mid x \leq 4\}$
- $C := \{2, 3, 5, 7, 11, \ldots\} = \{x \in \mathbb{N} \mid x \text{ prim}\}$

Bezeichnungen

- Objekte in Mengen

$a \in A$	a ist Element von A
$b \notin A$	b ist kein Element von A
$\lvert A \rvert$	Anzahl der Elemente in A, Kardinalität

- Relationen zwischen Mengen

$B \subseteq A$	B ist Teilmenge von A, $\quad x \in B \rightarrow x \in A$
$B \subset A$	B ist echte Teilmenge von A
$B = A$	$B \subseteq A$ und $A \subseteq B$

Beispiel

- $1 \in \{1, 2, 3, 4\}$, aber $9 \notin \{1, 2, 3, 4\}$
- $\{1, 2\} \subseteq \{1, 2, 3, 4\}$, aber $\{1, 5\} \not\subseteq \{1, 2\}$
- $\emptyset \subseteq [5] \subseteq \mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Operationen

$\overline{A}$	$:= \{x \mid x \notin A\}$	Komplement
$A \cup B$	$:= \{x \mid x \in A \text{ oder } x \in B\}$	Vereinigung
$A \cap B$	$:= \{x \mid x \in A \text{ und } x \in B\}$	Schnitt
$A \setminus B$	$:= A \cap \overline{B}$	Differenz
$A \triangle B$	$:= (A \setminus B) \cup (B \setminus A)$	Symmetrische Differenz

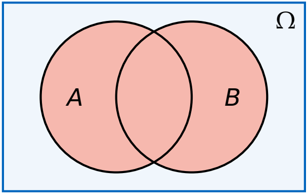
Für mehrere Mengen schreibt man

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

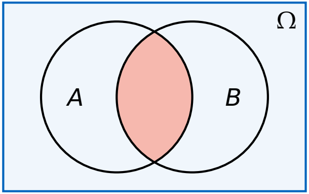
$$\bigcup_{i=1}^{n} A_i := A_1 \cup A_2 \cup \ldots \cup A_n$$

Venn-Diagramme visualisieren Mengen $A, B, \ldots$ im Universum Ω.

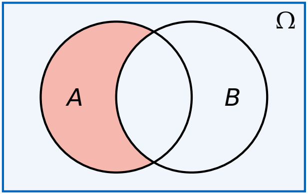
- $A \cup B$



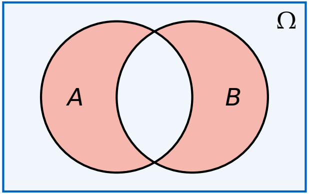
- $A \cap B$



- $A \setminus B$



- $A \triangle B = (A \setminus B) \cup (B \setminus A)$



Satz (De Morgansche Gesetze)

Sind A, B Mengen, dann gilt

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}$$

Für Mengen A_i gilt

$$\overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A_i} \qquad \overline{\bigcap_{i=1}^{n} A_i} = \bigcup_{i=1}^{n} \overline{A_i}$$

- Zusammen mit $\overline{\overline{A}} = A$ wichtigste Regel
- Gilt auch in der Aussagenlogik

Definition (Potenzmenge)

Die Potenzmenge $\mathcal{P}(M)$ zu einer Menge M ist die Menge all ihrer Teilmengen.

$$\mathcal{P}(M) := \{X \mid X \subseteq M\}$$

- $\mathcal{P}(M)$ enthält für endliche Mengen genau $2^{|M|}$ Elemente
- Man schreibt deshalb auch 2^M
- Es ist $M \in \mathcal{P}(M)$ und $\emptyset \in \mathcal{P}(M)$

Beispiel

Für $M = \{a, b, c\}$ ist

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

mit $|\mathcal{P}(M)| = 2^3 = 8$

Definition (Tupel)

Ein n-Tupel ist eine geordnete Sammlung n beliebiger Objekte.
Mit Tupelklammern werden Objekte zusammengefasst.

$$T := (t_1, t_2, \ldots, t_n)$$

- Reihenfolge nicht egal
- Elemente dürfen mehrmals vorkommen

Beispiel

- $(a, b, c) \neq (c, a, b) \neq (a, b, c, a, c)$
- $(1, 2, 3) \neq \{3, 2, 1\} = \{1, 2, 3\}$
- $(\{\alpha, \beta\}, \emptyset, \mathbb{N})$

Definition (Kreuzprodukt)

Sind A, B Mengen, dann ist ihr kartesisches Produkt (Kreuzprodukt)

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

Für Mengen A_i ist

$$A_1 \times \ldots \times A_n := \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}$$

- Für endliche A_i ist $|A_1 \times \ldots \times A_n| = |A_1| \cdot \ldots \cdot |A_n|$
- Man schreibt $A^n := \underbrace{A \times \ldots \times A}_{\text{n mal}}$ mit $A^0 = \{\emptyset\}$

Beispiel

- $\{1, 2\} \times \{a, b\} = \{(1, a), (2, a), (1, b), (2, b)\}$
- $\{\alpha, \beta\}^2 = \{(\alpha, \alpha), (\alpha, \beta), (\beta, \alpha), (\beta, \beta)\}$

Definition (Relation)

Eine binäre Relation R verbindet Elemente zweier Mengen A und B.

$$R \subseteq A \times B$$

Ist $(a, b) \in R$, so schreibt man auch $a \mathrm{R} b$.

- Eine Relation über $M \times M$ nennt man homogen
- Es gibt $|\mathcal{P}(A \times B)|$ Relationen über A, B

Beispiel

- Die Gleichheitsrelation über $\mathbb{N} \times \mathbb{N}$
  $\{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(7,7)\ldots\}$
- Die Teilbarkeitsrelation über $\mathbb{N}$
  $\{(1,1),(1,2),(1,3),\ldots,(2,2),(2,4),\ldots,(3,3),(3,6),\ldots\}$

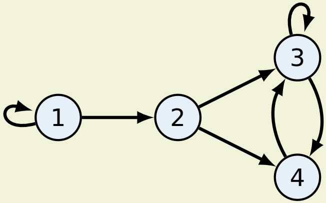
Grafische Darstellung von Relationen

Jede Relation $R \subseteq M \times M$ kann als Graph dargestellt werden. Die Elemente aus M werden zu Knoten und für jedes Tupel $(a, b) \in R$ wird ein Pfeil von a nach b eingefügt.

