# Einführung in die Informatik 2

## – Mathematische Grundbegriffe –

Sven Kosub

AG Algorithmik/Theorie komplexer Systeme
Universität Konstanz

http://www.inf.uni-konstanz.de/algo/lehre/ss08/info2

Sommersemester 2008

# Mengen

- (mathematischer) Begriff der Menge fundamental für nahezu alle Gebiete der Informatik
- verwenden intuitiven Mengenbegriff (daher auch „naive Mengenlehre")
- Menge nach Georg Cantor (1895):

  > *Unter einer „Menge" verstehen wir jede Zusammenfassung M von bestimmten, wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die „Elemente" von M genannt werden) zu einem Ganzen.*

- Wieso naiv?
  - Was ist die „die Menge aller Mengen"?
  - Was ist „die Menge aller Mengen, die sich nicht selbst als Element enthalten"?
  - Ausweg: Typentheorie (Russell), axiomatische Mengenlehre (Zermelo-Fraenkel-Axiome)

# Mengen

Darstellung von Mengen

- extensional: Angabe aller Elemente der Menge

$$\{x_1, x_2, x_3, \dots\}$$

- intensional: Angabe eines definierenden Ausdrucks $E$

$$\{x \mid E(x)\}$$

- $\{1, 3, 5, 7, 9\}$
- $\{x \mid x$ ist eine natürliche Zahl und $x$ ist ungerade und $x < 10\}$

- Menge, die kein Element enthält, heißt leere Menge und wird mit $\varnothing$ bezeichnet

# Mengen

- bei extensionaler Darstellung spielt Reihenfolge der Elemente keine Rolle, d.h.

$$\{1, 3, 5, 7, 9\} \quad \text{und} \quad \{5, 7, 3, 1, 9\}$$

  beschreiben dieselbe Menge

  sonst: Folgen oder Tupel

- Anzahl des Vorhandenseins eines Elementes irrelevant, d.h.

$$\{1, 3, 3, 5, 5, 5, 7, 9, 9, 9\}$$

  beschreibt auch dieselbe Menge

  sonst: Multimenge

# Mengen

- $e \in A$ steht für „Objekt $e$ ist Element von $A$“
- Anzahl der Elemente von $A$ heißt Mächtigkeit bzw. Kardinalität von $A$, symbolisch: $\|A\|, |A|, \#A$

  beachte: mehrfach dargestellte Element werden nur einmal gezählt, d.h.

  $$\|\{1, 3, 3, 1, 5, 5, 7, 5, 9, 3, 9, 9, 7\}\| = 5$$

- leere Menge hat Kardinalität 0, d.h. $\|\varnothing\| = 0$

# Mengen

Mengenvergleiche:

- $A \subseteq B$ steht für: $A$ ist Teilmenge von $B$, d.h. jedes Element von $A$ ist Element von $B$
- $A = B$ steht für: $A$ und $B$ sind gleich, d.h. $A \subseteq B$ und $B \subseteq A$
- $A \subset B$ steht für: $A$ ist echte Teilmenge von $B$, d.h. $A \subseteq B$, aber $A$ und $B$ sind nicht gleich

negative Mengenvergleiche:

- $A \not\subseteq B$ steht für: $A$ ist keine Teilmenge von $B$, d.h. mindestens ein Element von $A$ ist nicht Element von $B$
- $A \neq B$ steht für: $A$ und $B$ sind nicht gleich, d.h. $A \not\subseteq B$ oder $B \not\subseteq A$
- $A \not\subset B$ steht für: $A$ ist keine echte Teilmenge von $B$, d.h. $A \not\subseteq B$ oder $A = B$
- $e \notin A$ steht für: $e$ ist nicht Element von $A$

# Mengen

Potenzmenge von $A$:

- Menge aller Teilmengen von $A$, symbolisch: $\mathcal{P}(A), 2^A$
- $B \in \mathcal{P}(A)$ genau dann, wenn $B \subseteq A$

Fakten:

- Es gilt stets $\emptyset \in \mathcal{P}(A)$ und $A \in \mathcal{P}(A)$
- Ist $A$ endlich, so gilt $\|\mathcal{P}(A)\| = 2^{\|A\|}$

Für $A = \{0, 1\}$ gilt $\mathcal{P}(A) = \big\{\emptyset, \{0\}, \{1\}, \{0, 1\}\big\}$.

