

# Kapitel 1 – Grundlagen

## 1. Mathematische Grundlagen

## 2. Beispielrechner ReTI

Albert-Ludwigs-Universität Freiburg

Prof. Dr. Christoph Scholl

Institut für Informatik

WS 2015/16

- Verständigung auf gemeinsame Basis
- Die meisten Begriffe sollten bekannt sein, bzw. werden in anderen Vorlesungen noch formal und im Detail eingeführt.
- Hier: Informale, möglichst intuitive Einführung
  - Mengen, Funktionen, Relationen
  - Boolesche Algebra ( $\{0, 1\}, \wedge, \vee, \neg$ )
  - Graphen, O-Notation
  - Beweistechniken

- Gegeben gewisse Aussagen (**Axiome**), welche andere Aussagen lassen sich aus ihnen herleiten?
- Sind die Axiome wahr und existiert eine solche Herleitung (**Beweis**), so sind die Folgerungen unumstößlich und indiskutabel wahr!
- Beschreiben die Axiome etwa ein **physikalisches System**, so gelten die hergeleiteten Folgerungen für dieses System.
- Die Frage, ob Axiome Realitätsbezug haben, ist aber außerhalb der (reinen) Mathematik!

## Definition

Eine **Menge** ist eine Zusammenfassung von wohldefinierten, paarweise verschiedenen Objekten zu einem Ganzen.

- Die Objekte nennt man **Elemente** der Menge.  
(Für eine formal vollständige Definition der Menge bräuchte man mehrere Vorlesungsstunden.)
- Notation: Sind  $a_1, a_2, \dots, a_n$  paarweise verschieden, so schreibt man die Menge  $M$ , die aus ihnen besteht, als  $M = \{a_1, a_2, \dots, a_n\}$ .
  - $a_i \in M$  bezeichnet, dass  $a_i$  Element von  $M$  ist.

# Beispiele für Mengen

---

- Leere Menge:  $\emptyset$  (es gibt kein  $a \in \emptyset$ ).
- Menge der natürlichen Zahlen:  $\mathbb{N} = \{0, 1, 2, \dots\}$ .
- Menge der booleschen Werte:  $\mathbb{B} = \{0, 1\}$ .
- Achtung: Die Anordnung von Elementen der Menge und gegebenenfalls Wiederholungen sind belanglos:  
 $\{a, b, c\} = \{c, a, b\} = \{a, a, b, c, a, b\}$ .
- Eine Menge kann Elemente enthalten, die selber Mengen sind, z.B.  $\{a, b, \{a\}, \{a, b\}\}$ .

- Man kann eine Menge durch Angabe von **Zusatzbedingungen** spezifizieren.

Beispiele:

- Menge der **ganzen Zahlen**:  
 $\mathbb{Z} = \{z, -z \mid z \in \mathbb{N}\}.$
- Menge der **rationalen Zahlen**:  
 $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{N}, q \neq 0, p, q \text{ teilerfremd}\}.$
- Menge der **endlichen Zeichenketten**:  
 $STRINGS = \{s_1 s_2 \dots s_n \mid n \in \mathbb{N}, s_i \text{ ein Buchstabe}\}.$

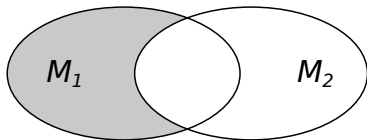
# Teilmengen, Potenzmenge, Mächtigkeit

---

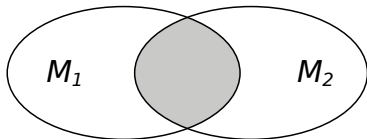
- Menge  $U$  ist **Teilmenge** von  $M$ , wenn jedes Element von  $U$  auch Element von  $M$  ist.
  - Notation:  $U \subset M$  bzw.  $M \supset U$
  - Achtung:  $\{a\} \subset \{a, b, c\}$ , aber  $a \in \{a, b, c\}$
- **Potenzmenge** von  $M$ :  $Pot(M) = \{m \mid m \subset M\}$ .
  - $Pot(\{a, b, c\})$   
 $= \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
- Die Anzahl  $|M|$  der Elemente einer Menge  $M$  heißt **Mächtigkeit** oder **Kardinalität** von  $M$ .