Beispiel

Sei $R \subseteq [4] \times [4]$ eine Relation über den natürlichen Zahlen.

$$R := \{(1,1), (1,2), (2,3), (2,4), (3,3), (3,4), (4,3)\}$$



Eigenschaften homogener Relationen

Sei $R \in M \times M$ eine homogene Relation. Man nennt R

reflexiv	$\forall a \in M.\ (a, a) \in R$
total	$\forall a, b \in M.\ (a, b) \in R \lor (b, a) \in R$
symmetrisch	$\forall a, b \in M.\ (a, b) \in R \to (b, a) \in R$
asymmetrisch	$\forall a, b \in M.\ (a, b) \in R \to (b, a) \notin R$
antisymmetrisch	$\forall a, b \in M.\ (a, b) \in R \land (b, a) \in R \to a \equiv b$
transitiv	$\forall a, b, c \in M.\ (a, b) \in R \land (b, c) \in R \to (a, c) \in R$

- Jede totale Relation ist reflexiv
- Jede asymmetrische Relation ist antisymmetrisch
- Äquivalenzrelationen sind reflexiv, symmetrisch und transitiv
- R^+ ist die transitive Hülle, R^* die reflexive transitive Hülle

Definition (Funktion)

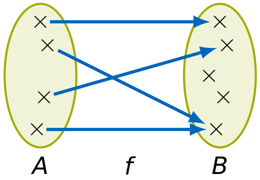
Eine Relation $f \subseteq A \times B$ ist eine Funktion von A nach B wenn es für alle $a \in A$ genau ein Element $b \in B$ mit $a \, \mathfrak{f} \, b$ gibt.

$$\forall a \in A. \, |\{(a,b) \mid b \in B\}| = 1$$

Man schreibt

$$\begin{aligned} f : A &\to B \\ a &\mapsto f(a) = b \end{aligned}$$

$A \to B$ bezeichnet die Menge aller Funktionen von A nach B.



Definition (Bild)

Sei $f : A \to B$ eine Funktion, $X \subseteq A$, $Y \subseteq B$, $b \in B$. Dann ist

$$f(X) := \{f(x) \mid x \in X\}$$

das Bild der Menge X unter f. Außerdem ist

$$f^{-1}(b) := \{a \mid a \in A, f(a) = b\}$$

$$f^{-1}(Y) := \bigcup_{y \in Y} \left\{f^{-1}(y)\right\}$$

das Urbild des Elements b und der Menge Y unter f.

- Man nennt $A = f^{-1}(B)$ Urbild oder Definitionsmenge von f
- Man nennt $f(A) \subseteq B$ Bild oder Wertemenge von f

Definition (Funktionskomposition)

Seien $f : B \to C$ und $g : A \to B$ Funktionen. Dann ist

$$\begin{aligned} h : A &\to C \\ a &\mapsto (f \circ g)(a) = f(g(a)) \end{aligned}$$

die Komposition der Funktionen f und g.
Man ließt $f \circ g$ als „f nach g“.

Man definiert die Potenzierung von Funktionen ähnlich der Mengentheorie.

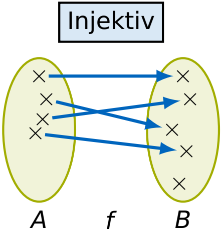
$$\begin{aligned} f^0 &:= id \\ f^n &:= \underbrace{f \circ \ldots \circ f}_{\text{n mal}} \end{aligned}$$

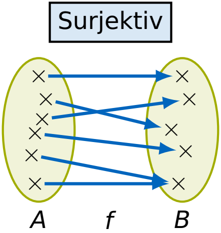
Dabei bezeichnet id die Identität mit $id(x) := x$.

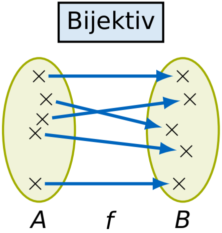
Eigenschaften von Funktionen

Sei $f : A \to B$ eine Funktion. Man nennt f

injektiv	$\forall b \in B. \left\|f^{-1}(b)\right\| \leq 1$	(Kein b wird doppelt getroffen)
surjektiv	$\forall b \in B. \left\|f^{-1}(b)\right\| \geq 1$	(Jedes b wird getroffen)
bijektiv	$\forall b \in B. \left\|f^{-1}(b)\right\| = 1$	(Jedes b wird genau einmal getroffen)







Definition (Syntax der Aussagenlogik)

Aussagenlogische Formeln bestehen aus Konstanten, Variablen und Operatoren. Die Menge $\mathcal{F}$ aller Formeln ist induktiv definiert.

- $\text{false} = 0 = \bot \in \mathcal{F}, \quad \text{true} = 1 = \top \in \mathcal{F}$ (Konstanten)
- $V = \{a, b, c, \ldots\} \subseteq \mathcal{F}$ (Variablen)
- Ist $A \in \mathcal{F}$ eine aussagenlogische Formel, dann auch

$$\neg A \in \mathcal{F} \qquad \text{(Negation)}$$

- Sind $A, B \in \mathcal{F}$ aussagenlogische Formeln, dann auch

$$(A \wedge B) \in \mathcal{F} \qquad \text{(Konjunktion)}$$
$$(A \vee B) \in \mathcal{F} \qquad \text{(Disjunktion)}$$
$$(A \rightarrow B) \in \mathcal{F} \qquad \text{(Implikation)}$$

Alle Formeln lassen sich so konstruieren.

Definition (Bindungsregeln)

Die Bindungsstärke der Operatoren in absteigender Reihenfolge ist

$$\neg \quad \wedge \quad \vee \quad \rightarrow \quad \leftrightarrow$$

Die Implikation ist rechtsassoziativ

$$a \rightarrow b \rightarrow c \rightarrow d \quad \text{steht für} \quad (a \rightarrow (b \rightarrow (c \rightarrow d)))$$

- Üblicherweise klammert man $\wedge$ und $\vee$

$$(a \wedge b) \vee c \quad \text{statt} \quad a \wedge b \vee c$$

Beispiel

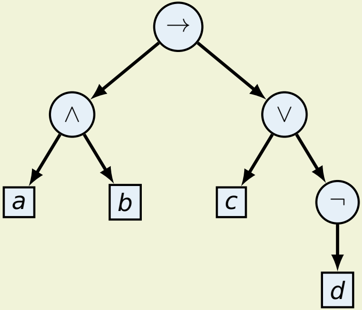
- $\neg a \wedge b$ steht für $((\neg a) \wedge b)$
- $a \wedge b \rightarrow c \vee \neg d$ steht für $((a \wedge b) \rightarrow (c \vee (\neg d)))$

Syntaxbaum

Syntaxbäume visualisieren in welcher Reihenfolge die Regeln zur induktiven Definition angewandt werden müssen, um eine Formel zu erzeugen.