# Mengen

Grundlegende Operationen auf Mengen $A$ und $B$:

- Vereinigung: $A \cup B =_{\text{def}} \{e \mid e \in A \text{ oder } e \in B\}$
- Durchschnitt: $A \cap B =_{\text{def}} \{e \mid e \in A \text{ und } e \in B\}$
- Differenz: $A \setminus B =_{\text{def}} \{e \mid e \in A \text{ und } e \notin B\}$

- $\{1,2\} \cup \{2,3\} = \{1,2,3\}$
- $\{1,2\} \cap \{2,3\} = \{2\}$
- $\{1,2\} \setminus \{2,3\} = \{1\}$

- bezüglich fester Grundmenge $M$ wird $\overline{A}$ für $M \setminus A$ verwendet
- de Morgan'sche Regeln:

$$\begin{aligned} \overline{A \cup B} &= \overline{A} \cap \overline{B} \\ \overline{A \cap B} &= \overline{A} \cup \overline{B} \end{aligned}$$

- $A$ und $B$ heißen disjunkt, wenn $A \cap B = \emptyset$ gilt

# Mengen

- $A \times B =_{\text{def}} \{(a, b) \mid a \in A \text{ und } b \in B\}$ heißt (kartesisches) Produkt von $A$ und $B$
- $A_1 \times \cdots \times A_n =_{\text{def}} \{(a_1, \ldots, a_n) \mid a_i \in A_i\}$ heißt verallgemeinertes Produkt von $A_1 \ldots, A_n$
- Elemente des Produktes von $n$ Mengen heißen $n$-Tupel
- spezielle Bezeichnung für $n$-Tupel:
  - Paare für $n = 2$
  - Tripel für $n = 3$
  - Quadrupel für $n = 4$

Fakt: Für endliche Mengen $A_1, \ldots, A_n$ gilt

$$\|A_1 \times \cdots \times A_n\| = \|A_1\| \cdot \cdots \cdot \|A_n\|$$

# Relationen

- Jede Teilmenge $R \subseteq A_1 \times \cdots \times A_n$ heißt Relation
- Relationen modellieren Beziehungen zwischen Objekten
- Relationen werden oft als Tabellen dargestellt

Für $A_1 = \{a, b, c\}$, $A_2 = \{1, 2\}$ und $A_3 = \{\%, \$\}$ könnte Relation gegeben sein als:

| | | |
|---|---|---|
| $a$ | 1 | % |
| $a$ | 1 | $ |
| $b$ | 2 | $ |

- binäre Relationen, d.h. zweistellige Relation, werden als Graphen dargestellt

# Ordnungen

- binäre Relationen über Grundmenge $A$ können zum Ordnen von $A$ verwendet werden
- $R \subseteq A \times A$ heißt Halbordnung (partielle Ordnung), falls für beliebige Elemente $a, b, c \in A$ gilt
  - Reflexivität: $(a, a) \in R$
  - Transitivität: wenn $(a, b) \in R$ und $(b, c) \in R$, dann ist $(a, c) \in R$
  - Antisymmetrie: wenn $(a, b) \in R$ und $(b, a) \in R$, dann ist $a = b$
- Halbordnung $R \subseteq A \times A$ heißt Ordnung (totale Ordnung, lineare Ordnung), falls zusätzlich gilt
  - Totalität: $(a, b) \in R$ oder $(b, a) \in R$
- für Halbordnung $R$ schreiben wir Paare $(a, b) \in R$ auch als $a \leq_R b$
- für Halbordnung $R \subseteq A \times A$ heißt $(A, \leq_R)$ partiell geordnete Menge
- für Ordnung $R \subseteq A \times A$ heißt $(A, \leq_R)$ total geordnete Menge

