

Kapitel 1 – Grundlagen

1. Mathematische Grundlagen

2. Beispielrechner ReTI

Albert-Ludwigs-Universität Freiburg

Dr. Tobias Schubert, Dr. Ralf Wimmer

Professur für Rechnerarchitektur

WS 2016/17

- 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? *die gelten*
- 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 $a \in \emptyset$). \mathbb{N}
- Menge der natürlichen Zahlen: $\mathbb{N} = \{0, 1, 2, \dots\}$.
- Menge der booleschen Werte: $\mathbb{B} = \{0, 1\}$. \mathbb{B}
falsch wahr
- 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. $\{a, b, \{a\}, \{a, b\}\} = M$ enthält 4 Elemente, wobei die letzten beiden wieder Mengen sind.

Spezifikation von Mengen

- 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**:

$$\mathbb{Q} = \{p/q \mid p \in \mathbb{N}, q \in \mathbb{Z}, q \neq 0, p, q \text{ teilerfremd}\}.$$

- Menge der **endlichen Zeichenketten**:

$$\text{STRINGS} = \{s_1 s_2 \dots s_n \mid n \in \mathbb{N}, s_i \text{ ein Buchstabe}\}.$$

Menge $\{a\}$ ist
Untermenge

- Menge U ist Untermenge 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 $a \in \{a, b, c\}$

a ist Element

- Potenzmenge von M : $Pot(M) = \{m \mid m \subset M\}$.

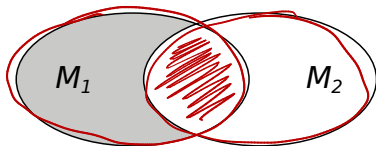
- $(Pot(\{a, b, c\})) \mid \rightsquigarrow 8$

$$= \{\underbrace{\emptyset}_1, \underbrace{\{a\}}_2, \underbrace{\{b\}}_2, \underbrace{\{c\}}_2, \underbrace{\{a, b\}}_4, \underbrace{\{a, c\}}_4, \underbrace{\{b, c\}}_4, \underbrace{\{a, b, c\}}_8\}$$

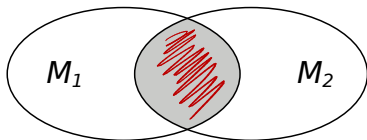
- Die Anzahl $|M|$ der Elemente einer Menge M heißt Mächtigkeit oder Kardinalität von M .

Operationen auf Mengen 1/2

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

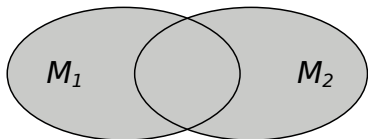


- **Mengenschnitt:** $M_1 \cap M_2 = \{m \mid m \in M_1 \text{ und } m \in M_2\}$



Operationen auf Mengen 2/2

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



- **Kartesisches Produkt:**

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

- (m_1, m_2) ist ein Tupel, bei dem es, im Gegensatz zu einer Menge $\{m_1, m_2\}$, auf die Reihenfolge ankommt!

$$\hookrightarrow = \{m_2, m_1\}$$

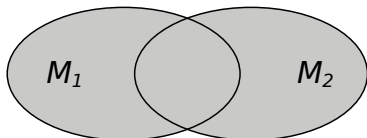
- Notation: $\underline{M^n} = M \times \dots \times M$ (n mal).

$$M^2 = M \times M$$

$$\{(m_1, \dots, m_n) \mid \begin{matrix} m_1 \in M, \\ m_2 \in M, \\ \vdots \\ m_n \in M \end{matrix}\}$$



- **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).

SMILE – Mengen

Handwritten notes above the table:

- $\{ \emptyset, \{1\}, \dots, \{3, \dots, 3\} \}$
- $\{2, 4, 3\}$
- $\{1, 2, 3\}$
- $\{1, 1 \notin UH_1\}$

	①	2	3	4	5
UH_1	0	1	0	1	0
UH_2	1	1	0	0	0

Frage: Welche der folgenden Aussagen sind wahr?

a. Pot($\{a, b, c\}$) = 3 Elemente $\rightarrow 2^3 = 8$ Gilt
 $\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

b. Pot($\{1, 2, 3, 4, 5\}$) = 32 unknown

c. $\{a, a, b, c\}$ \ $\{a, b\}$ = $\{a, c\}$ gilt nicht!

d. $|\{a, a, b, c\}|$ = 3 gilt

e. $(\mathbb{Z} \setminus \mathbb{Q}) \cup \mathbb{Q} = \mathbb{Z}$ gilt nicht!