Beispiel

Sei $F :\equiv a \wedge b \rightarrow c \vee \neg d$ dann ist der dazu passende Syntaxbaum



Definition (Belegung)

Eine passende Belegung β zu einer Formel F ordnet jeder Variable in V einen Wahrheitswert aus $\{0, 1\}$ zu. Es ist

$$\beta : V \to \{0, 1\}$$

- Belegungen formalisieren Einsetzen
- Für n Variablen existieren 2^n Belegungen

Beispiel

Sei $F := \neg(a \wedge b)$ mit $V = \{a, b\}$ und

$$\begin{aligned} \beta : \{a, b\} &\to \{0, 1\} \\ a &\mapsto 1 \\ b &\mapsto 0 \end{aligned}$$

Dann ist β eine zu F passende Belegung.

Definition (Semantik einer Formel)

Die Semantik $[F]$ einer aussagenlogischen Formel F ist eine Funktion, die jeder passenden Belegung β einen Wahrheitswert zuordnet.
Sei $\mathcal{B} = \{\beta_0, \beta_1, \ldots\}$ die Menge aller Belegungen zu F. Dann ist

$$[F] : \mathcal{B} \to \{0, 1\}$$

- Die Semantik löst eingesetzte Formeln auf
- Wird anhand der induktiven Syntax definiert
- Es gibt syntaktisch verschiedene Formeln gleicher Semantik

Beispiel

Sei $F :\!= (G \to H)$ mit G, H Formeln. Dann ist

$$[F](\beta) = \begin{cases} 0 & \text{falls } [G](\beta) = 1 \text{ und } [H](\beta) = 0 \\ 1 & \text{sonst} \end{cases}$$

Wahrheitstabelle

Die Semantik einer Formel kann mit Hilfe einer Wahrheitstabelle visualisiert werden. Die Tabelle gibt den Wahrheitswert der Formel für jede mögliche Belegung an.

Beispiel

Sei $F :\equiv a \vee b \rightarrow \neg c \wedge b$. Die zu $[F]$ gehörige Wahrheitstabelle ist

a	b	c	$a \vee b$	$\rightarrow$	$\neg c$	$\wedge$	b
0	0	0	0	1	1	0	
0	0	1	0	1	0	0	
0	1	0	1	1	1	1	
0	1	1	1	0	0	0	
1	0	0	1	0	1	0	
1	0	1	1	0	0	0	
1	1	0	1	1	1	1	
1	1	1	1	0	0	0	

Wahrheitstabelle

Die Semantik einer Formel kann mit Hilfe einer Wahrheitstabelle visualisiert werden. Die Tabelle gibt den Wahrheitswert der Formel für jede mögliche Belegung an.

Beispiel

Sei $F :\equiv a \vee b \rightarrow \neg c \wedge b$. Die zu $[F]$ gehörige Wahrheitstabelle ist

a	b	c	$a \vee b$	$\rightarrow$	$\neg c$	$\wedge$	b
0	0	0	0	1	1	0	
0	0	1	0	1	0	0	
0	1	0	1	1	1	1	
0	1	1	1	0	0	0	
1	0	0	1	0	1	0	
1	0	1	1	0	0	0	
1	1	0	1	1	1	1	
1	1	1	1	0	0	0	

Wahrheitstabelle

Die Semantik einer Formel kann mit Hilfe einer Wahrheitstabelle visualisiert werden. Die Tabelle gibt den Wahrheitswert der Formel für jede mögliche Belegung an.

Beispiel

Sei $F :\equiv a \vee b \rightarrow \neg c \wedge b$. Die zu $[F]$ gehörige Wahrheitstabelle ist

a	b	c	$a \vee b$	$\rightarrow$	$\neg c$	$\wedge$	b
0	0	0	0	1	1	0	
0	0	1	0	1	0	0	
0	1	0	1	1	1	1	
0	1	1	1	0	0	0	
1	0	0	1	0	1	0	
1	0	1	1	0	0	0	
1	1	0	1	1	1	1	
1	1	1	1	0	0	0	

Äquivalente Formeln

Definition (Äquivalente Formeln)

Man nennt zwei Formeln äquivalent, wenn sie dieselbe Semantik besitzen.
Seien F, G Formeln mit Belegungen $\mathcal{B} = \mathcal{B}_F = \mathcal{B}_G$. F und G sind äquivalent wenn

$$\forall \beta \in \mathcal{B}. [F](\beta) = [G](\beta)$$

Man schreibt $F \equiv G$ oder $F \leftrightarrow G$.

Beispiel

Für $F := a \rightarrow b$ und $G := \neg a \vee b$ gilt $F \equiv G$.

a	b	$a \rightarrow b$	$\neg a$	$\vee$	b
0	0	1	1	1	
0	1	1	1	1	
1	0	0	0	0	
1	1	1	0	1	

Eigenschaften aussagenlogischer Formeln

Sei F eine aussagenlogische Formel mit Variablen V und der Menge der passenden Belegungen $\mathcal{B}$. Man nennt F

erfüllbar	$\exists \beta \in \mathcal{B}.[F](\beta) = 1$	(F kann wahr sein)
unerfüllbar	$\forall \beta \in \mathcal{B}.[F](\beta) = 0$	(F ist nie wahr)
gültig	$\forall \beta \in \mathcal{B}.[F](\beta) = 1$	(F ist immer wahr)

- Eine unerfüllbare Formel nennt man Widerspruch
- Eine gültige Formel nennt man Tautologie

Äquivalenzregeln

Identität	$F \wedge \text{true} \equiv F$	$F \vee \text{false} \equiv F$
Dominanz	$F \vee \text{true} \equiv \text{true}$	$F \wedge \text{false} \equiv \text{false}$
Idempotenz	$F \vee F \equiv F$	$F \wedge F \equiv F$
Doppelte Negation	$\neg\neg F \equiv F$	
Triviale Tautologie	$F \vee \neg F \equiv \text{true}$	
Triviale Kontradiktion	$F \wedge \neg F \equiv \text{false}$	

Kommutativität	$F \vee G \equiv G \vee F$
	$F \wedge G \equiv G \wedge F$
Assoziativität	$(F \vee G) \vee H \equiv F \vee (G \vee H)$
	$(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$
Distributivität	$F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
	$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
De Morgan	$\neg(F \wedge G) \equiv \neg F \vee \neg G$
	$\neg(F \vee G) \equiv \neg F \wedge \neg G$

Implikation	$F \rightarrow G \equiv \neg F \vee G$
Bikonditional	$F \leftrightarrow G \equiv \neg(F \otimes G)\ [\equiv (F \rightarrow G) \wedge (G \rightarrow F)]$

Definition (Literal)

Ein Literal ist eine Variable $v \in V$ oder die Negation $\neg v$ einer Variable.