# Ordnungen

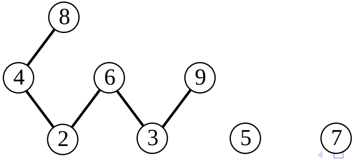
- $(\mathbb{R}, \leq)$ und $(\mathbb{N}, \leq)$ sind total geordnete Mengen
- $(\mathcal{P}(A), \subseteq)$ ist für alle Mengen $A$ eine partiell geordnete Menge
- Auf $\{2, 3, 4, 5, 6, 7, 8, 9\}$ betrachten wir die Relation

$$R =_{\text{def}} \{(x, y) \mid (x, y) \in A \text{ und } x \text{ teilt } y\ \}$$

Dann ist $R$ eine Halbordnung mit folgender Extension:

$$\begin{aligned} R \quad = \quad \{\ & (2,2), (2,4), (2,6), (2,8), (3,3), (3,6), (3,9), \\ & (4,4), (4,8), (5,5), (6,6), (7,7), (8,8), (9,9)\ \} \end{aligned}$$

Darstellung als Hasse-Diagramm



# Äquivalenzrelationen

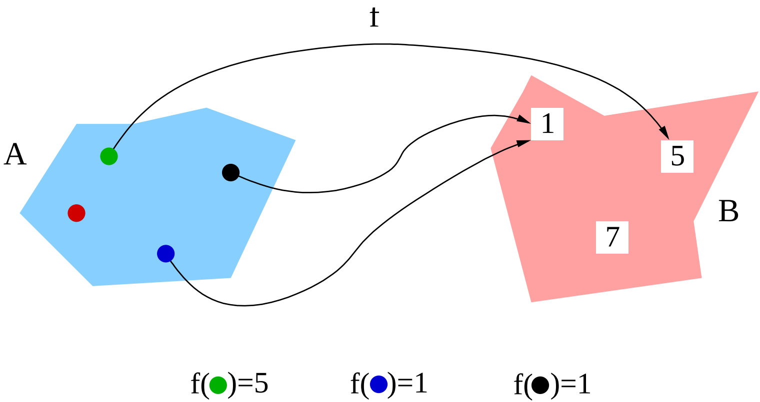
- Relation $R \subseteq A \times A$ heißt symmetrisch, falls für alle $a, b \in A$ gilt: Ist $(a, b) \in R$, so ist auch $(b, a) \in R$
- beachte: antisymmetrisch ist nicht die Negation von symmetrisch
- Relation heißt Äquivalenzrelation, falls sie reflexiv, transitiv und symmetrisch ist

Erreichbarkeitsrelation auf ungerichteten Graphen ist Äquivalenzrelation:

- Reflexivität: jeder Knoten erreicht sich selbst über einen Weg der Länge 0
- Transitivität: gibt es Weg von Knoten $u$ zu Knoten $v$ und gibt es Weg von Knoten $v$ zu Knoten $w$, so gibt es auch Weg von Knoten $u$ zu Knoten $w$
- Symmetrie: gibt es Weg von $u$ nach $v$, so gibt es Weg von $v$ nach $u$ durch Umkehrung der Kantentraversierung

# Funktionen

- binäre Relation $R \subseteq A \times B$ heißt
  - rechtseindeutig, falls für jedes $a \in A$ höchstens ein $b \in B$ mit $(a, b) \in R$ existiert
  - linkseindeutig, falls für jedes $b \in B$ höchstens ein $a \in A$ mit $(a, b) \in R$ existiert
- rechtseindeutige Relation $f$ über $A \times B$ wird als Funktion von $A$ nach $B$ bezeichnet
- Notation: $f : A \to B$ statt $f \subseteq A \times B$
- Notation: $f(a) = b$ statt $(a, b) \in f$
- $A$ heißt Definitionsbereich von $f$
- $B$ heißt Bildbereich von $f$

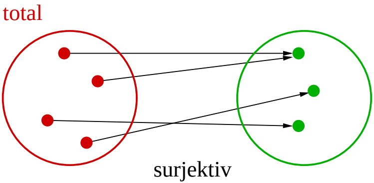

f
A
B
1
5
7
f(●)=5
f(●)=1
f(●)=1

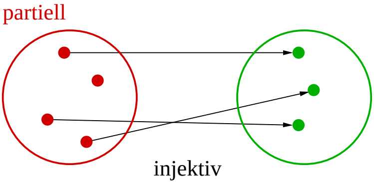
# Funktionen

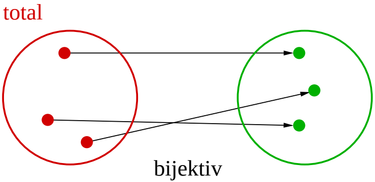
Eigenschaften von Funktionen:

- $f : A \rightarrow B$ heißt total, falls jedem Element $a \in A$ ein „Bild“ $b \in B$ durch $f$ zugeordnet wird
- $f : A \rightarrow B$ heißt partiell, falls es Elemente ohne Bilder gibt
- manchmal heißen totale Funktionen einfach Funktionen und partielle Funktionen Abbildungen
- $f : A \rightarrow B$ heißt surjektiv, falls jedes Element von $B$ Bild eines Elementes $a$ ist
- $f : A \rightarrow B$ heißt injektiv, falls $f$ auch linkseindeutig ist
- $f : A \rightarrow B$ heißt bijektiv, falls $f$ sowohl injektiv als auch surjektiv ist (Beachte: Für bijektive Funktionen existiert eine Umkehrabbildung)

# Funktionen



Fakt:

Es sei $f : A \rightarrow B$ eine Funktion mit $\|A\| = \|B\| < \infty$.

Dann sind folgende Aussagen äquivalent:

1. $f$ ist bijektiv.
2. $f$ is surjektiv.
3. $f$ ist injektiv.

Wieso?

# Asymptotik von Funktionen

- Asymptotik beschreibt das Verhalten von Funktionen im Unendlichen
- asymptotisches Wachstum von Funktionen wird durch die Landau-Symbole $O, o, \Omega, \omega, \Theta$ ausgedrückt
- Landau-Symbole definieren binäre Relationen auf Funktionen

Im Folgenden betrachten wir totale Funktionen $f : \mathbb{N} \to \mathbb{R}_+$

# Asymptotik von Funktionen

- $f \in O(g) \iff_{\text{def}}$ es gibt $c > 0$ und $n_0 \in \mathbb{N}$, so dass $f(n) \leq c \cdot g(n)$ für alle $n \geq n_0$ gilt (*f* wächst höchstens so schnell wie *g*)
- $f \in \Omega(g) \iff_{\text{def}}$ es gibt $c > 0$ und $n_0 \in \mathbb{N}$, so dass $f(n) \geq c \cdot g(n)$ für alle $n \geq n_0$ gilt (*f* wächst mindestens so schnell wie *g*)
- $f \in o(g) \iff_{\text{def}}$ für alle $c > 0$ gibt es $n_0 \in \mathbb{N}$, so dass $f(n) < c \cdot g(n)$ für alle $n \geq n_0$ gilt (*f* wächst langsamer als *g*)
- $f \in \omega(g) \iff_{\text{def}}$ für alle $c > 0$ gibt es $n_0 \in \mathbb{N}$, so dass $f(n) > c \cdot g(n)$ für alle $n \geq n_0$ gilt (*f* wächst schneller als *g*)
- $f \in \Theta(g) \iff_{\text{def}} f \in O(g) \cap \Omega(g)$ (*f* wächst genauso schnell wie *g*)

# Asymptotik von Funktionen

- $4n + 9996 \in O(n^2)$ mittels $c = 1$ und $n_0 = 102$ (oder $c = 2$ und $n_0 = 72$ oder ...)
- $100n^5 + 200n^4 + n^3 + 1000357n^2 + 7n + 33 = O(n^5)$ mittels $c = 1000400$ und $n_0 = 1$
- $\log^{k+1} n = \Omega(\log^k n)$ mittels $c = 1$ und $n_0 = 1$
- $n^k \in o(n^{k+1})$ mittels $n_0 = \lceil \frac{1}{c} \rceil$ für $c > 0$
- $\log n^k \in \Theta(\log n^{k+1})$
- $3^n \in \omega(2^n)$
- $\max\{0, (-1)^n \cdot n^3\}$ und $n^2$ sind unvergleichbar

- oft wird $f = O(g)$ an Stelle von $f \in O(g)$ geschrieben
- aber Vorsicht: $f = O(g)$ bedeutet nicht $g = O(f)$
- $f = o(g)$ äquivalent zu $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$