Theoretische Informatik

für

Ingenieurinformatik

berufsbegleitendes Studium Lehramt Informatik
(Berufsschule+Sekundarschule)

http://theo.cs.uni-magdeburg.de/lehre05s/

Vorlesung: Dr. Ralf Stiebe
Übung: Dr. Bernd Reichel
Email: {reichel,stiebe}@iws.cs.uni-magdeburg.de

Inhalt der Vorlesung

- Berechenbarkeit
  - Formale Definition des Begriffes Algorithmus
  - Nachweis, dass verschiedene Probleme algorithmisch nicht lösbar sind
- Komplexität
  - Schwierigkeit algorithmisch lösbarer Probleme (Zeitbedarf, Platzbedarf)
- Formale Sprachen
  - enge Beziehung zur Berechenbarkeitstheorie
  - Anwendungen in Compilerbau, Textverarbeitung

Literatur

- Uwe Schöning: Theoretische Informatik – kurzgefasst.
  Die Vorlesung orientiert sich stark an diesem Buch.
- Hopcroft, Motwani, Ullman: Einführung in die Automatentheorie, Formale Sprachen und Komplexitätstheorie.
  Sehr ausführliches Standardwerk
- Script

Mathematische Grundlagen

Script, Kapitel 1

- Mengen, Relationen, Funktionen
- Alphabete, Wörter, Sprachen

Mengen, Relationen, Funktionen

Menge: Zusammenfassung von Elementen.

$$M = \{2, 4, 6, 8\},\ 4 \in M,\ 3 \notin M$$

Reihenfolge der Elemente beliebig, Mehrfachnennungen zählen nicht:

$$\{4, 6, 8, 2, 8, 8\} = \{2, 4, 6, 8\}$$

Beschreibung einer Menge durch definierende Eigenschaft:

$$P = \{n \in \mathbb{N} | n \text{ ist eine Primzahl}\}$$

Wichtige spezielle Mengen

- $\emptyset$: leere Menge (enthält keine Elemente)
- $\mathbb{N}$: Menge der natürlichen Zahlen (einschließlich 0)
- $\mathbb{Z}$: Menge der ganzen Zahlen
- $\mathbb{R}$: Menge der reellen Zahlen
- $\mathbb{Q}$: Menge der rationalen Zahlen

Teilmengen

A heißt Teilmenge von B, wenn alle Elemente von A in B sind.
Bezeichnung: $A \subseteq B$.

A heißt echte Teilmenge von B, wenn $A \subseteq B$ und $A \neq B$.
Bezeichnung: $A \subsetneq B$.

Potenzmenge von A: Menge aller Teilmengen von A
Bezeichnung: $\mathcal{P}(A)$ bzw. 2^A

Beispiel: $A = \{0, 1, 4\}$, $2^A = \{\emptyset, \{0\}, \{1\}, \{4\}, \{0, 1\}, \{0, 4\}, \{1, 4\}, \{0, 1, 4\}\}$

Mengenoperationen

A und B seien Teilmengen einer Grundmenge G

Vereinigung: $A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$

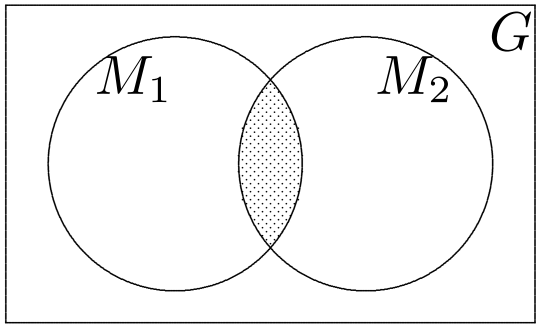
Durchschnitt: $A \cap B = \{x \mid x \in A \text{ und } x \in B\}$

Differenz: $A \setminus B = \{x \mid x \in A \text{ und } x \notin B\}$

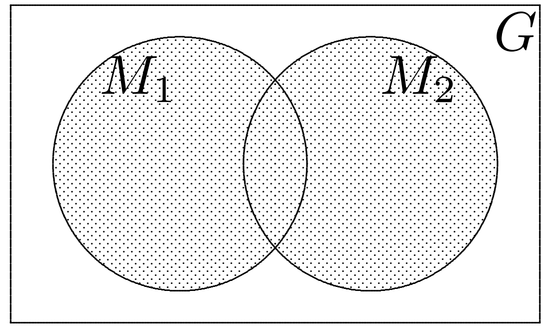
Komplement: (von A bez. G): $\overline{A} = \{x \mid x \in G \text{ und } x \notin A\}$

