Kapitel 1 – Grundlagen

1. Mathematische Grundlagen
2. Beispielrechner ReTI

Albert-Ludwigs-Universität Freiburg

Prof. Dr. Christoph Scholl
Institut für Informatik
WS 2015/16

Mathematische Grundlagen

- 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
    - e
      Boolsche Algebra $(\{0,1\},\wedge,\vee,\neg)$
    - Graphen, O-Notation
    - Beweistechniken

„Philosophie" der Mathematik

- 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!

Bsp. für Axiome: – Geg. Gerade g und Punkt P nicht auf Gerade, dann gibt es genau eine Gerade, die durch P verläuft und parallel ist zu g
– jede natürliche Zahl hat einen Nachfolger

3

Menge (Naive Definition)

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

Spezifikation von Mengen

- Man kann eine Menge durch Angabe von Zusatzbedingungen spezifizieren.

  Beispiele:

  - Menge der ganzen Zahlen:
    $\mathbb{Z} = \{z, -z \mid z \in \mathbb{N}\}$. (Beachte: Man geht davon aus, dass die Objekte 0 und -0 gleich sind.)
  - Menge der rationalen Zahlen:
    $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{N}, q \neq 0, p, q$ teilerfremd$\}$. Was ist mit $\frac{6}{8}$?
    Wenn man „teilerfremd" nicht fordert, dann man eine Regel für Gleichheit definieren, z.B. $\frac{3}{4} = \frac{6}{8}$.
  - Menge der endlichen Zeichenketten:
    $STRINGS = \{s_1 s_2 \ldots s_n \mid n \in \mathbb{N}, s_i$ ein Buchstabe$\}$.
    Element einer speziellen Menge (Alphabet)

Wenn $n=0$, dann ergibt sich das „leere Wort", man bezeichnet das leere Wort mit ε.

Teilmengen, Potenzmenge, Mächtigkeit

- Menge U ist Teilmenge von M, wenn jedes Element von U auch Element von M ist.
  - Notation: $U \subset M$ bzw. $M \supset U$ „ist Obermenge von"
  - Achtung: $\{a\} \subset \{a,b,c\}$, aber $a \in \{a,b,c\}$
- Potenzmenge von M : $Pot(M) = \{m \mid m \subset M\}$. $= \mathcal{P}(M) = 2^M$
  - $Pot(\{a,b,c\})$
    $= \{\emptyset,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$

$M = \{a, \{b\}\}$
$\Rightarrow \mathcal{P}(M) = \{\emptyset, \{a\}, \{\{b\}\}, \{a, \{b\}\}\}$

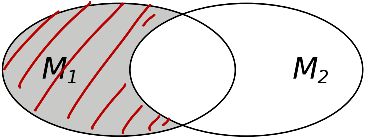
- Die Anzahl $|M|$ der Elemente einer Menge M heißt Mächtigkeit oder Kardinalität von M.

Sei M eine n-elementige Menge.
Was ist die Mächtigkeit von $Pot(M)$ $(= \mathcal{P}(M))$?
$\Longrightarrow 2^n$

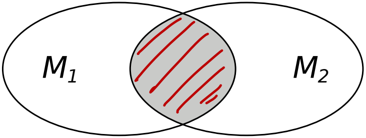
Operationen auf Mengen 1/2

„M_1 ohne M_2“

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

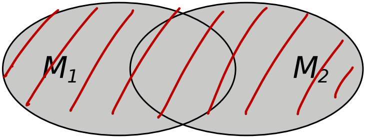


- **Mengenschnitt**: $M_1 \cap M_2 = \{m \mid m \in M_1 \text{ \underline{und} } m \in M_2\}$



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: Paare, 2-Tupel
  $M_1 \times M_2 = \{(m_1, m_2) \mid m_1 \in M_1 \text{ und } m_2 \in M_2\}$
  - (m_1, m_2) ist ein Tupel, bei dem es, im Gegensatz zu einer Menge $\{m_1, m_2\}$, auf die Reihenfolge ankommt!
  - Notation: $M^n = \underbrace{M \times \cdots \times M}$ (n mal).
    $= \{(m_1, m_2, \ldots, m_n) \mid m_1, \ldots, m_n \in M\}$

Bem.: Rein formal ist $\underline{((M_1 \times M_2) \times M_3)}$ also ungleich $(M_1 \times (M_2 \times M_3))$, aber meistens identifiziert man Elemente $((m_1, m_2), m_3) \in ((M_1 \times M_2) \times M_3)$ und $(m_1, (m_2, m_3)) \in (M_1 \times (M_2 \times M_3))$ mit $(m_1, m_2, m_3) \in$

$M_1 \times M_2 \times M_3$.