Definition (Klausel)

Eine Klausel verknüpft mehrere Literale mit einem assoziativen Operator.

Beispiel

Seien $a, \neg b, c$ Literale. Dann sind

- $a \wedge \neg b \wedge c$
- $a \vee \neg b \vee c$

Klauseln.

Definition (Disjunktive Normalform)

Eine DNF-Klausel ist eine Konjunktion von Literalen L_i.
Eine Formel F, ist in Disjunktiver Normalform, wenn sie eine Disjunktion von DNF-Klauseln ist.

$$F := \bigvee \bigwedge_i L_i$$

- Ausnahme: false ist auch in DNF

Beispiel

F ist in DNF.

$$F := \underbrace{(a \wedge b \wedge \neg c)}_{\text{DNF-Klausel}} \vee \underbrace{(\neg b \wedge c)}_{\text{DNF-Klausel}} \vee \underbrace{(\neg a \wedge b \wedge \neg c)}_{\text{DNF-Klausel}}$$

Definition (Konjunktive Normalform)

Eine KNF-Klausel ist eine Disjunktion von Literalen L_i.
Eine Formel F, ist in Konjunktiver Normalform, wenn sie eine Konjunktion von KNF-Klauseln ist.

$$F := \bigwedge \bigvee_i L_i$$

- Ausnahme: true ist auch in KNF

Beispiel

F ist in KNF.

$$F := \underbrace{(\neg a \vee b)}_{\text{KNF-Klausel}} \wedge \underbrace{(\neg b \vee c)}_{\text{KNF-Klausel}} \wedge \underbrace{(a \vee b \vee \neg c)}_{\text{KNF-Klausel}}$$

- Jede nicht-triviale Formel ist in DNF und KNF umwandelbar
- Durch Äquivalenzumformungen berechenbar (exponentiell groß!)
- Oder: Konstruktion mit Wahrheitstabellen

Normalformen aus Wahrheitstabellen

Gegeben eine Formel F und ihre Wahrheitstabelle

- DNF
  1. Betrachte Zeilen mit Eintrag 1
  2. Bilde Konjunktion aus der Belegung
  3. Bilde Disjunktion aller erhaltenen Klauseln
- KNF
  1. Betrachte Zeilen mit Eintrag 0
  2. Bilde Disjunktion aus der Negation der Belegung
  3. Bilde Konjunktion aller erhaltenen Klauseln

Beispiel

Gegeben eine Formel F mit folgender Semantik

a	b	c	F
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

F dargestellt in

- DNF $\quad (\neg a \wedge b \wedge c) \vee (a \wedge \neg b) \vee (a \wedge b \wedge \neg c)$
- KNF $\quad (a \vee b) \wedge (\neg a \vee b \vee \neg c) \wedge (\neg a \vee \neg b \vee \neg c)$

Mengendarstellung der KNF

Eine Formel $F = \bigwedge \bigvee L_i$ in KNF kann in einer Mengendarstellung repräsentiert werden.

- Klauseln werden durch Mengen von Literalen dargestellt

$$\{a, \neg b, c\} \text{ steht für } (a \vee \neg b \vee c)$$

- KNF-Formeln sind Mengen von Klauseln

$$\{\{\neg a\}, \{a, \neg b, c\}\} \text{ steht für } \neg a \wedge (a \vee \neg b \vee c)$$

- $\emptyset$ steht für true, $\{\emptyset\}$ für false

Beispiel

Gegeben $F := (a \vee b) \wedge (\neg a \vee b \vee \neg c) \wedge (\neg a \vee \neg b \vee \neg c)$ in KNF.

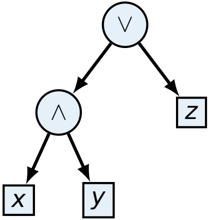
$$\{\{a, b\}, \{\neg a, b, \neg c\}, \{\neg a, \neg b, \neg c\}\}$$

Idee

Erzeuge die KNF aus dem Syntaxbaum

1. Weise jedem inneren Knoten eine Variable zu
2. Variablen sind abhängig von ihren Kindern
3. Berechne kleine KNFs und führe diese zusammen

$$
\begin{aligned}
(x \land y) \lor z \equiv\ & \\
& \land (A_\lor \leftrightarrow A_\land \lor z) \\
& \land (A_\land \leftrightarrow x \land y) \\
\equiv\ & \\
& \land (A_\lor \lor \neg A_\land) \land (A_\lor \lor \neg z) \\
& \qquad \land (\neg A_\lor \lor A_\land \lor z) \\
& \land (\neg A_\land \lor x) \land (\neg A_\land \lor y) \\
& \qquad \land (A_\land \lor \neg x \lor \neg y)
\end{aligned}
$$

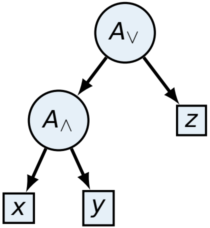


Idee

Erzeuge die KNF aus dem Syntaxbaum

1. Weise jedem inneren Knoten eine Variable zu
2. Variablen sind abhängig von ihren Kindern
3. Berechne kleine KNFs und führe diese zusammen

$$
\begin{aligned}
(x \wedge y) \vee z \equiv\ & \\
& \wedge (A_\vee \leftrightarrow A_\wedge \vee z) \\
& \wedge (A_\wedge \leftrightarrow x \wedge y) \\
\equiv\ & \\
& \wedge (A_\vee \vee \neg A_\wedge) \wedge (A_\vee \vee \neg z) \\
& \qquad \wedge (\neg A_\vee \vee A_\wedge \vee z) \\
& \wedge (\neg A_\wedge \vee x) \wedge (\neg A_\wedge \vee y) \\
& \qquad \wedge (A_\wedge \vee \neg x \vee \neg y)
\end{aligned}
$$

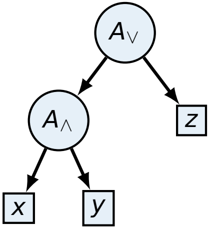


Idee

Erzeuge die KNF aus dem Syntaxbaum

1. Weise jedem inneren Knoten eine Variable zu
2. Variablen sind abhängig von ihren Kindern
3. Berechne kleine KNFs und führe diese zusammen

$$
\begin{aligned}
(x \land y) \lor z \equiv \quad & A_\lor \\
& \land (A_\lor \leftrightarrow A_\land \lor z) \\
& \land (A_\land \leftrightarrow x \land y) \\
\equiv \quad & \\
& \land (A_\lor \lor \neg A_\land) \land (A_\lor \lor \neg z) \\
& \qquad \land (\neg A_\lor \lor A_\land \lor z) \\
& \land (\neg A_\land \lor x) \land (\neg A_\land \lor y) \\
& \qquad \land (A_\land \lor \neg x \lor \neg y)
\end{aligned}
$$