# Operationen auf Mengen 1/2

- **Mengendifferenz:**  $M_1 \setminus M_2 = \{m \mid m \in M_1 \text{ und } m \notin M_2\}$

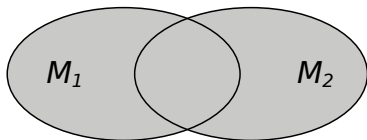


- **Mengenschnitt:**  $M_1 \cap M_2 = \{m \mid m \in M_1 \text{ und } m \in M_2\}$





- Mengenvereinigung:  $M_1 \cup M_2 = \{m \mid m \in M_1 \text{ oder } m \in M_2\}$



- Kartesisches Produkt:

$$M_1 \times M_2 = \{(m_1, m_2) \mid m_1 \in M_1 \text{ und } m_2 \in M_2\}$$

- $(m_1, m_2)$  ist ein Tupel, bei dem es, im Gegensatz zu einer Menge  $\{m_1, m_2\}$ , auf die Reihenfolge ankommt!
- Notation:  $M^n = M \times \dots \times M$  ( $n$  mal).

## Definition

Eine **Relation**  $R$  zwischen den Mengen  $X$  und  $Y$  ist eine Teilmenge von  $X \times Y$ .

- Notation: Statt  $(x, y) \in R$  schreibt man  $xRy$ .
- Beispiele:
  - Relation  $<$  zwischen  $\mathbb{N}$  und  $\mathbb{N}$ .  
 $< = \{(0, 1), (0, 2), \dots, (1, 2), (1, 3), \dots\}$
  - $R = \{(a, b) \mid a, b \in \mathbb{N}, a + b \text{ ungerade}\}$

## Definition

Seien  $X$  und  $Y$  Mengen. Eine **Funktion**  $f : X \rightarrow Y$  ist eine Relation zwischen den Mengen  $X$  und  $Y$ , wobei für jedes  $x \in X$  genau ein  $y \in Y$  existiert, so dass  $(x, y) \in f$ .

■  $X$  heißt Definitionsbereich,  $Y$  Wertebereich von  $f$ .

■ Notation: Statt  $(x, y) \in f$  schreibt man  $y = f(x)$ .

■ Beispiele:

■ **Quadratfunktion**  $f : \mathbb{N} \rightarrow \mathbb{N}, f(x) = x^2$ .

$$f = \{(0, 0), (1, 1), (2, 4), (3, 9), (4, 16), (5, 25), \dots\}$$

■ **Kardinalitätsfunktion**  $f : \text{Pot}(\{a, b, c\}) \rightarrow \mathbb{N}$ .

$$f = \{(\emptyset, 0), (\{a\}, 1), (\{b\}, 1), (\{c\}, 1), (\{a, b\}, 2), (\{a, c\}, 2), (\{b, c\}, 2), (\{a, b, c\}, 3)\}$$

■ **Sinusfunktion**  $\sin = \{(x, \sin(x)) \mid x \in \mathbb{R}\}$

- Jede Funktion ist auch eine Relation.
- Aber es gibt natürlich Relationen, die keine Funktionen sind.
- Beispiel:
  - $\sin^{-1} = \{(\sin(x), x) \mid x \in \mathbb{R}\}$  ist eine Relation, aber keine Funktion!