Relationen

Definition

Eine Relation R zwischen den Mengen X und Y ist eine Teilmenge von $X \times Y$. $= \{(x,y) \mid x \in X, y \in Y\}$

- Notation: Statt $(x,y) \in R$ schreibt man xRy.
- Beispiele:
  - Relation $<$ zwischen $\mathbb{N}$ und $\mathbb{N}$. $(< \subseteq \mathbb{N} \times \mathbb{N})$

    $<= \{(0,1),(0,2),\ldots,(1,2),(1,3),\ldots\}$ $\quad 1 < 3$ bzw. $(1,3) \in <$

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

- $S = \{(a,b) \mid a,b \in \mathbb{N},$ (a ungerade und b gerade) oder (a gerade und b ungerade) $\}$

Wie steht R zu S? $\quad R = S$ (Gleichheit von Mengen R und S zeigt man durch $R \subseteq S$ und $S \subseteq R$)

Funktionen

Definition

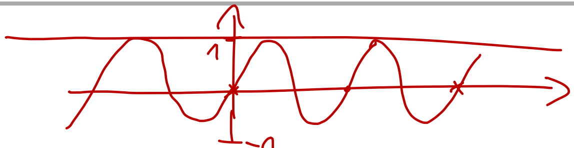
Seien X und Y Mengen. Eine Funktion $f : X \to Y$ ist eine Relation zwischen den Mengen X und Y, wobei für jedes $x \in X$ genau ein $y \in Y$ existiert, so dass $(x, y) \in f$.

- X heißt Definitionsbereich, Y Wertebereich von f.

es gibt eines und es darf nicht mehr geben!

- Notation: Statt $(x, y) \in f$ schreibt man $y = f(x)$.
- Beispiele: $f \subseteq \mathbb{N} \times \mathbb{N}$
  - Quadratfunktion $f : \mathbb{N} \to \mathbb{N}, f(x) = x^2$. (x, x^2)
    $f = \{(0, 0), (1, 1), (2, 4), (3, 9), (4, 16), (5, 25), \ldots\}$
  - Kardinalitätsfunktion $f : Pot(\{a, b, c\}) \to \mathbb{N}$. $2 = f(\{b, c\})$
    $f = \{(\emptyset, 0), (\{a\}, 1), (\{b\}, 1), (\{c\}, 1), (\{a, b\}, 2), (\{a, c\}, 2), (\{b, c\}, 2), (\{a, b, c\}, 3)\}$ $\subseteq Pot(\{a, b, c\}) \times \mathbb{N}$
  - Sinusfunktion $\sin = \{(x, \sin(x)) \mid x \in \mathbb{R}\}$ $\subseteq \mathbb{R} \times \mathbb{R}$

Beispiele: Relationen, Funktionen



- Jede Funktion ist auch eine Relation.

- Aber es gibt natürlich Relationen, die keine Funktionen sind.

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

Wieso keine Funktion?

Betrachte $(r, s) \in \mathbb{R} \times \mathbb{R}$. Existiert für jedes $r \in \mathbb{R}$ genau ein $s \in \mathbb{R}$, so dass $(r, s) \in \sin^{-1}$? Nein!

1) Wähle $r = 0$: $(0,0) \in \sin^{-1}$, $(0, 2\pi) \in \sin^{-1}$, $(0, 4\pi) \in \sin^{-1}$, ...

2) Wähle $r = 2$: $(2, s) \notin \sin^{-1} \; \forall s \in \mathbb{R}$

Summen und Produkte (Notation)

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

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

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

- Beispiel:

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

- Schreibweise mit beliebigen Bedingungen:

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

$\boxed{(1,1),(1,2),(2,1),(3,1)}$

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

bzw. Aussagenlogik: $0 \hat{=}$ Wahrheitswert „falsch“, $1 \hat{=}$ Wahrheitswert „wahr“

Definition

- $\mathbb{B} := \{0,1\}$
- Konjunktion (UND-Verknüpfung) $\wedge : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$
  $0 \wedge 0 = 0, \quad 0 \wedge 1 = 0, \quad 1 \wedge 0 = 0, \quad 1 \wedge 1 = 1$
- Disjunktion (ODER-Verknüpfung) $\vee : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$
  $0 \vee 0 = 0, \quad 0 \vee 1 = 1, \quad 1 \vee 0 = 1, \quad 1 \vee 1 = 1$
- Negation $\neg : \mathbb{B} \to \mathbb{B}$
  $\neg 0 = 1, \quad \neg 1 = 0$
- 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.

