Diskrete Mathematik I

Wintersemester 2007

A. May

Literatur

Vorlesung richtet sich nach

- A. Steger: Diskrete Strukturen
  Band 1: Kombinatorik-Graphentheorie- Algebra
  Springer Verlag
- T. Schickinger, A. Steger: Band 2: Wahrscheinlichkeitstheorie

Zusätzliche Literatur:

- Cormen, Leiserson, Rivest: Introduction to Algorithms, MIT Press
- T. Ihringer: Diskrete Mathematik, Teubner Verlag
- B. Korte, J. Vygen: Kombinatorische Optimierung, Springer

Organisatorisches

- Vorlesung 4+2 SWS (9 CP)
  - Di. 10-12, HNC 30
  - Mi. 12-14, HZO 50
- Übungen
  - Tutor: Nikolas List, Korrektor: Christian Weiers
  - Di. 8-10, ND 5/99 und Mi. 8-10, NA 2/99
  - Beginn: Di. 23. Oktober
  - Abgaben: Mo. 18:00 Uhr, Kasten im 02-Flur
  - Bonussystem: 50% = 1 Notenstufe
75 %= 2 Notenstufen
  - Gruppenabgaben bis zu 4 Personen
  - Korrektur: 2 von 4 Aufgaben (zufällig)

Inhalte der Vorlesung

- Kombinatorik: Abzählprobleme
- Graphen: Traversierung, Eigenschaften
- Zahlentheorie: Modulare und Polynomarithmetik
- Komplexität: Algorithmik, Laufzeitanalyse
- Wahrscheinlichkeit: Diskrete Verteilungen

Was bedeutet diskret?

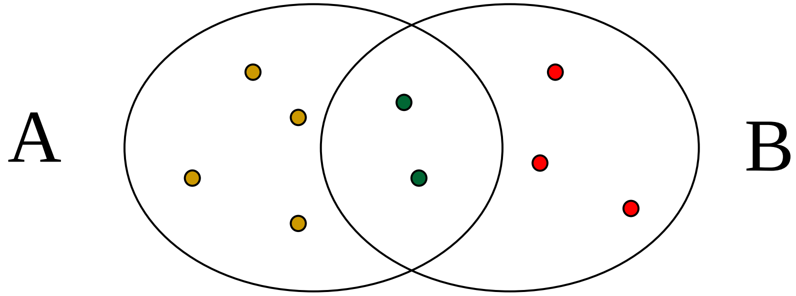
- Intuitiv: Alles, was man mit Computern exakt darstellen kann.
- Gegenteil von analog
- Probleminstanzen sind aus Menge mit endlicher Kardinalität

Notationen für Mengen

- $\mathbb{N}$: natürliche Zahlen ohne Null
- $\mathbb{N}_0$: natürliche Zahlen mit Null
- $\mathbb{Z}$: ganze Zahlen
- $\mathbb{Z}_n$: {0, 1, …, n-1}
- [n]: {1, 2, …, n}
- $\mathbb{Q}$: rationale Zahlen
- $\mathbb{R}$: reelle Zahlen

Operationen auf Mengen

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



- Kartesisches Produkt $A \times B := \{ (a,b) \mid a \in A \text{ und } b \in B\}$
- Potenzmenge $\mathcal{P}(M) := \{ N \mid N \subseteq M\}$

Bsp: $M=\{\text{rot, blau}\}$, $\mathcal{P}(M)=\{ \emptyset, \{\text{rot}\}, \{\text{blau}\}, \{\text{rot, blau}\} \}$

Relationen zwischen Mengen

Def:Eine Relation zwischen A und B ist eine Teilmenge R $\subseteq$ A $\times$ B.

Falls A=B, spricht man von einer Relation auf A.