# Summen und Produkte (Notation)

---

- Wir schreiben für  $f : \mathbb{N} \rightarrow \mathbb{R}$

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

$$\prod_{i=m}^n f(i) = f(m) \cdot f(m+1) \cdot \dots \cdot f(n-1) \cdot f(n)$$

- Beispiel:

$$\sum_{i=0}^5 i^2 = 0^2 + 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$$

- Schreibweise mit beliebigen Bedingungen:

$$\sum_{i,j>0, i+2j\leq 5} (i^2/j) = (1^2/1) + (1^2/2) + (2^2/1) + (3^2/1) = 14,5$$

## Definition

- $\mathbb{B} := \{0, 1\}$
- **Konjunktion** (UND-Verknüpfung)  $\wedge : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$   
 $0 \wedge 0 = 0, \quad 0 \wedge 1 = 0, \quad 1 \wedge 0 = 0, \quad 1 \wedge 1 = 1$
- **Disjunktion** (ODER-Verknüpfung)  $\vee : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$   
 $0 \vee 0 = 0, \quad 0 \vee 1 = 1, \quad 1 \vee 0 = 1, \quad 1 \vee 1 = 1$
- **Negation**  $\neg : \mathbb{B} \rightarrow \mathbb{B}$   
 $\neg 0 = 1, \quad \neg 1 = 0$
- **Boolescher Ausdruck**
  - Die Elemente aus  $\mathbb{B}$  sind boolesche Ausdrücke.
  - Seien  $A$  und  $B$  boolesche Ausdrücke, dann sind  $(A \wedge B)$ ,  $(A \vee B)$ ,  $(\neg A)$  wieder boolesche Ausdrücke.

## Konventionen

- Man schreibt auch  $\cdot$  statt  $\wedge$  und  $+$  statt  $\vee$ .
- Für  $\neg x$  sind viele Notationen üblich:  $\sim x$ ,  $x'$  oder  $\bar{x}$ .
- Zur Vereinfachung der Notation bei booleschen Ausdrücken vereinbaren wir:  
Negation  $\sim$  bindet stärker als Konjunktion  $\cdot$ , Konjunktion  $\cdot$  bindet stärker als Disjunktion  $+$ .

## Axiome der booleschen Algebra

**Kommutativität:**  $x + y = y + x$

$$x \cdot y = y \cdot x$$

**Assoziativität:**  $x + (y + z) = (x + y) + z$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

**Absorption:**  $x + (x \cdot y) = x$

$$x \cdot (x + y) = x$$

**Distributivität:**  $x + (y \cdot z) = (x + y) \cdot (x + z)$

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

**Komplement:**  $x + (y \cdot \neg y) = x$

$$x \cdot (y + \neg y) = x$$



- Neben der vorgestellten gibt es weitere boolesche Algebren, in denen diese Axiome gelten.
- Die folgenden Regeln sind aus den Axiomen ableitbar:

## Weitere Regeln für boolesche Algebren

**Doppeltes Komplement:**  $\neg(\neg x) = x$

**Idempotenz:**  $x + x = x \cdot x = x$

**De-Morgan-Regel:**  $\neg(x + y) = (\neg x) \cdot (\neg y)$

$$\neg(x \cdot y) = (\neg x) + (\neg y)$$

**Consensus-Regel:**

$$\begin{aligned} & (x \cdot y) + ((\neg x) \cdot z) \\ &= (x \cdot y) + ((\neg x) \cdot z) + (y \cdot z) \\ & (x + y) \cdot ((\neg x) + z) \\ &= (x + y) \cdot ((\neg x) + z) \cdot (y + z) \end{aligned}$$

## Definition

Eine **boolesche Funktion**  $f$  in  $n$  Variablen und mit  $m$  Ausgängen ist eine Funktion

$$f : \mathbb{B}^n \rightarrow \mathbb{B}^m (n, m \in \mathbb{N}).$$

- Die Menge aller booleschen Funktionen in  $n$  Variablen mit  $m$  Ausgängen ist

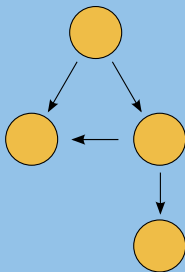
$$\mathbb{B}_{n,m} := \{f \mid f : \mathbb{B}^n \rightarrow \mathbb{B}^m\}.$$