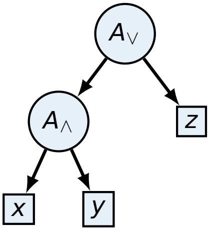


Idee

Erzeuge die KNF aus dem Syntaxbaum

1. Weise jedem inneren Knoten eine Variable zu
2. Variablen sind abhängig von ihren Kindern
3. Berechne kleine KNFs und führe diese zusammen

$$
\begin{aligned}
(x \land y) \lor z \equiv\ & A_\lor \\
& \land (A_\lor \leftrightarrow A_\land \lor z) \\
& \land (A_\land \leftrightarrow x \land y) \\
\equiv\ & A_\lor \\
& \land (A_\lor \lor \neg A_\land) \land (A_\lor \lor \neg z) \\
& \qquad \land (\neg A_\lor \lor A_\land \lor z) \\
& \land (\neg A_\land \lor x) \land (\neg A_\land \lor y) \\
& \qquad \land (A_\land \lor \neg x \lor \neg y)
\end{aligned}
$$



Definition (DPLL-Belegung)

Sei F eine Formel in KNF und p eine Variable von F.
Dann bezeichnet $F[p\backslash \mathrm{true}]$ die Formel, die entsteht, wenn jedes Vorkommnis von p in F durch true ersetzt und vereinfacht wird.

DPLL

Gegeben eine Formel F in KNF

- Wenn $F = \mathrm{true}$ dann antworte erfüllbar
- Wenn $F = \mathrm{false}$ dann antworte unerfüllbar
- Sonst
  1. Wähle eine Variable p in F
  2. Prüfe ob $F[p\backslash \mathrm{true}]$ oder $F[p\backslash \mathrm{false}]$ erfüllbar

- Schlaue Wahl der Variable beschleunigt Ausführung
- Wähle Variablen die einzeln stehen (One-Literal-Rule)

Definition (Resolvent)

Seien K_1, K_2 und R Klauseln in Mengendarstellung. Dann heißt R Resolvent von K_1 und K_2 wenn $L \in K_1$, $\neg L \in K_2$ und

$$R = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$$

Resolution

Gegeben eine Formel F in KNF in Mengendarstellung.

while $\square = \emptyset \notin F$ **do**
  $R \leftarrow$ Resolvent aus F mit $R \notin F$
  if R existiert **then**
    $F \leftarrow F \cup R$
  else
    return erfüllbar
return unerfüllbar

Definition (Kalkül)

Ein Logikkalkül stellt Inferenzregeln bereit, mit denen Formeln syntaktisch umgeformt werden können.

Definition (Folgerung)

F folgt aus A, wenn mit Hilfe der Semantik der Aussagenlogik F unter der Annahme dass A gilt zu true ausgewertet wird. Wir schreiben

$$A \models F$$

Definition (Ableitung)

F kann aus A abgeleitet werden, wenn mit Hilfe syntaktischer Umformungen in einem Logikkalkül F unter der Annahme A bewiesen werden kann. Wir schreiben

$$A \vdash F$$

Eigenschaften von Kalkülen

korrekt (sound) Es können nur semantisch gültige Formeln abgeleitet werden.

Aus $A \vdash F$ folgt $A \models F$

vollständig (complete) Alle semantisch gültigen Formeln können abgeleitet werden.

Aus $A \models F$ folgt $A \vdash F$

- Für uns nur korrekte vollständige Kalküle
- Beispiel für die Aussagenlogik: Natürliches Schließen
- Es gibt keine solchen Kalküle für die
  - Prädikatenlogik
  - Arithmetik
- Deshalb sind nicht alle Sätze der Mathematik beweisbar

Natürliches Schließen

	Introduktion	Elimination
$\wedge$	$\dfrac{\tau \qquad \varphi}{\tau \wedge \varphi}\ {+\wedge}$	$\dfrac{\tau \wedge \varphi}{\tau}\ {-\wedge_1}$ $\quad$ $\dfrac{\tau \wedge \varphi}{\varphi}\ {-\wedge_2}$
$\vee$	$\dfrac{\tau}{\tau \vee \varphi}\ {+\vee_1}$ $\quad$ $\dfrac{\varphi}{\tau \vee \varphi}\ {+\vee_2}$	$\dfrac{\tau \vee \varphi \qquad \boxed{\begin{array}{c}\tau\\ \vdots\\ \chi\end{array}} \qquad \boxed{\begin{array}{c}\varphi\\ \vdots\\ \chi\end{array}}}{\chi}\ {-\vee}$
$\rightarrow$	$\dfrac{\boxed{\begin{array}{c}\tau\\ \vdots\\ \varphi\end{array}}}{\tau \rightarrow \varphi}\ {+\rightarrow}$	$\dfrac{\tau \qquad \tau \rightarrow \varphi}{\varphi}\ {-\rightarrow}$, MP
$\neg$	$\dfrac{\boxed{\begin{array}{c}\tau\\ \vdots\\ \bot\end{array}}}{\neg\tau}\ {+\neg}$	$\dfrac{\tau \qquad \neg\tau}{\bot}\ {-\neg}$

	Introduktion	Elimination
$\perp$		$\dfrac{\perp}{\tau}\ {-\perp}$
$\neg\neg$	$\dfrac{\tau}{\neg\neg\tau}\ {+\neg\neg}$	$\dfrac{\neg\neg\tau}{\tau}\ {-\neg\neg}$

- Praktische abgeleitete Regeln

$$\frac{}{\tau \vee \neg\tau}\ \text{LEM}$$

$$\frac{\boxed{\begin{array}{c}\neg\tau\\ \vdots\\ \perp\end{array}}}{\tau}\ {-\neg},\ \text{PBC}$$

$$\frac{\neg\varphi \qquad \tau \to \varphi}{\neg\tau}\ \text{MT}$$

Definition (Term)

Die Menge $\mathcal{T}$ aller Terme ist induktiv definiert.

- Jede Konstante ist in $\mathcal{T}$
- Jede Variable ist in $\mathcal{T}$
- Sind f eine Funktion und $t_1, \ldots, t_n$ Terme, dann auch

$$f(t_1, \ldots, t_n)$$

Funktionen wandeln Terme in Terme um. Wir beschreiben sie mit Kleinbuchstaben.