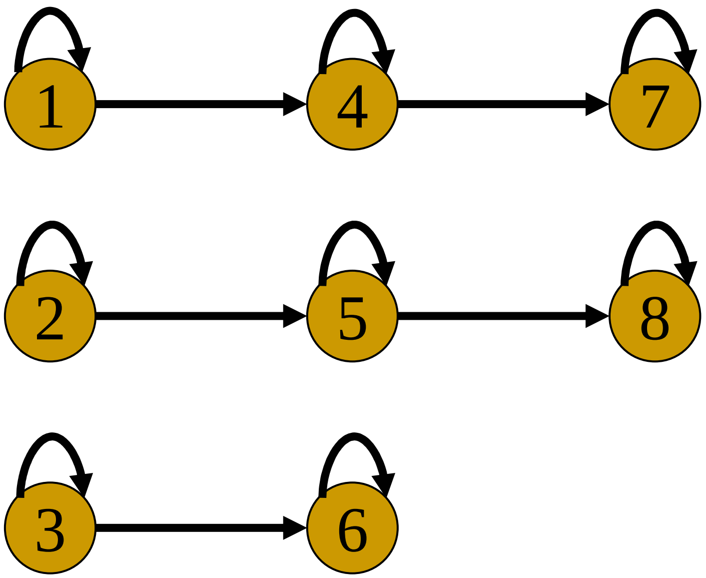
Eigenschaften von Relationen auf einer Menge:

- Reflexiv: $\forall$ a $\in$ A: (a,a) $\in$ R
- Symmetrisch: $\forall$ a,b $\in$ A: (a,b) $\in$ R $\Rightarrow$ (b,a) $\in$ R
- Antisymmetrisch: $\forall$ a,b $\in$ A: (a,b) $\in$ R $\wedge$ (b,a) $\in$ R $\Rightarrow$ a=b
- Transitiv: $\forall$ a,b,c $\in$ A: (a,b) $\in$ R $\wedge$ (b,c) $\in$ R $\Rightarrow$ (a,c) $\in$ R

- R_1:={(a,b) $\in \mathbb{N}^2$| a teilt b}:
  - r, a, t (partielle Ordnung)
- R_2:={(a,b) $\in \mathbb{Z}^2$ | (a mod 3) = (b mod 3)}:
  - r, s, t (Äquivalenzrelation)
- R_3:={(a,b) $\in \mathbb{Z}^2$ | a teilt b}:
  - r, t (Quasiordnung)

Graphische Darstellung

Bsp: R:={(a,b) $\in$ [8]^2 | (a mod 3)=(b mod 3), a$\leq$b}



Abbildungen/Funktionen

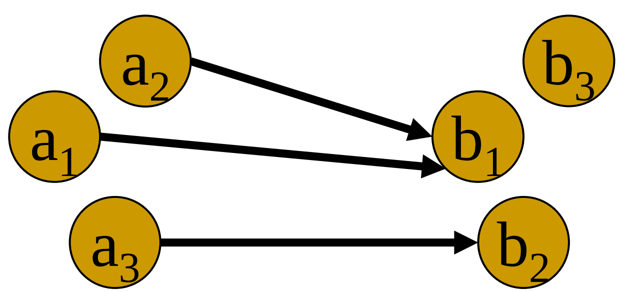
Def: Eine Abbildung/Funktion ist eine Relation $R \subseteq A \times B$ mit:

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

Schreibweise:

$$f: A \to B$$
$$a \mapsto f(a)$$

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

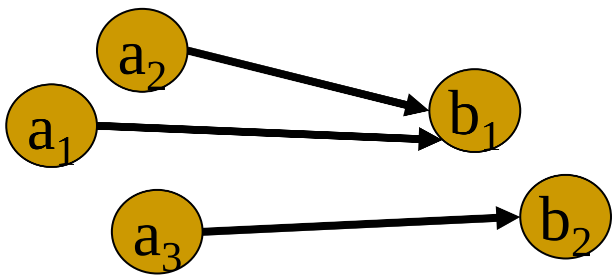


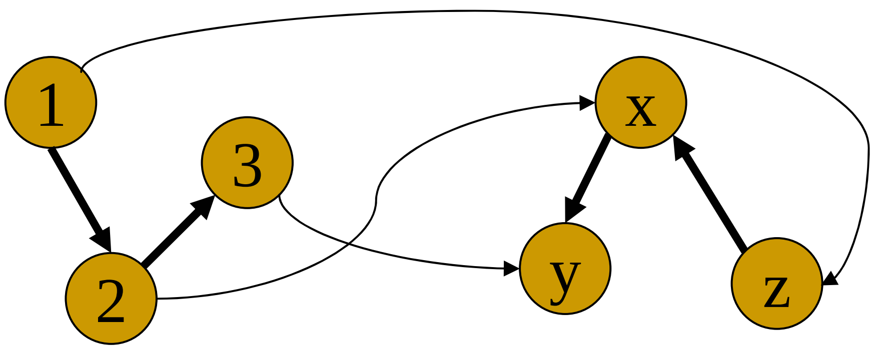
Definieren für $A' \subseteq A$, $B' \subseteq B$: $f(A') = \bigcup_{a \in A'} \{f(a)\}$