- Wir schreiben abkürzend  $\mathbb{B}_n$  statt  $\mathbb{B}_{n,1}$ .
- Ein digitaler Schaltkreis ohne Speicherelemente, mit  $n$  Eingängen und  $m$  Ausgängen realisiert eine solche Funktion! (Details später)

## Definition

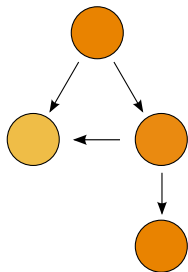
$G = (V, E)$  ist ein **gerichteter Graph**, wenn folgendes gilt:

- $V$  endliche, nichtleere Menge (**Knoten**)
- $E$  endliche Menge (**Kanten**)
- Abbildungen  $Q : E \rightarrow V$  und  $Z : E \rightarrow V$   
 $Q(e)$  ist Quelle,  $Z(e)$  Ziel einer Kante  $e$
- Abbildungen  $indeg : V \rightarrow \mathbb{N}$  und  $outdeg : V \rightarrow \mathbb{N}$   
 $indeg(v) = |\{e \mid Z(e) = v\}|$  ist der **Eingangsgrad**,  
 $outdeg(v) = |\{e \mid Q(e) = v\}|$  der **Ausgangsgrad** von  $v$ .



# Pfade in gerichteten Graphen

- Ein Knoten mit
  - $\text{indeg}(v) = 0$  heißt **Wurzel**.
  - $\text{outdeg}(v) = 0$  heißt **Blatt**.
  - $\text{outdeg}(v) > 0$  heißt **innerer Knoten**.
- Ein **Pfad** (der Länge  $k$ ) in  $G$  ist eine Folge von  $k$  Kanten  $e_1, e_2, \dots, e_k$  ( $k \geq 0$ ) mit  $Z(e_i) = Q(e_{i+1})$  für alle  $i$  ( $k-1 \geq i \geq 1$ )
- Ein **Zyklus** in  $G$  ist ein Pfad der Länge  $\geq 1$  in  $G$ , bei dem Ziel und Quelle identisch sind ( $G$  heißt **azyklisch**, falls kein Zyklus in  $G$  existiert).
- Die **Graph-Tiefe** eines azyklischen Graphen ist definiert als die Länge des längsten Pfades in  $G$ .

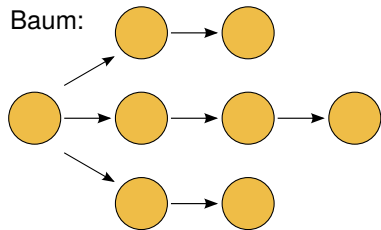


## Definition

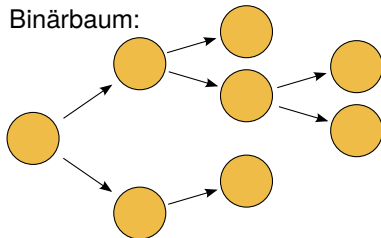
Ein **Baum** ist ein gerichteter, azyklischer Graph mit genau einer Wurzel  $w$  ( $\text{indeg}(w) = 0$ ) und  $\text{indeg}(v) = 1$  für alle andere Knoten  $v$ . Ein Baum heißt **binär** (bzw. **Binärbaum**), wenn für seine innere Knoten  $v$   $\text{outdeg}(v) \leq 2$  gilt.

Beispiele:

Baum:



Binärbaum:



# Groß-O-Notation (1/2)

- Seien  $f, g: \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$ .

Man schreibt  $f(x) \in O(g(x))$ , wenn es  $c \in \mathbb{R}_0^+, x_0 \in \mathbb{R}_0^+$  gibt, so dass  $f(x) \leq c \cdot g(x)$  für alle  $x > x_0$  gilt.