Beispiel: $G = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $A = \{0, 1, 2, 3, 4\}$, $B = \{2, 4, 6, 8\}$
$A \cup B = \{0, 1, 2, 3, 4, 6, 8\}$, $A \cap B = \{2, 4\}$, $A \setminus B = \{0, 1, 3\}$,
$\overline{A} = \{5, 6, 7, 8\}$

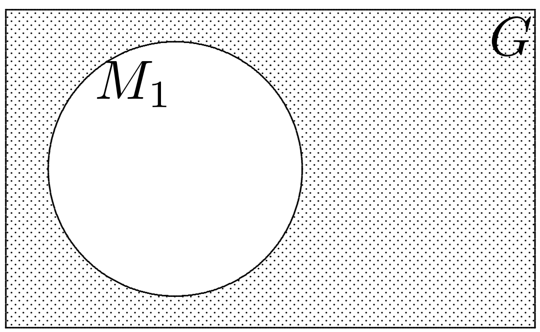
Mengenoperationen: Venn Diagramme



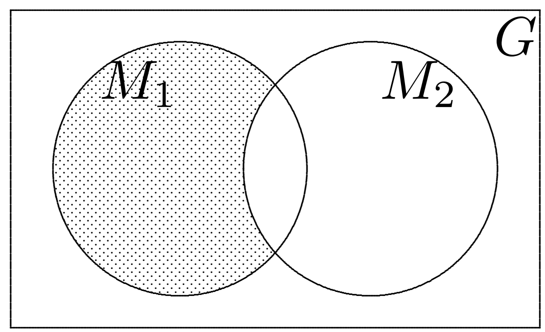
$M_1 \cap M_2$



$M_1 \cup M_2$



$\overline{M_1}$



$M_1 \setminus M_2$

Tupel und Kartesische Produkte

Geordnetes Paar: (a, b)

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

Geordnetes k-Tupel: $(a_1, a_2, \ldots, a_k)$, $k \geq 2$
$k = 2$: Paar, $k = 3$: Tripel, $k = 4$: Quadrupel, $k = 5$: Quintupel

Kartesisches Produkt von k Mengen:
$A_1 \times A_2 \times \ldots \times A_k = \{(a_1, a_2, \ldots, a_k) \mid a_1 \in A_1, a_2 \in A_2, \ldots a_k \in A_k\}$
$A^k = \{(a_1, a_2, \ldots, a_k) \mid a_1 \in A, a_2 \in A, \ldots a_k \in A\}$