$f(B') = \bigcup_{b \in B'} f^{-1}(b)$

Eigenschaften von Funktionen

- f injektiv $\Leftrightarrow \forall\, b \in B{:}\ |f^{-1}(b)| \leq 1$
- f surjektiv $\Leftrightarrow \forall\, b \in B{:}\ |f^{-1}(b)| \geq 1$
- f bijektiv $\Leftrightarrow$ f injektiv und f surjektiv





Def (Isomorphismus): $R_1 \subseteq A_1^2$, $R_2 \subseteq A_2^2$ isomorph $\Leftrightarrow$
$\exists$ bijektives $f{:}\ A_1 \to A_2{:}\ \forall\, (a,b) \in A_1^2{:}\ (a,b) \in R_1 \Leftrightarrow (f(a), f(b)) \in R_2$.

Indirekter Beweis/Widerspruchsbeweis

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

$$n^2 \text{ gerade} \Rightarrow n \text{ gerade.}$$

Beweis:

Kontraposition: $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$

Genügt zu zeigen: n ungerade $\Rightarrow$ n^2 ungerade.

$$\begin{aligned} n \text{ ungerade} \quad &\Rightarrow n=2k+1,\ k \in \mathbb{N}_0 \\ &\Rightarrow n^2=4k^2+4k+1 \\ &\Rightarrow n^2 \text{ ungerade} \end{aligned}$$

Induktionsbeweis

Satz: Jede Zahl n $\geq$ 2 lässt sich als Produkt von Primzahlen darstellen.

Beweis durch Induktion über n:

- (IV) Induktionsverankerung: n=2 prim.
- (IA) Induktionsannahme: Satz ist korrekt für alle Zahlen $\leq$ n.
- (IS) Induktionsschritt n$\rightarrow$ n+1:

  Fallunterscheidung:
  - n+1 prim, d.h. n+1 ist Produkt von Primzahlen.
  - n+1 zusammengesetzt, d.h. n+1 = a*b mit 1< a,b $\leq$ n.

    Wende Induktionsannahme auf a und b an.

Widerspruchsbeweis

Satz: Es gibt unendlich viele Primzahlen.

Annahme: $\exists$ endlich viele Primzahlen $p_1, \ldots, p_n$, n beliebig,aber fest

Setze $m = 1+\prod^{n}_{i=1} p_i$.

$\Rightarrow$ $m=1 \bmod p_i$ für $i=1,\ldots,n$

$\Rightarrow$ p_i teilt m nicht (wegen $p_i \geq 2$).

$\Rightarrow$ $m \neq p_i$, $i=1,\ldots,n$ und m ist prim.

$\Rightarrow$ Es existieren mindestens n+1 viele Primzahlen.

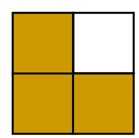
(Widerspruch: Nach Annahme existieren nur n Primzahlen.)

Induktionsbeweis

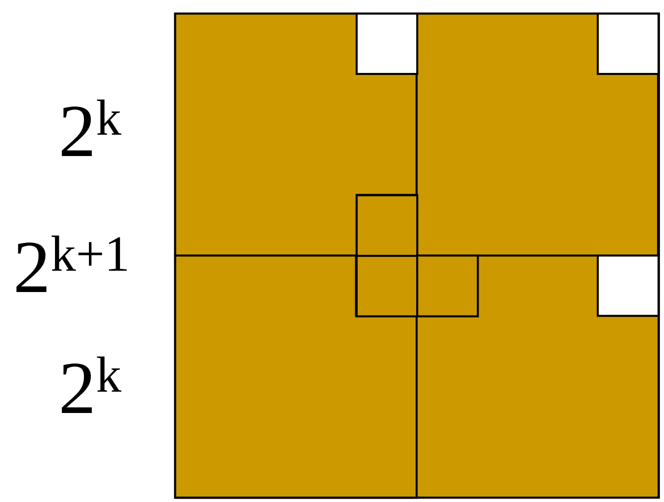
Satz: Jedes Schachbrett mit Seitenlänge 2^k lässt sich durch 3-Felder große L-Teile so kacheln, dass die rechte obere Ecke frei bleibt.