Definition (Prädikat)

Prädikate P wandeln Terme in Wahrheitswerte um. Wir beschreiben sie mit Großbuchstaben.
Die Menge $\mathcal{P}$ enthält alle Prädikate.

Definition (Syntax der Prädikatenlogik)

Die Menge $\mathcal{L}$ aller prädikatenlogischen Formeln ist induktiv definiert. Seien $A, B \in \mathcal{L}$, $t_i \in \mathcal{T}$ und $P \in \mathcal{P}$. Dann sind alle Formeln

- Grundbausteine

$$V = \{a, b, \dots\} \subseteq \mathcal{L} \qquad \text{(Variablen)}$$

$$P(t_1, \dots, t_n) \in \mathcal{L} \qquad \text{(Prädikate, Konstanten)}$$

$$t_i = t_j \in \mathcal{L} \qquad \text{(Gleichheit)}$$

- Verknüpfungen der Aussagenlogik

$$\neg A \in \mathcal{L} \qquad \text{(Negation)}$$

$$(A \wedge B), (A \vee B) \in \mathcal{L} \qquad \text{(Konjunktion, Disjunktion)}$$

$$(A \rightarrow B) \in \mathcal{L} \qquad \text{(Implikation)}$$

- Quantoren

$$\exists x.A \in \mathcal{L} \qquad \text{(Existenzquantor)}$$

$$\forall x.A \in \mathcal{L} \qquad \text{(Allquantor)}$$

Definition (Bindungsregeln)

Die Bindungsstärke der Operatoren in absteigender Reihenfolge ist

$$\forall \quad \exists \quad \neg \quad \wedge \quad \vee \quad \rightarrow \quad \leftrightarrow$$

Die Implikation ist rechtsassoziativ.

- Üblicherweise klammert man wieder $\wedge$ und $\vee$
- Genauso klammert man Quantoren

$$(\forall x.F) \rightarrow G \quad \text{statt} \quad \forall x.F \rightarrow G$$

- Achtung! Äußere Quantoren werden öfter anders interpretiert

$$\forall x \forall y.F \wedge G \leftrightarrow H$$

Bindet formal nur an das F!

Definition (Struktur)

Eine passende Struktur $S = (U_s, I_s)$ zu einer Formel F besteht aus einem Universum U_s und einer Interpretation I_s.

- Alle Terme werten zu einem Wert im Universum U_s aus
- Die Interpretation I_s weist den Atomen der Formel Werte zu. Sie spezifiziert
  - Variablen x mit
    $$x_s \in U_s$$
  - Konstanten a mit
    $$a_s \in U_s$$
  - k-stellige Prädikate P mit
    $$P_s \subseteq U_s^k$$
  - Funktionen f mit
    $$f_s : U_s^k \to U_s$$

Definition (Ersetzung)

Sei φ eine Formel und a eine Konstante.
Mit $\varphi[x/a]$ bezeichnen wir die Formel die man erhält, wenn man alle freien Vorkommnisse von x in φ durch a ersetzt.

	Introduktion	Elimination
$\exists$	$\dfrac{\tau[x/a]}{\exists x.\tau}\ {+\exists}$	$\dfrac{\exists x.\tau \qquad \boxed{\begin{matrix} a.\tau[x/a] \\ \vdots \\ \chi \end{matrix}}}{\chi}\ {-\exists}$
$\forall$	$\dfrac{\boxed{\begin{matrix} a \\ \vdots \\ \tau[x/a] \end{matrix}}}{\forall x.\tau}\ {+\forall}$	$\dfrac{\forall x.\tau}{\tau[x/a]}\ {-\forall}$

- Man muss ein unbenutztes a in $+\forall$ und $-\exists$ wählen

Vollständige Induktion

Die vollständige Induktion ist eine Beweistechnik, um zu zeigen, dass alle natürlichen Zahlen ein Prädikat P erfüllen.

$$\forall n \in \mathbb{N}_0 . P(x)$$

Ein solcher Beweis besteht aus

Induktionsanfang Man zeigt, dass $P(0)$ gilt.

Induktionsschritt Man zeigt für ein beliebiges k, dass wenn $P(k)$ gilt (Induktionshypothese), dann auch $P(k+1)$.

Zusammen beweisen die Teile, dass das Prädikat für alle $n \in \mathbb{N}_0$ gilt.

In Prädikatenlogik formuliert gilt in $\mathbb{N}_0$

$$P(0) \land \forall k. (P(k) \rightarrow P(k+1)) \rightarrow \forall n.P(n)$$

- Kann verallgemeinert werden, z.B. auf $\mathbb{Z}$
- Aber nicht auf $\mathbb{R}$ (Warum?)

Definition (Wohlfundierte Relation)

Eine Relation $\prec \subseteq A \times A$ heißt wohlfundiert, wenn keine unendlichen Folgen von Elementen $a_1, a_2, a_3, \dots \in A$ existieren, sodass

$$a_1 \succ a_2 \succ a_3 \succ \dots$$

Jede Kette hat ein unteres Ende.

Beispiel

- $\prec_1 := \left\{(a, b) \in \mathbb{N}^2 \mid a < b\right\}$ ist wohlfundiert.
- $\prec_2 := \left\{(a, b) \in \mathbb{N}^2 \mid a > b\right\}$ ist nicht wohlfundiert.
- $\prec_3 := \left\{(a, b) \in \mathbb{Z}^2 \mid a < b\right\}$ ist nicht wohlfundiert.
- $\prec_4 := \left\{(a, b) \in \mathbb{N}^2 \mid \exists x. x \text{ teilt } a \wedge x \text{ teilt } b\right\}$ ist nicht wohlfundiert.
- $\prec_5 := \emptyset$ ist wohlfundiert.

Wohlfundierte Induktion

Die wohlfundierte Induktion verallgemeinert die vollständige Induktion.
Um für eine Menge A mit wohlfundierter Relation $\prec$ ein Prädikat

$$\forall a \in A.\ P(a)$$

zu zeigen, beweist man

- **Induktionsanfang** Man zeigt, dass für alle bezüglich $\prec$ minimalen Elemente m_i das Prädikat gilt.
- **Induktionsschritt** Man zeigt, dass wenn alle kleineren Elemente als n das Prädikat erfüllen, so auch n.

In Prädikatenlogik formuliert gilt

$$\forall a \in A.\ (\forall b \prec a.\ P(b) \rightarrow P(a)) \quad \text{gdw.} \quad \forall a \in A.\ P(a)$$

- Wo ist der Induktionsanfang?