Speziell gilt: $A \times \emptyset = \emptyset \times A = \emptyset$

Relationen

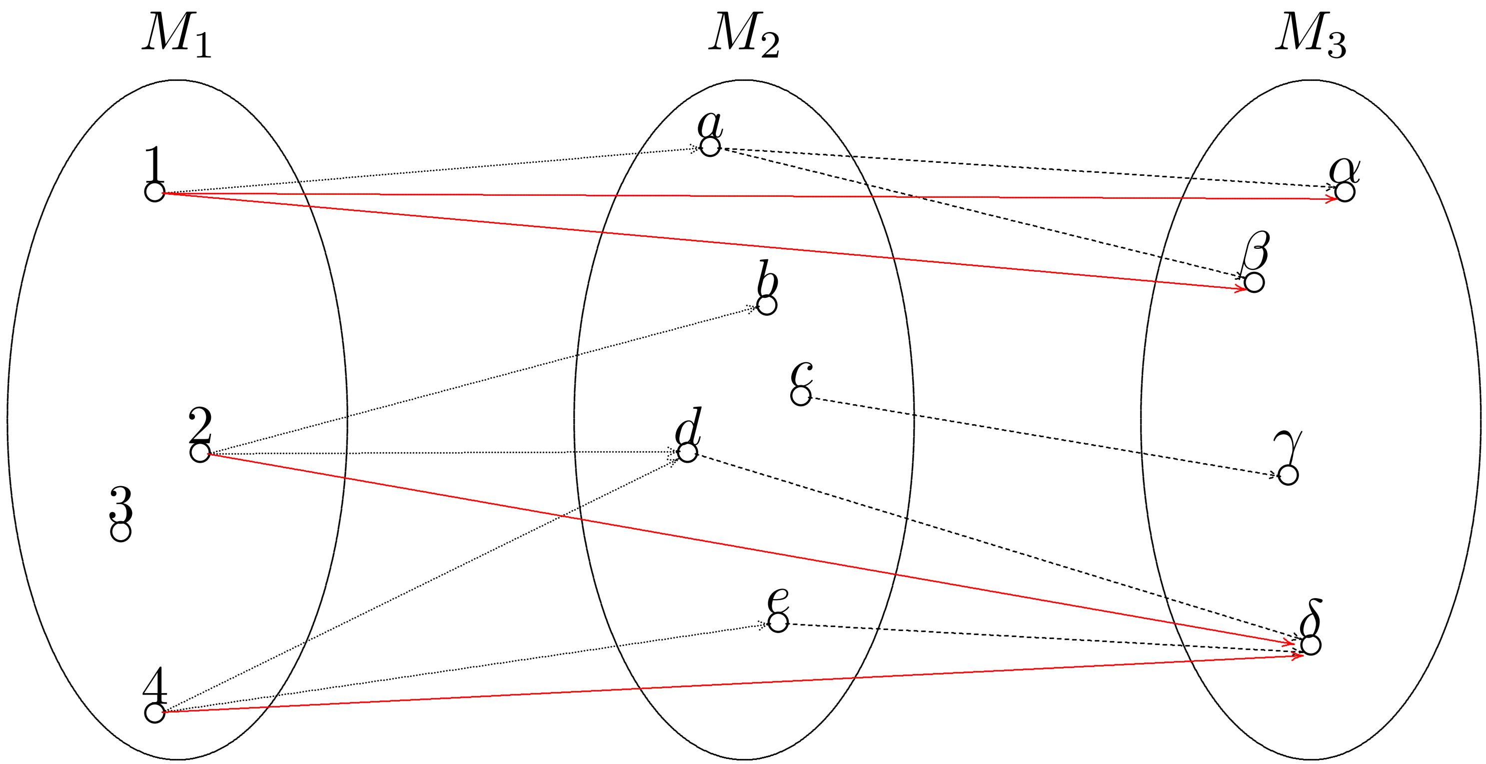
$R \subseteq A_1 \times A_2 \times \ldots \times A_k$ nennt man k-stellige Relation.

$R \subseteq A \times B$ nennt man speziell binäre Relation.
Schreibweise: xRy für $(x, y) \in R$
Bild von $x \in A$: $R(x) = \{y \in B \mid xRy\}$
Urbild von $y \in B$: $R^{-1}(y) = \{x \in A \mid xRy\}$

Verknüpfung oder Verkettung binärer Relationen
Sei $R \subseteq A \times B, S \subseteq B \times C$. Dann ist

$$R \circ S = \{(a, c) \mid (a, b) \in R \text{ und } (b, c) \in S \text{ für ein } b \in B\}$$

Verkettung von Relationen: Graphische Darstellung



Funktionen

$R \subseteq A \times B$ heißt (partielle) Funktion von A nach B, wenn für jedes $x \in A$ höchstens ein $y \in B$ mit xRy existiert.
Schreibweise: $R : A \rightarrow B$

Eine Funktion $f : A \rightarrow B$ heißt

- total, wenn für jedes $x \in A$ ein $y \in B$ mit $f(x) = y$ existiert.
- surjektiv, wenn für jedes $y \in B$ ein $x \in A$ mit $f(x) = y$ existiert.
- injektiv oder umkehrbar eindeutig, wenn für jedes $y \in B$ höchstens ein $x \in A$ mit $f(x) = y$ existiert.
- bijektiv, wenn f total, surjektiv und injektiv ist.

Mächtigkeit einer Menge

$|A|$: Mächtigkeit einer Menge A (Anzahl der Elemente)

Zwei Mengen A und B heißen gleichmächtig, wenn eine bijektive Abbildung $f : A \to B$ existiert.

Eine Menge heißt

- abzählbar unendlich, wenn sie gleichmächtig zu $\mathbb{N}$ ist;
- abzählbar, wenn sie endlich oder abzählbar unendlich ist.
- überabzählbar, wenn sie nicht abzählbar ist.

Beispiel einer abzählbaren Menge

Satz *Die Menge* $\mathbb{N}^2$ *ist abzählbar unendlich.*

Beweisidee: Dovetailing (Schwalbenschwanz)

Ordne die Paare diagonalenweise (d.h. nach aufsteigender Summe).

$$(0,0) \to 0; (0,1) \to 1; (1,0) \to 2; (0,2) \to 3; (1,1) \to 4; (2,0) \to 5; \ldots$$

Formal: bijektive Funktion $f : \mathbb{N}^2 \to \mathbb{N}$ vermöge

$$f(m,n) = \sum_{i=1}^{m+n} i + n = \frac{(m+n)(m+n-1)}{2} + n$$

Beispiel einer überabzählbaren Menge

Satz *Die Menge* $2^{\mathbb{N}}$ *ist überabzählbar unendlich.*

Beweisidee:

- indirekter Beweis
- Diagonalisierung

Angenommen, $2^{\mathbb{N}}$ sei abzählbar unendlich.
Dann gäbe es eine bijektive Funktion $\beta : \mathbb{N} \to 2^{\mathbb{N}}$.
Betrachte Menge D mit $D = \{n \in \mathbb{N} \mid n \notin \beta(n)\}$.
Gemäß der Annahme gäbe es dann ein n^* mit $\beta(n^*) = D$.