Beweis durch Induktion über k:

- IV (k=1):



- IA: Satz sei korrekt bis k.
- IS (k $\rightarrow$ k+1):



Landau Notation – Groß-Oh

Def: $f(n) = \mathcal{O}(g(n)) \Leftrightarrow \exists\, c, n_0 \in \mathbb{N}\ \forall\, n \geq n_0$: $|f(n)| \leq c^*|g(n)|$

Alternativ: $f(n) = O(g(n)) \Leftrightarrow \lim_{n \to \infty} \sup |f(n)|/|g(n)| < \infty$

Beispiele:

- $3n^2 + n + 2 = \mathcal{O}(n^2)$
- $3n^2 + n + 2 = \mathcal{O}(n^3 \log n)$
- $\sum^n_{i=1} i = \mathcal{O}(n^2)$
- $\sum^d_{i=1} a_i n^i = \mathcal{O}(n^d)$
- $\sum^n_{i=1} 1/i = \mathcal{O}(\log n)$
- $\log_2 n = O(\log_e n)$

Groß-Omega

Def: $f(n) = \Omega(g(n)) \Leftrightarrow \exists\ c, n_0 \in \mathbb{N}\ \forall\ n \geq n_0: |f(n)| \geq c^*|g(n)|$

Alternativ: $f(n) = O(g(n)) \Leftrightarrow \lim_{n \to \infty} \sup |f(n)|/|g(n)| > 0$

Beispiele:

- $3n^2 + n + 2 = \Omega(n^2)$
- $3n^2 + n + 2 = \Omega(n \log n)$
- $\sum^n_{i=1} i = \Omega(n^2)$
- $\sum^d_{i=1} a_i n^i = \Omega(n^d)$
- $\sum^n_{i=1} 1/i = \Omega(\log n)$
- $\log_2 n = \Omega(\log_e n)$

Theta, Klein-Oh, Klein-Omega

$f(n) = \Theta(g(n)) \Leftrightarrow f(n) = \mathcal{O}(g(n))$ und $f(n) = \Omega(g(n))$

- $\sum^{d}_{i=1} a_i n^i = \Theta(n^d)$
- $\log_2 n = \Theta(\log_e n)$

$f(n) = o(g(n)) \Leftrightarrow \forall\, c\ \exists\, n_0 \in \mathbb{N}\ \forall\, n \geq n_0: |f(n)| < c*|g(n)|$

Alternativ: $f(n) = o(g(n)) \Leftrightarrow \lim_{n \to \infty} |f(n)|/|g(n)| = 0$

- $n=o(n^2)$
- $10n^2/\text{loglogn} = o(n^2)$

$f(n) = \omega(g(n)) \Leftrightarrow \forall\, c\ \exists\, n_0 \in \mathbb{N}\ \forall\, n \geq n_0: |f(n)| > c*|g(n)|$

Alternativ: $f(n) = o(g(n)) \Leftrightarrow \lim_{n \to \infty} |f(n)|/|g(n)| \to \infty$

- $n^2=\omega(n)$
- $10n^2\ \text{loglogn} = \omega(n^2)$

Zusammenfassung

- Operationen auf Mengen
  - $A \cup B$, $A \cap B$, $A \times B$, $A \setminus B$, $\mathcal{P}(A)$
- Relationen, Abbildungen/Funktionen
  - Reflexiv, symmetrisch, antisymmetrisch, transitiv
  - Injektiv, surjektiv, bijektiv
- Beweistechniken:
  - Indirekter Beweis, Widerspruchsbeweis
  - Induktionsbeweis
- Landau-Notation
  - $\mathcal{O}$, Ω, Θ, o, ω