$|\{a, b, c\}| = 3$

$\{a, a, b, c\} = \{a, b, c\}$
 $\{a, b, c\} \setminus \{a, b\} = \{c\}$

00000
 00001
 00010
 ...

2^5
 =
 32

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} .

$$\leq = \{(\underline{0}, \underline{1}), (\underline{0}, \underline{2}), \dots, (\underline{1}, \underline{2}), (\underline{1}, \underline{3}), \dots\}$$

- $R = \{(a, b) \mid a, b \in \mathbb{N}, a + b \text{ ungerade}\}$

$$\uparrow \rightarrow (2, 5) \in R$$

$$R := <$$

$$0 < 1$$

$$< : \mathbb{N} \times \mathbb{N}$$

$$\begin{array}{l} x = 0 \rightarrow \begin{array}{l} y = 1 \\ y = 2 \\ y = 3 \end{array} \end{array}$$

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: ~~x~~ y

■ **Quadratfunktion** $f : \mathbb{N} \rightarrow \mathbb{N}, f(x) = x^2$.
 $f = \{(\underline{0}, \underline{0}), (\underline{1}, \underline{1}), (\underline{2}, \underline{4}), (\underline{3}, \underline{9}), (\underline{4}, \underline{16}), (\underline{5}, \underline{25}), \dots\}$

■ **Kardinalitätsfunktion** $f : \text{Pot}(\{a, b, c\}) \rightarrow \mathbb{N}$.
 $f = \{(\emptyset, 0), (\{a\}, 1), (\{b\}, 1), (\{c\}, 1), (\{a, b\}, 2), (\{a, c\}, 2), (\{b, c\}, 2), (\{a, b, c\}, 3)\}$

\rightarrow da $\{a, b\}$ besteht aus 2 Elementen
 εf

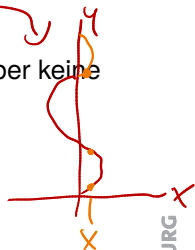
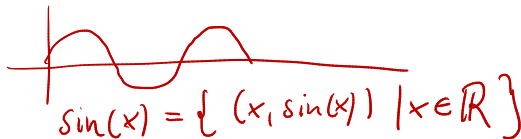
Beispiele: Relationen, Funktionen

- Jede Funktion ist auch eine Relation. ✓

- Aber es gibt natürlich Relationen, die keine Funktionen sind. *(liegt an dem „genau“ in Def. Folie 12)*

- Beispiel:

- $\sin^{-1}(x) = \{(\sin(x), x) \mid x \in \mathbb{R}\}$ ist eine Relation, aber keine Funktion!



Summen und Produkte (Notation)

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

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

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

- Beispiel:

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

- Schreibweise mit beliebigen Bedingungen:

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

Handwritten notes:

- Red arrows pointing to the terms: $(1^2/1)$, $(1^2/2)$, $(2^2/1)$, $(3^2/1)$.
- Red text: $i \in \{1, 2, 3\}$
- Red text: $j \in \{1, 2\}$

Boolesche Algebra ($\{0, 1\}, \wedge, \vee, \neg$) 1/4

Definition

$$x, y, z \in \mathbb{B}$$

$$\mathbb{B} := \{0, 1\}$$

$$\text{Konjunktion (UND-Verknüpfung)} \wedge : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$$

$$\underline{0 \wedge 0 = 0}, \quad \underline{0 \wedge 1 = 0}, \quad \underline{1 \wedge 0 = 0}, \quad \underline{1 \wedge 1 = 1}$$

$$\text{Disjunktion (ODER-Verknüpfung)} \vee : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$$

$$\underline{0 \vee 0 = 0}, \quad \underline{0 \vee 1 = 1}, \quad \underline{1 \vee 0 = 1}, \quad \underline{1 \vee 1 = 1}$$

$$\text{Negation } \neg : \mathbb{B} \rightarrow \mathbb{B}$$

$$\neg 0 = 1, \quad \neg 1 = 0$$

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.

$$\begin{array}{l} x \mapsto 0/1 \\ y \mapsto 0/1 \\ z \mapsto 0/1 \end{array}$$

$$x \wedge (y + z)$$

$$\begin{array}{l} x=1 \\ y=0 \\ z=0 \end{array}$$

$$\begin{array}{l} 1 \wedge (0 \vee 0) \\ = 1 \wedge 0 \\ = 0 \end{array}$$

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 \wedge bindet stärker als Disjunktion $+$ \vee