$((\neg 0) \vee 1) \wedge (0 \wedge 1)) \hat{=} 0$

Ergebnis ist genau dann wahr, wenn beide Operanden wahr sind.

Ergebnis ist genau dann falsch, wenn beide Operanden falsch sind.

Entweder-Oder: $\oplus : \mathbb{B} \times \mathbb{B} \to \mathbb{B}$

$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0$

kein direkter Bestandteil der Bool. Algebra

$a \oplus b = ((\neg a \wedge b) \vee (a \wedge \neg b))$

später: Boolesche Variablen eingeführt

bzgl. lässt $\cdot$ sogar ganz weg

Konventionen

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

$$\neg 0 \cdot 1 + 0 = (((\neg 0) \cdot 1) + 0)$$

UNI FREIBURG

16

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

später: $(M, \wedge, \vee, \neg)$ nennt man Boolesche Algebra, wenn die folgenden Axiome gelten:

zunächst mal: Regeln der booleschen Algebra!

Axiome der booleschen Algebra

Kommutativität:	$x+y=y+x$	$\forall x,y \in \{0,1\}$	$\forall x,y \in M$
	$x \cdot y = y \cdot x$	$\forall x,y \in \{0,1\}$	"
Assoziativität:	$x+(y+z)=(x+y)+z$	"	"
	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	"	"
Absorption:	$x+(x \cdot y) = x$	$\forall x,y \in \{0,1\}$	
	$x \cdot (x+y) = x$	$\forall x,y \in \{0,1\}$	
Distributivität:	$\underline{x+(y \cdot z) = (x+y) \cdot (x+z)}$	$\forall x,y,z \in \{0,1\}$	
	$\underline{x \cdot (y+z) = (x \cdot y)+(x \cdot z)}$	"	
Komplement:	$x+(y \cdot \neg y) = x$	$\forall x,y \in \{0,1\}$	
	$x \cdot (y + \neg y) = x$	"	

Nachweis, dass $(\{0,1\}, \wedge, \vee, \neg)$ eine Boolesche Algebra ist, erfolgt dann durch Nachrechnen, ob die obigen Axiome gelten!

Bsp.: „Absorption": $\underline{x + xy} = x \quad \forall x, y \in \{0,1\}$

x	y	$x \cdot y$	$x + xy$
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	1

$\overset{!}{=}$

„Komplement": $x + (y \cdot \neg y) = x \quad \forall x, y \in \{0,1\}$

x	y	$\neg y$	$y \cdot \neg y$	$x + (y \cdot \neg y)$
0	0	1	0	0
0	1	0	0	0
1	0	1	0	1
1	1	0	0	1

$=$

- 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:	$\neg(\neg x) = x$	$\forall x \in \{0,1\} = \mathbb{B}$
Idempotenz:	$x + x = x \cdot x = x$	"
De-Morgan-Regel:	$\neg(x+y) = (\neg x)\cdot(\neg y)$	$\forall x,y \in \mathbb{B}$
	$\neg(x \cdot y) = (\neg x)+(\neg y)$	" "
Consensus-Regel:	$(x\cdot y)+((\neg x)\cdot z)$ $= (x\cdot y)+((\neg x)\cdot z)+(y\cdot z)$	$\forall x,y,z \in \mathbb{B}$
	$(x+y)\cdot((\neg x)+z)$ $= (x+y)\cdot((\neg x)+z)\cdot(y+z)$	

Beweis der Konsensusregel für <u>spezielle</u> Boolesche Algebra $(\{0,1\}, \wedge, \vee, \neg)$ (kein allgemeiner Beweis für beliebige Boolesche Algebren!):

z.z.: $\forall x,y,z \in \mathbb{B}$: $xy + \bar{x}z = xy + \bar{x}z + yz$

bzw.: „$xy + \bar{x}z = 1$" $\Longleftrightarrow$ „$xy + \bar{x}z + yz = 1$"

„$\Longrightarrow$": $xy + \bar{x}z = 1 \Longrightarrow \underbrace{xy + \bar{x}z}_{=1} + yz = 1 + yz = 1$