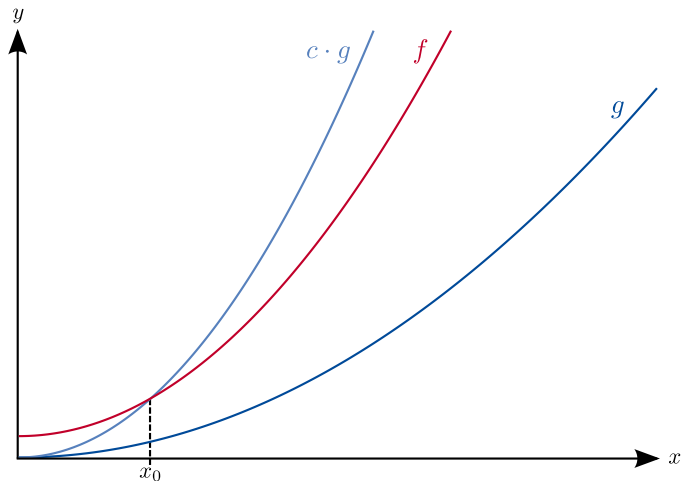
- Beispiel:  $5x + 2 \in O(x^2)$

Beweis: Setze  $c = 6, x_0 = 2$

$$5x + 2 < 5x + x = 6x \leq 6 \cdot x^2, \text{ für } x > 2.$$

- Groß-O-Notation wird verwendet, um Größe von parametrisierten Objekten (z.B. Graphen), Laufzeit von Algorithmen (Anzahl von Rechenschritten in Abhängigkeit von der Eingabe) usw. **asymptotisch**, d.h. bis auf eine multiplikative Konstante, abzuschätzen.
- Die Notation  $f(x) = O(g(x))$  ist weit verbreitet, aber eigentlich falsch, da  $O(g(x))$  eine Menge ist. So folgt aus  $f(x) = O(g(x))$  und  $h(x) = O(g(x))$  keinesfalls  $f(x) = h(x)$ !

# Groß-O-Notation (2/2)



- Sukzessive Folgerungen bzw. Direkter Beweis
- Indirekter Beweis bzw. Beweis durch Widerspruch
- Vollständige Induktion



Gegeben Aussage  $A$ , es soll Aussage  $B$  bewiesen werden.

■ Sukzessive Folgerungen:

Aus  $A$  folgt  $C$ , aus  $C$  folgt  $D$ , aus  $D$  folgt  $B$ , also gilt  $B$ .

# Beispiel: Sukzessive Folgerungen

- Gegeben  $f, g, h$ ,  $f(x) \in O(g(x))$ ,  $g(x) \in O(h(x))$ .  
Dann gilt  $f(x) \in O(h(x))$ .

## Beweis:

- 1 Aus  $f(x) \in O(g(x))$  folgt die Existenz von  $c_f, x_{0f} \in \mathbb{R}_0^+ : f(x) \leq c_f \cdot g(x)$  für alle  $x > x_{0f}$ . Aus  $g(x) \in O(h(x))$  folgt die Existenz von  $c_g, x_{0g} \in \mathbb{R}_0^+ : g(x) \leq c_g \cdot h(x)$  für alle  $x > x_{0g}$ .
- 2 Man setze  $x_0 := \max\{x_{0f}, x_{0g}\}$ . Dann gilt für alle  $x > x_0$  sowohl  $f(x) \leq c_f \cdot g(x)$  als auch  $g(x) \leq c_g \cdot h(x)$ .
- 3 Man setze  $c := c_f \cdot c_g$ . Dann gilt für alle  $x > x_0$  :  
 $f(x) \leq c_f \cdot g(x) \leq c_f \cdot (c_g \cdot h(x)) = c \cdot h(x)$ .  
Dies bedeutet aber gerade  $f(x) \in O(h(x))$

Es soll Aussage  $S$  bewiesen werden.

- **Indirekter Beweis:** Man nimmt an,  $\neg S$  (also die Umkehrung von  $S$ ) würde gelten. Daraus leitet man einen Widerspruch her (z.B. “es gilt  $C$  **und**  $\neg C$ ”, “ $31 = 42$ ”, ...).
- Da der Widerspruch schrittweise aus  $\neg S$  logisch hergeleitet wurde, kann  $\neg S$  nicht gelten und somit muss  $S$  gelten.