Boolesche Algebra ($\{0, 1\}, \wedge, \vee, \neg$) 3/4

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

Auslöschung

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

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

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

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

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

$x = 1 \rightarrow 1 \vee (1 \cdot y) = 1 \vee x$
 $x = 0 \rightarrow 0 \vee (0 \cdot y) = 0 \vee 0 = 0$
 $x = 1$

immer gleich

$$(0 \wedge \neg 0) = 0 \wedge 1 = 0$$

$$(1 \wedge \neg 1) = 1 \wedge 0 = 0$$



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

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

SMILE – Boolesche Ausdrücke

$13 = 42$ $\swarrow \searrow$ gleichbed.
mit
 $13 \neq 42$

Frage: Welche dieser Umformungen Boolescher Ausdrücke sind richtig? Das heißt, die Gleichung ist immer erfüllt für alle möglichen Werte von $x, y \in \mathbb{B}$.

a. $x + \underline{1} = \underline{1} + x \cdot y$

$\Leftrightarrow 1 = 1$

b. $x + \neg x = x$

$x=0 \rightarrow 0+1 \neq 0$ $\swarrow \searrow$

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

$\underbrace{\underbrace{\underbrace{\neg x + 0}_{=0}}_{\neg x}}_{\neg x}$
 $x \cdot \neg x = 0$

$\rightarrow 0 = x$

$\{$
 x kann auch 1
sein $\Rightarrow 0=1$ $\swarrow \searrow$

Boolesche Algebra ($\{0, 1\}, \wedge, \vee, \neg$) 4/4

- 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: $(x \cdot y) + ((\neg x) \cdot z) = (x \cdot y) + ((\neg x) \cdot z) + (y \cdot z)$

Resolutions-Regeln

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

"mit $y = z = 1$ habe ich erfüllt ($= 1$)"

$x = 1: (1 + y) \wedge (0 + z) = 1 \wedge z = z$
 $x = 0: (0 + y) \wedge (1 + z) = y \wedge (1 + z) = y$

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)



Gerichteter Graph

Definition

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

- V endliche, nichtleere Menge (**Knoten**)

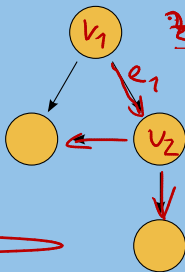
↳ Vertex

- E endliche Menge (**Kanten**)

↳ edge

- Abbildungen $Q : E \rightarrow V$ und $Z : E \rightarrow V$
 $Q(e)$ ist Quelle, $Z(e)$ Ziel einer Kante e

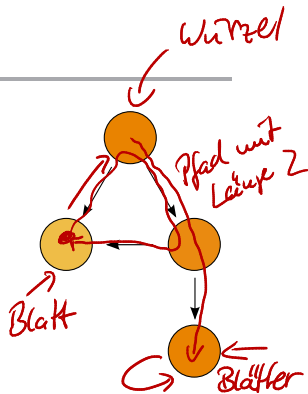
- Abbildungen $\text{indeg} : V \rightarrow \mathbb{N}$ und $\text{outdeg} : V \rightarrow \mathbb{N}$
 $\text{indeg}(v)$ = $|\{e \mid Z(e) = v\}|$ ist der **Eingangsgrad**,
 $\text{outdeg}(v)$ = $|\{e \mid Q(e) = v\}|$ der **Ausgangsgrad** von v .



outdeg = out degree

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 ≥ 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 .

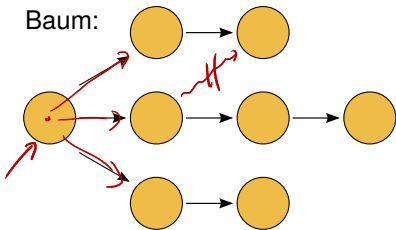


Definition

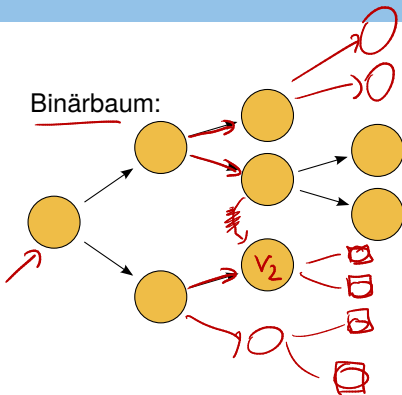
Ein **Baum** ist ein gerichteter, azyklischer Graph mit genau einer Wurzel w ($\text{indeg}(w) = 0$) und $\text{indeg}(v) = 1$ für alle andere Knoten v . Ein Baum heißt **binär** (bzw. **Binärbaum**), wenn für seine innere Knoten v $\text{outdeg}(v) \leq 2$ gilt.