1. Fall: $n^* \in \beta(n^*)$. Dann folgt $n^* \notin D$, d.h. $n^* \notin \beta(n^*)$; Widerspruch.
2. Fall: $n^* \notin \beta(n^*)$. Dann folgt $n^* \in D$, d.h. $n^* \in \beta(n^*)$; Widerspruch.

Alphabete, Wörter, Sprachen

Alphabet: endliche nichtleere Menge, z.B. $\Sigma = \{a, b, c\}$
Elemente eines Alphabetes nennt man Buchstaben bzw. Symbole

Wort: endliche Folge von Buchstaben, z.B.: $w = abbcbba$

$|w|$: Länge des Wortes w, z.B. $|abbcbba| = 7$
$|w|_x$: Anzahl der Vorkommen des Buchstaben x in w, z.B. $|abbcbba|_b = 4$

ε: leeres Wort (der Länge 0)

Σ^*: Menge aller Wörter über dem Alphabet Σ (einschließlich ε)

$\Sigma^+ = \Sigma^* \setminus \{\varepsilon\}$

(Formale) Sprache über Σ: Teilmenge $L \subseteq \Sigma^*$

Konkatenation von Wörtern

Produkt oder Konkatenation von Wörtern:
2 Wörter werden hintereinander geschrieben, z.B. $abba \cdot ba = abbaba$

$$(w_1 \cdot w_2) \cdot w_3 = w_1 \cdot (w_2 \cdot w_3) \text{ (Assoziativgesetz)}$$
$$w \cdot \varepsilon = \varepsilon \cdot w = w \text{ (}\varepsilon\text{ ist das neutrale Element)}$$

Potenzen eines Wortes:

$$w^0 = \varepsilon; \;\; w^n = w^{n-1} \cdot w \text{ für } n \geq 1$$

Konkatenation von Sprachen

Produkt oder Konkatenation von Sprachen:

$$L_1 \cdot L_2 = \{w_1 \cdot w_2 \mid w_1 \in L_1 \text{ und } w_2 \in L_2\}$$

$$\begin{aligned} \{abba, ab\} \cdot \{ba, baba\} &= \{abbaba, abbababa, abba, abbaba\} \\ &= \{abbaba, abbababa, abba\} \end{aligned}$$

$(L_1 \cdot L_2) \cdot L_3 = L_1 \cdot (L_2 \cdot L_3)$	(Assoziativgesetz)
$L \cdot \{\varepsilon\} = \{\varepsilon\} \cdot L = L$	($\{\varepsilon\}$ ist das neutrale Element)
$L \cdot \emptyset = \emptyset \cdot L = \emptyset$	($\emptyset$ ist das Nullelement)

Potenzen einer Sprache:
$L^0 = \{\varepsilon\}$; $L^n = L^{n-1} \cdot L$ für $n \geq 1$

Kleene'sche Hülle: $L^* = \bigcup_{n=0}^{\infty} L^n$

Darstellung von Zahlen

Eine natürliche Zahl n wird eindeutig durch ihre Binärkodierung $\mathrm{bin}(n)$ dargestellt.

Ein k-Tupel $(n_1, n_2, \ldots, n_k)$ wird eindeutig durch das Wort $\mathrm{bin}(n_1)\#\mathrm{bin}(n_2)\ldots\#\mathrm{bin}(n_k)$ dargestellt.

Eine Funktion $f : \mathbb{N}^k \to \mathbb{N}$ wird eindeutig durch die (Wort-)Funktion $F : \{0, 1, \#\}^* \to \{0, 1\}^*$ dargestellt.

$$F(w) = \begin{cases} \mathrm{bin}(f(n_1, n_2, \ldots, n_k)), & \text{falls } w = \mathrm{bin}(n_1)\#\mathrm{bin}(n_2)\ldots\#\mathrm{bin}(n_k) \\ \text{nicht definiert} & \text{sonst.} \end{cases}$$