- Betrachte den Spezialfall  $S = A \Rightarrow B$ .
  - Dann ist  $\neg S = A \wedge \neg B$ . Man nimmt also an, dass  $A$  gilt, aber  $\neg B$ .
  - Ergibt sich aus der Annahme ein Widerspruch, dann muss aus der Gültigkeit von  $A$  die Gültigkeit von  $B$  folgen.
  - Ergibt sich der Widerspruch speziell durch Herleitung von  $\neg A$  aus  $\neg B$ , dann reduziert sich der Widerspruchsbeweis auf den Spezialfall Beweis der "Kontraposition"  $\neg B \Rightarrow \neg A$ .
  - $A \Rightarrow B$  und  $\neg B \Rightarrow \neg A$  sind logisch äquivalent.
- Implizit setzt man immer die Gültigkeit sämtlicher Axiome voraus. Sei  $Ax$  die Aussage "Sämtliche Axiome gelten".
- Dann ist  $S' = (A \wedge Ax) \Rightarrow B$  zu beweisen.
- Annahme ist dann also:  $\neg S' = A \wedge Ax \wedge \neg B$  gilt.

# Beispiel: Indirekter Beweis

- Zu zeigen:  $x^2 \notin O(x)$

## Beweis:

- Wir nehmen an, dass  $x^2 \in O(x)$  wäre. Dann gibt es  $c$  und  $x_0 \in \mathbb{R}_0^+$ , so dass für alle  $x > x_0$  gilt:

$$x^2 \leq c \cdot x \quad (1)$$

- Beweisstrategie: Versuche ein  $x_1 > x_0$  zu finden mit  $x_1^2 > c \cdot x_1$  – das wäre der gewünschte Widerspruch.
- Für alle  $x > c \in \mathbb{R}_0^+$  ist  $x^2 > c \cdot x$ . Ein beliebiges  $x_1 > c$  liefert also einen Widerspruch zu (1)!

# Vollständige Induktion

---

- Die vollständige Induktion ist eine Beweismethode für Aussagen, die für alle natürlichen Zahlen  $n$  gelten sollen.
- Zuerst wird die Aussage für den Basisfall  $n = 0$  beweisen (manchmal auch  $n = 1$  oder höher).
- Dann wird der Induktionsschritt durchgeführt:  
Unter der Annahme, dass die Aussage für  $n$  gilt (Induktionsvoraussetzung) wird bewiesen, dass die Aussage auch für  $n + 1$  gilt.
- Daraus folgt die Gültigkeit der Aussage für alle natürlichen Zahlen.

## ■ Behauptung:

$$\sum_{k=1}^n \frac{1}{k(k+1)} = \frac{n}{n+1} \text{ gilt für alle } n \in \mathbb{N}.$$

## ■ Induktionsanfang:

Zeige die Behauptung für  $n = 0$ .

$$\sum_{k=1}^0 \frac{1}{k(k+1)} = 0 = \frac{0}{0+1}$$

# Vollständige Induktion: Beispiel (2/2)

## ■ Induktionsvoraussetzung (IV):

Nehme an, die Behauptung gilt für *ein*  $n \in \mathbb{N}$ .

Also: Es gibt ein  $n \in \mathbb{N}$  für das gilt:  $\sum_{k=1}^n \frac{1}{k(k+1)} = \frac{n}{n+1}$

## ■ Induktionsschritt:

Zeige die Behauptung für  $n+1$ .

$$\begin{aligned} \sum_{k=1}^{n+1} \frac{1}{k(k+1)} &= \sum_{k=1}^n \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} \stackrel{\text{IV}}{=} \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} \\ &= \frac{n(n+2)+1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{(n+1)}{(n+2)} = \frac{(n+1)}{(n+1)+1} \quad \square \end{aligned}$$