„$\Longleftarrow$": Voraus.: $xy + \bar{x}z + yz = 1$

Beh.: $xy + \bar{x}z = 1$

Fall 1: $yz = 0$

$$1 = xy + \bar{x}z + \underbrace{yz}_{=0} = xy + \bar{x}z + 0 = xy + \bar{x}z$$

Fall 2: $yz = 1 \Longrightarrow y = 1$ <u>und</u> $z = 1$

Fall 2.1: $x = 0$

$\Longrightarrow \bar{x}z = 1 \Longrightarrow xy + \bar{x}z = 1$

Fall 2.2: $x = 1$

$\Longrightarrow xy = 1 \Longrightarrow xy + \bar{x}z = 1$ ∎

Boolesche Funktion

Definition

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

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

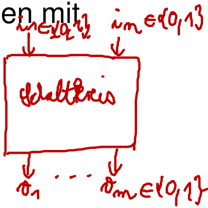
n-Tupel von $0,1$

$(i_1, \ldots, i_n) \in \mathbb{B}^n$

$\mapsto (o_1, \ldots, o_m) \in \mathbb{B}^m$

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

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



- 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)

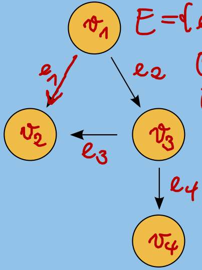
Gerichteter Graph

Definition

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

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

$V = \{v_1, v_2, v_3, v_4\}$
$E = \{e_1, e_2, e_3, e_4\}$



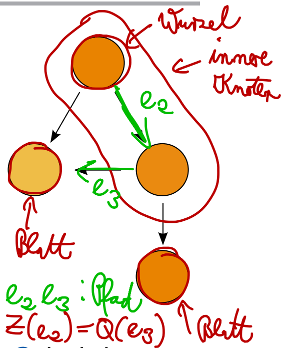
$Q(e_1) = v_1$
$Q(e_3) = v_3$
$Z(e_4) = v_4$

$indeg(v) = 3$

$outdeg(w) = 2$

Pfade in gerichteten Graphen

- Ein Knoten mit
  - $indeg(v) = 0$ heißt Wurzel.
  - $outdeg(v) = 0$ heißt Blatt.
  - $outdeg(v) > 0$ heißt innerer Knoten.



- Ein Pfad (der Länge k) in G ist eine Folge von k Kanten $e_1, e_2, \ldots, e_k$ $(k \geq 0)$ mit $Z(e_i) = Q(e_{i+1})$ für alle i $(k-1 \geq i \geq 1)$

$Q(e_1) \xrightarrow{e_1} Z(e_1) = Q(e_2) \xrightarrow{e_2} \bigcirc \xrightarrow{e_3} \ldots \xrightarrow{e_k} Z(e_k))$ (*)

- 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).

$Q(e) = Z(e)$

- Die Graph-Tiefe eines azyklischen Graphen ist definiert als die Länge des längsten Pfades in G.

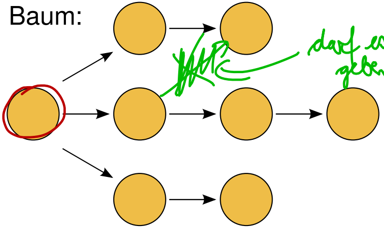
(*) $Q(e_1)$ heißt Quelle des Pfades, $Z(e_k)$ heißt Ziel des Pfades.

Definition

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

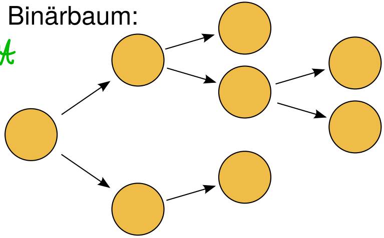
Beispiele:

Baum:



darf es nicht geben!

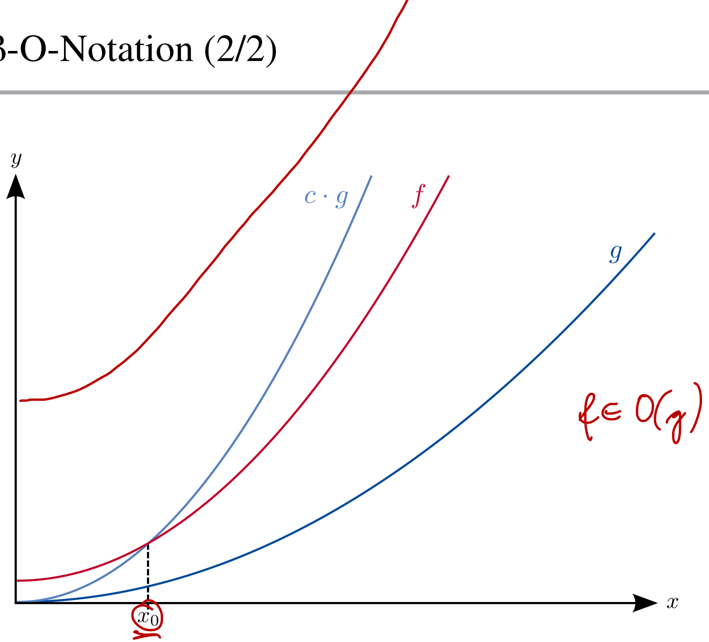
Binärbaum:



Groß-O-Notation (1/2)

- Seien $f, g : \mathbb{R}_0^+ \to \mathbb{R}_0^+$.
  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. „f wächst asymptotisch nicht stärker als g."
  - Beispiel: $5x + 2 \in O(x^2)$
    Beweis: Setze $c = 6, x_0 = 2$
    $$5x + 2 \underset{2<x}{<} 5x + x = 6x \underset{1 \leq x}{\leq} 6 \cdot x^2, \text{ für } x > 2.$$
- 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)



Beweistechniken

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

$A \to B$

$\neg B \to \neg A$

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.

$A \to C \ , \ C \to D \ , \ D \to B$

$A \Longrightarrow B$

Beispiel: Sukzessive Folgerungen

A ussagen:
gegeben
Voraussetzungen

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

Behauptung

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 $g(x) \leq c_g \cdot h(x)$.

   $x > max\{x_{0f}, x_{0g}\}$
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 $f(x) \in O(h(x))$

Indirekter Beweis 1/2

Widerspruch Beweis

Es soll Aussage $\boxed{S}$ 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

$S = A \to B = \neg A \vee B \Rightarrow$

$\bar S = \overline{(\bar A \vee B)} = \bar{\bar A} \wedge \bar B = A \wedge \bar B$

- Betrachte den Spezialfall $S = \boxed{A} \Rightarrow B$.
  - 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.

    $\neg B \to \ldots \to \ldots \to \neg A$
  - 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.

    $\neg B \to \neg A = \bar B \to \bar A = \bar{\bar B} \vee \bar A = B \vee \bar A = \bar A \vee B = A \to B$
  - 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: $\neg S' = \boxed{A \wedge Ax \wedge \neg B}$ gilt.

$S' = \neg(A \wedge Ax) \vee B$

$\neg S' = \neg(\neg(A \wedge Ax) \vee B)$

$\neg S' = \neg\neg(A \wedge Ax) \wedge \neg B$

$\neg S' = (A \wedge Ax) \wedge \neg B$

31

Beispiel: Indirekter Beweis

x_0 wählen so dass irgendwann f.a. $x > x_0$ $x^2 \leq x$ gilt (wenn $x^2 \in O(x)$)

$c = 2$ $\quad x^2 < c \cdot x$

$x_0 = 1$ $\quad 1^2 < 2 \cdot 1$ ✓

$x_0 = 3$ $\quad 3^2 < 2 \cdot 3$

$9 < 6$ ✗

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

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:

$$\boxed{x^2 \leq c \cdot x} \tag{1}$$

- 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.

$A(0)$

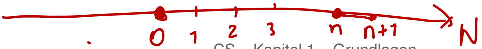
- Zuerst wird die Aussage für den Basisfall $n = 0$ beweisen (manchmal auch $n = 1$ oder höher).

IV $A(n)$

$A(n) \to A(n+1)$

- 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.



Vollständige Induktion: Beispiel (1/2)

zu zeigen

- **Behauptung:**

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

- **Induktionsanfang:**

  Zeige die Behauptung für $n = 0$.

  $n = 1$

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

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

UNI FREIBURG

Vollständige Induktion: Beispiel (2/2)

e n ℕ

- **Induktionsvoraussetzung** (IV):
  Nehme an, die Behauptung gilt für *ein* $n \in \mathbb{N}$.
  Also: Es gibt ein $n \in \mathbb{N}$ für das gilt: $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$

A(n) gilt

- **Induktionsschritt:**
  Zeige die Behauptung für $n+1$.

$$\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} \overset{\text{IV}}{=} \frac{n}{n+1} + \frac{1}{(n+1)(n+2)}$$

A(n) → A(n+1)

$$= \frac{n(n+2)+1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{(n+1)}{(n+2)} = \frac{(n+1)}{(n+1)+1} \quad \square$$

$$\sum_{k=1}^{n+1} x = \sum_{k=1}^{n} x + (n+1)$$