Beispiele:

Baum:



Binärbaum:



Groß-O-Notation (1/2)

positive, reelle Zahlen (inklusive 0)

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

Beweis: Setze $c = 5, x_0 = 1$

$$5x + 2 \leq 5 \cdot x^2, \text{ für } x > 1.$$

$$x=1: 5 \cdot 1 + 2 = 7 \not\leq 5 \cdot 1^2 = 5$$

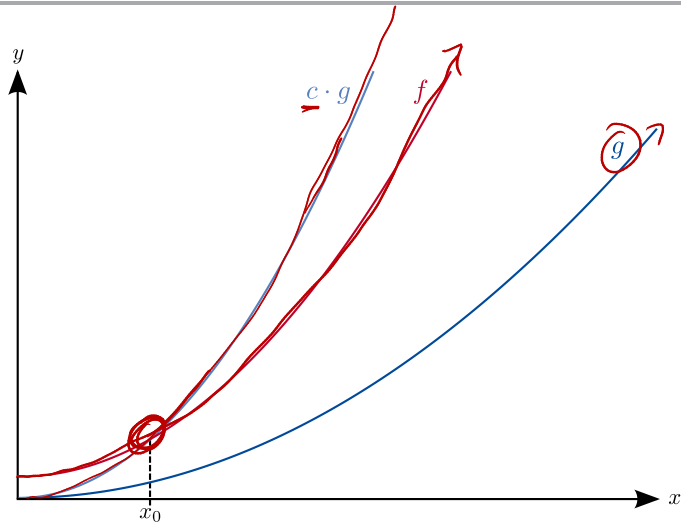
$$x=2: 5 \cdot 2 + 2 = 12 \leq 5 \cdot 2^2 = 20$$

- 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.

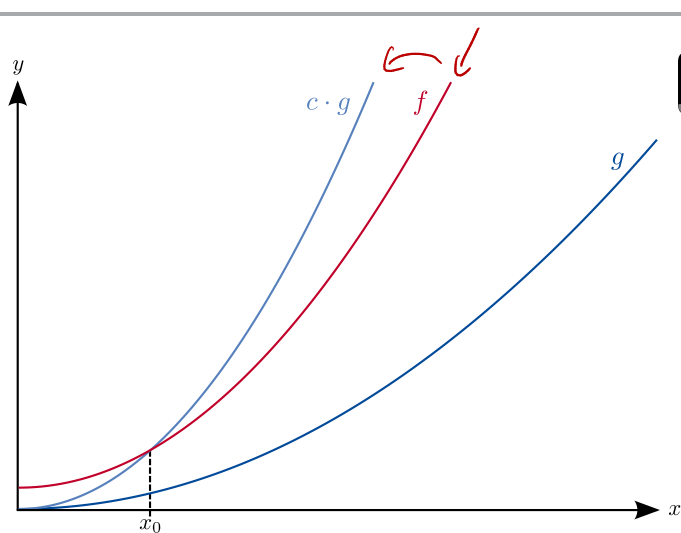
$$f(x) = 5x + 2$$
$$g(x) = 2x^2$$

- Die Notation $f(x) = O(g(x))$ ist weit verbreitet, aber $\Rightarrow f(x), h(x) \in O(x^2)$ 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)

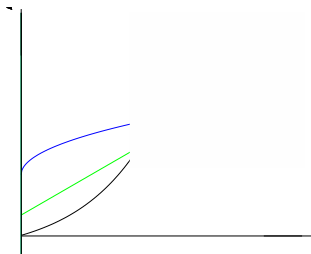


Groß-O-Notation (2/2)



SMILE – O-Notation

Gegeben: *blau*
 $f(x) = \sqrt{x} + 2$, *schwarz*
 $g(x) = 0,5e^x$, *grün*
 $h(x) = x + 1$,
Welche Aussagen sind dann wahr?