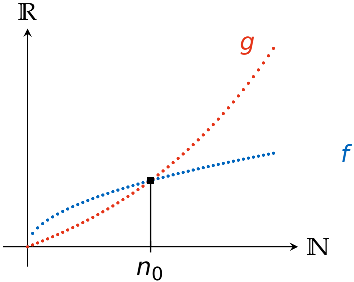
Definition (Asymptotisches Verhalten)

Eine Funktion g ist asymptotisch größer (wächst asymptotisch schneller) als eine andere Funktion f, wenn gilt

$$\exists n_0 > 0 \forall n \geq n_0.\ |f(n)| < |g(n)|$$

- Der Einfachheit halber betrachten wir strikt positive Funktionen
- Dann sind die Beträge egal

- Oftmals sind Vorfaktoren nicht interessant



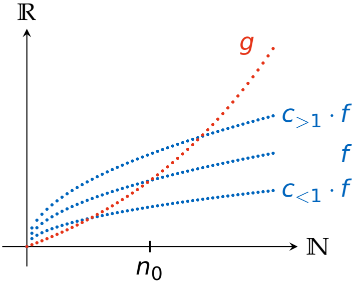
Definition (Asymptotisches Verhalten)

Eine Funktion g ist asymptotisch größer (wächst asymptotisch schneller) als eine andere Funktion f, wenn gilt

$$\exists n_0 > 0 \forall n \geq n_0.\ |f(n)| < |g(n)|$$

- Der Einfachheit halber betrachten wir strikt positive Funktionen
- Dann sind die Beträge egal

- Oftmals sind Vorfaktoren nicht interessant



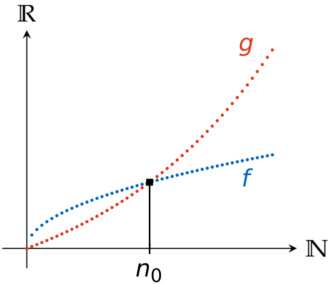
Definition (Asymptotische obere Schranke)

Seien f, g strikt positiv. Eine Funktion f wächst asymptotisch maximal so schnell wie eine Funktion g, wenn gilt

$$\exists c > 0 \exists n_0 > 0 \forall n \geq n_0 . \; f(n) \leq c \cdot g(n)$$

wir schreiben dann

$$f \in \mathcal{O}(g)$$



- $\mathcal{O}(g)$ ist eine Menge von Funktionen ...
- ... die maximal so schnell wachsen wie g

Definition (Landausymbole)

Seien f, g strikt positiv. Analog zu $\mathcal{O}(g)$ definiert man weitere Mengen von Funktionen.

$$o(g) := \{f \mid \forall c > 0 \exists n_0 > 0 \forall n \geq n_0.\ f(n) < c \cdot g(n)\} \qquad \text{(langsamer)}$$

$$\mathcal{O}(g) := \{f \mid \exists c > 0 \exists n_0 > 0 \forall n \geq n_0.\ f(n) \leq c \cdot g(n)\} \qquad \text{(nicht schneller)}$$

$$\Theta(g) := \mathcal{O}(g) \cap \Omega(g) \qquad \text{(gleich schnell)}$$

$$\Omega(g) := \{f \mid \exists c > 0 \exists n_0 > 0 \forall n \geq n_0.\ f(n) \geq c \cdot g(n)\} \qquad \text{(nicht langsamer)}$$

$$\omega(g) := \{f \mid \forall c > 0 \exists n_0 > 0 \forall n \geq n_0.\ f(n) > c \cdot g(n)\} \qquad \text{(schneller)}$$

Es ist

$$o(g) \subseteq \mathcal{O}(g) \qquad o(g) \cap \Omega(g) = \emptyset$$

$$\omega(g) \subseteq \Omega(g) \qquad \omega(g) \cap \mathcal{O}(g) = \emptyset$$

Satz (Landausymbole mit Grenzwerten)

Existiert der Grenzwert $\lim_{n\to\infty} \left|\frac{f(n)}{g(n)}\right|$, *dann gilt*

$$
\begin{array}{lll}
f \in o(g) & \textit{gdw.} & \lim\limits_{n\to\infty} \left|\dfrac{f(n)}{g(n)}\right| = 0 \\
f \in \mathcal{O}(g) & \textit{gdw.} & 0 \leq \lim\limits_{n\to\infty} \left|\dfrac{f(n)}{g(n)}\right| < \infty \\
f \in \Theta(g) & \textit{gdw.} & 0 < \lim\limits_{n\to\infty} \left|\dfrac{f(n)}{g(n)}\right| < \infty \\
f \in \Omega(g) & \textit{gdw.} & 0 < \lim\limits_{n\to\infty} \left|\dfrac{f(n)}{g(n)}\right| \leq \infty \\
f \in \omega(g) & \textit{gdw.} & \lim\limits_{n\to\infty} \left|\dfrac{f(n)}{g(n)}\right| = \infty
\end{array}
$$

Definition (Fakultät)

Die Fakultät $n!$ einer natürlichen Zahl $n \in \mathbb{N}_0$ ist

$$n! := \prod_{i=1}^{n} i = n \cdot (n-1) \cdot \ldots \cdot 1$$

mit $0! := 1$.

Definition (Steigende und fallende Faktorielle)

Für $n, m \in \mathbb{N}_0$ mit $m \leq n$ ist

$$n^{\underline{m}} := \frac{n!}{(n-m)!} = n \cdot (n-1) \cdot \ldots \cdot (n-m+1) \qquad \text{(fallende Faktorielle)}$$

$$n^{\overline{m}} := \frac{(n+m-1)!}{(n-1)!} = n \cdot (n+1) \cdot \ldots \cdot (n+m-1) \qquad \text{(steigende Faktorielle)}$$

Definition (Binomialkoeffizient)

Der Binomialkoeffizient $\binom{n}{k}$ gibt die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge an.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n^{\underline{k}}}{k!}$$

Man sagt n über k oder k aus n.

- $\binom{n}{k}$ viele Möglichkeiten, k Elemente aus n Elementen zu wählen

Satz (Pascalsche Identität)

Die Pascalsche Identität liefert eine rekursive Definition des Binomialkoeffizienten.

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Definition (Multimenge)

Multimengen sind eine Verallgemeinerung gewöhnlicher Mengen.
Elemente können nun mehrfach vorkommen, die Reihenfolge spielt weiterhin keine Rolle.
Sie werden meist auch mit $\{\cdot\}$ notiert, alternativ $\{\!|\cdot|\!\}$.

Satz (Anzahl von Multiteilmengen)

Eine k-Multiteilmenge von M mit $|M| = n$ ist eine Multimenge, die k (nicht unbedingt verschiedene) Elemente aus M enthält.
Es gibt

$$\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$$

solche Multiteilmengen.

Beispiel

- $M := \{1, 2, 2, 2, 3\} = \{2, 1, 2, 3, 2\} \qquad |M| = 5$

Doppeltes Abzählen

Ermittelt man die Mächtigkeit einer Menge auf zwei Arten, so müssen beide Ergebnisse übereinstimmen.
Eine so ermittelte Gleichung kann die gesuchte Mächtigkeit festlegen.

Beispiel (Matrizen)

In einer Matrix müssen die Summen von Zeilensummen und Spaltensummen übereinstimmen.

Beispiel (Studenten)

In einer Vorlesung sitzen 64 Studenten und n Studentinnen.
Jeder Student kennt genau 5 Studentinnen und jede Studentin 8 Studenten. Wenn „bekannt sein“ symmetrisch ist, wie viele Studentinnen besuchen die Vorlesung?

$$64 \cdot 5 = n \cdot 8$$

$$n = \frac{64 \cdot 5}{8} = 40$$

Definition (Schubfachprinzip)

Sei $f : X \to Y$ eine Abbildung und $|X| > |Y|$.
Dann gilt

$$\exists y \in Y.\ \left|f^{-1}(y)\right| \geq 2$$

Wenn man n Elemente auf m < n Fächer verteilt, dann gibt es mindestens ein Fach, das mindestens 2 Elemente enthält.

Definition (Verallgemeinertes Schubfachprinzip)

Sei $f : X \to Y$ eine Abbildung und $|X| > |Y|$.
Dann gilt

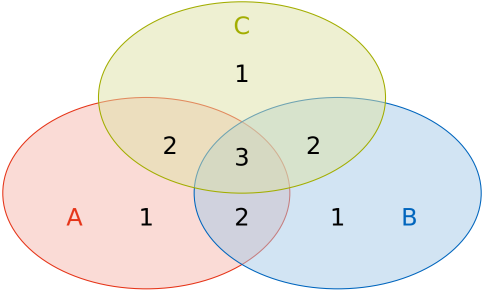
$$\exists y \in Y.\ \left|f^{-1}(y)\right| \geq \left\lceil \frac{|X|}{|Y|} \right\rceil$$

Wenn man n Elemente auf m < n Fächer verteilt, dann gibt es mindestens ein Fach, das mindestens $\left\lceil \frac{|X|}{|Y|} \right\rceil$ Elemente enthält.

Inklusion und Exklusion

Das Prinzip der Inklusion und Exklusion erweitert die Summenregel um nicht disjunkte Mengen.
Für drei Mengen A, B, C gilt

$$\begin{aligned}|A \cup B \cup C| = |A| &+ |B| + |C| \\ &- |A \cap B| - |A \cap C| - |B \cap C| \\ &+ |A \cap B \cap C|\end{aligned}$$



Definition (k-Partition)

Eine k-Partition einer Menge A ist eine Zerlegung von A in k disjunke, nichtleere Teilmengen $A_1, \ldots, A_k$ mit

$$\biguplus_{i=1}^{k} A_i = A$$

Dabei bezeichnet $\uplus$ die disjunkte Vereinigung.

Beispiel

Einige mögliche 3-Partitionen von $[5]$ sind

$$\{\{1,2\},\{3,4\},\{5\}\} \qquad \{\{1\},\{3,4\},\{2,5\}\}$$
$$\{\{1,2,3\},\{4\},\{5\}\} \qquad \{\{1,5\},\{2,4\},\{3\}\}$$

Es existieren genau 25 solche 3-Partitionen.

Definition (Stirlingzahlen zweiter Art)

Die Stirlingzahl zweiter Art $S_{n,k}$ gibt die Anzahl der k-Partitoinen einer n-elementigen Menge an. Wir schreiben

$$\left\{ n \atop k \right\} := S_{n,k}$$

Es ist

$$\left\{ n \atop k \right\} = \left\{ n-1 \atop k-1 \right\} + k \cdot \left\{ n-1 \atop k \right\}$$

- $\left\{ n \atop k \right\}$ viele Möglichkeiten, n unterscheidbare Objekte in k gleiche Fächer zu verteilen, sodass jedes Fach ein Objekt bekommt

Beispiel

- Es gibt $\left\{ 5 \atop 3 \right\} = 25$ 3-Partitionen von $[5]$.

Definition (Permutation)

Eine Permutation einer Menge $A = \{a_1, \ldots, a_n\}$ ist eine bijektive Abbildung $\pi : A \to A$.
Wir notieren Permutationen in zweizeiligen Vektoren.

$$\pi = \begin{pmatrix} a_1 & \ldots & a_n \\ \pi(a_1) & \ldots & \pi(a_n) \end{pmatrix}$$

- Weist jedem Element in A ein neues, eindeutiges Element in A zu.
- „Mischt“ die Elemente einer Menge

Beispiel

π ist eine Permutation auf $[9]$.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 7 & 2 & 6 & 1 & 9 & 8 \end{pmatrix}$$

Es ist $\pi(1) = 3$, $\pi(4) = 7$.

Definition (k-Zyklus)

Ein *k-Zyklus* ist eine Permutation π, die k verschiedene Zahlen $i_1, \ldots, i_k$ im Kreis vertauscht.

$$\pi = \begin{pmatrix} i_1 & i_2 & \ldots & i_k \\ i_2 & i_3 & \ldots & i_1 \end{pmatrix}$$

Wir schreiben auch

$$\pi = \begin{pmatrix} i_1 & i_2 & \ldots & i_k \end{pmatrix}$$

Jede Permutation ist eine Verkettung disjunkter Zyklen.

Beispiel

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 7 & 2 & 6 & 1 & 9 & 8 \end{pmatrix}$$

π enthält vier Zyklen.

$$\pi = \begin{pmatrix} 1 & 3 & 4 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 6 \end{pmatrix} \begin{pmatrix} 8 & 9 \end{pmatrix}$$

Definition (Stirlingzahlen erster Art)

Die Stirlingzahl erster Art $s_{n,k}$ gibt die Anzahl der Permutationen mit n Elementen und k Zyklen an. Wir schreiben

$$\begin{bmatrix} n \\ k \end{bmatrix} := s_{n,k}$$

Es ist

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}$$

- Es gilt $\sum_{k=1}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n!$

Beispiel

- Es gibt $\begin{bmatrix} 9 \\ 4 \end{bmatrix} = 67284$ Permutationen über $[9]$ mit vier Zyklen.