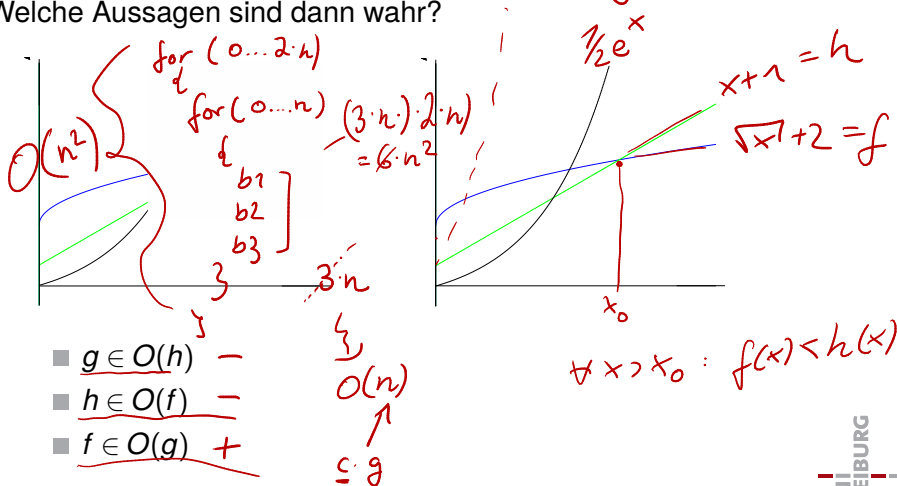
- $g \in O(h)$ *NEIN*
- $h \in O(f)$ *NEIN*
- $f \in O(g)$ *JA*

SMILE – O-Notation

Gegeben:

$$f(x) = \sqrt{x} + 2, \quad g(x) = 0,5e^x, \quad h(x) = x + 1,$$

Welche Aussagen sind dann wahr?



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

Sukzessive Folgerungen

Gegeben Aussage A , es soll Aussage B bewiesen werden.

■ **Sukzessive Folgerungen:**

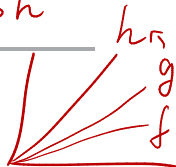
Aus A folgt C , aus C folgt D , aus D folgt B , also gilt B .

$$A \rightarrow C \rightarrow D \rightarrow \frac{B}{\uparrow}$$

□
q.e.d.

Beispiel: Sukzessive Folgerungen

„ $f \leadsto g \leadsto h$ “



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

Beweis:

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

Annahme: $\neg S$

$$\underbrace{31=42} \rightarrow \text{Widerspruch} \rightarrow S$$

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.

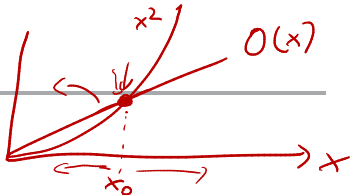
Indirekter Beweis 2/2

aus A folgt B

$$A=1 \rightarrow B=1$$

- Betrachte den Spezialfall $\underbrace{S \approx A \Rightarrow B}_{\text{aus } A \text{ folgt } B}$.
 - Dann ist $\underbrace{\neg S \approx A \wedge \neg B}_{\text{aus } A \text{ folgt } B}$. 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. $B=0 \rightarrow A=0$
- 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 , so dass für $x > x_0$ gilt:

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

- Nun suchen wir ein x_1 , für das $x_1^2 = c \cdot x_1$. Dies ist für $x_1 = c$ der Fall.

- Für alle $x > x_1 = c$ ist $x^2 > c \cdot x$. Man wähle ein $x_2 > \max\{x_0, x_1\}$. Dann gilt auch für x_2 :

$$\rightarrow x_2^2 > c \cdot x_2 \quad (2)$$

- Andererseits muss für x_2 auch (1) gelten. Widerspruch! Somit kann die Annahme nicht stimmen.

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.

$n=0, 1, 2, 3$
↓
↓
↓
↓
 n
 $(n+1)$

Vollständige Induktion: Beispiel (1/2)

■ 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 $n = 1$.

$$\sum_{k=1}^1 \frac{1}{k(k+1)} = \frac{1}{1(1+1)} = \frac{1}{2} = \frac{1}{1+1}$$

Vollständige Induktion: Beispiel (2/2)

■ Induktionsvoraussetzung (IV):

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

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

■ Induktionsschritt:

Zeige die Behauptung für $n+1$.

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

(n+1) - Summenglied