h_da – Hochschule Darmstadt
FB Informatik
Winter 2017/18

Logik (nicht nur) für Informatiker

Dr. Bernd Baumgarten

baumgarten_bernd@web.de
http://bernd-baumgarten.de/ → Folien, Skript, PVL, Aufgaben, Lösungen 

Zur Lernmethodik:

 : Schubladen-Bild, Kaffee-Lemma, Sportschau-Gleichnis

Arbeitsmoral-Mantra:

ISBN 978-3936973204

Aufschieb-Problem: Später ist meist noch weniger Zeit.

Was ist und was nützt Logik?

Was ist und was nützt Logik?

Logik ist die Wissenschaft von den

- Regeln,
- Methoden und
- Grenzen

des Schlussfolgerns.

Anwendung: beim ...

- Argumentieren,
- Folgern,
- Beweisen,
- Widerlegen,

- Berechnen,
- Entwerfen,
- Prüfen.

Anwendungs**weisen**:

- produktiv oder
- nachprüfend

Übersicht über die Vorlesung

Themen

- **Mathematische Werkzeuge**
- **Aussagenlogik (AL)**
- **andere Logiken (hier nur auf AL-Basis), teilweise selbstständig zu erarbeiten**
- **Prädikatenlogik (PL)**

Aspekte

- **Grundlagen,**
- **Algorithmen,**
- **Anwendungen.**

Mathematische Werkzeuge

- **Mengen, Relationen, Funktionen**
- **Induktion und Rekursion**
- **Sprachen und Grammatiken**
- **Graphen und Bäume**

Metasprachliche Symbole

(Objekt-)Sprache: Hallo, wie geht's? $A \rightarrow \neg A$

Metasprache: „Hallo“ hat 6 Buchstaben. $A \rightarrow \neg A$ ist immer falsch

Die Vermischung von Meta- und Objektsprache ist – zusammen mit zyklischen Definitionen – die Hauptquelle von **Paradoxien** (z.B. „*Neunzehn Buchstaben* sind zwanzig Buchstaben.“ – „Dieser Satz ist gelogen.“)

$\Leftrightarrow$ *genau dann, wenn*

Die Sonne geht unter. $\Leftrightarrow$ Die Nacht beginnt.

$\Rightarrow$ *wenn, dann* / *daraus folgt*

Die Erde ist eine Scheibe. $\Rightarrow$ Ich fresse einen Besen.

$:\Leftrightarrow$ *ist dadurch definiert, dass* / *definitionsgemäß genau dann, wenn*

Die Spielerin hat ihr Skatspiel gewonnen.
$:\Leftrightarrow$ Sie hat mehr als 60 Punkte in ihren Stichen erzielt.

$:=$ *ist definiert als* $\max(a,b) := $ wenn $a > b$ dann a, sonst b.

Mengen (1)

Eine **Menge** ist eine „*Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die ‚Elemente' von M genannt werden) zu einem Ganzen*."

Georg **Cantor** 1895

$a \in A :\Leftrightarrow$ a ist **Element** von A

$a \notin A :\Leftrightarrow$ a ist kein Element von A

$\{a, b, c\} :=$ Menge mit den Elementen a, b und c ($= \{c, a, b\} = \{a, a, b, c\}$)

$\{\}, \varnothing :=$ leere Menge

$\{a_1, a_2, a_3, ...\} :=$ Menge mit den Elementen a_1, a_2 und a_3 „usw."

$\{a, b, c, ..., z\} :=$ Menge mit den Elementen a, b und c „usw. bis" z

$\{x \mid P(x)\} :=$ Menge aller Objekte mit der Eigenschaft P
(Existenz durch **Komprehensionsaxiom** garantiert)

Mengen (2)

Wichtige Mengen:

$\mathbb{N}$ **natürliche Zahlen ohne 0** $= \{1, 2, 3, ...\}$

$\mathbb{N}_0$ **natürliche Zahlen mit 0** $= \{0, 1, 2, ...\}$

Achtung: Manche Autoren (z.B. DIN 5473) verwenden $\mathbb{N} = \{0, 1, 2, ...\}$!

$\mathbb{R}$ **reelle Zahlen**

$\mathbb{Z}$ **ganze Zahlen**

$\mathbb{Q}$ **rationale Zahlen**

$A = B \Leftrightarrow$ Für alle x gilt: $x \in A \Leftrightarrow x \in B$. **Extensionalitätsaxiom**

$\Rightarrow$ Es gibt nur eine leere Menge.

$A \subseteq B :\Leftrightarrow$ Für alle $x \in A$ gilt $x \in B$. **Teilmenge**

$\mathbf{P}(A) := \{M \mid M \subseteq A\}$ (auch 2^A) **Potenzmenge**

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

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

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

Mengen (3)

$A_1 \times ... \times A_n$ bzw. $\prod_{i=1}^{n} A_i :=$

$$\{(a_1, ..., a_n) \mid a_i \in A_i \text{ für } i = 1,...,n\}$$ (**kartesisches**) **Produkt**

U mit: Für alle x gilt $x \in U$. **Allmenge**

$\overline{A} := U \setminus A$ **Komplement**

Ü1

Die Naive Mengenlehre ist **widersprüchlich** (s.u.) – aber ganz **brauchbar**.

Komprehensionsaxiom auf $P(x) :\Leftrightarrow x \notin x$ anwenden:

Sei $N := \{x \mid P(x)\}$. Dann ist $N \in N \overset{\text{Def. } N}{\Leftrightarrow} P(N) \overset{\text{Def. } P}{\Leftrightarrow} N \notin N$. (Bertrand Russell 1903)

Trotzdem: „Aus dem Paradies, das uns Cantor geschaffen,
soll uns niemand vertreiben können.“ David Hilbert 1926

Und wie? → Axiomatische Mengenlehre (zumindest theoretisch)

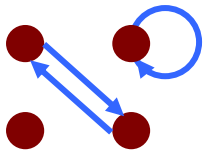
Relationen (1)

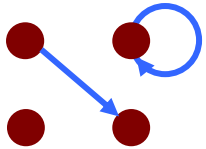
$R \subseteq A_1 \times ... \times A_n$ (***n*-stellige**) **Relation** R **zwischen** Mengen $A_1, ..., A_n$, $n \in \mathbb{N}_0$

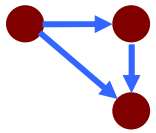
$R(a_1, ..., a_n) :\Leftrightarrow$ (*Schreibweise für …*) $(a_1, ..., a_n) \in R$

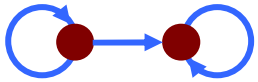
$aRb :\Leftrightarrow$ (*Schreibweise für …*) $R(a,b)$

Ein $R \subseteq A \times A$, also eine zweistellige Relation R **auf** einer Menge A ist …

symmetrisch  $:\Leftrightarrow$ für alle $a,b \in A$ gilt: $aRb \Rightarrow bRa$;

antisymmetrisch  $:\Leftrightarrow$ für alle $a,b \in A$ gilt: aRb und $bRa \Rightarrow a=b$;

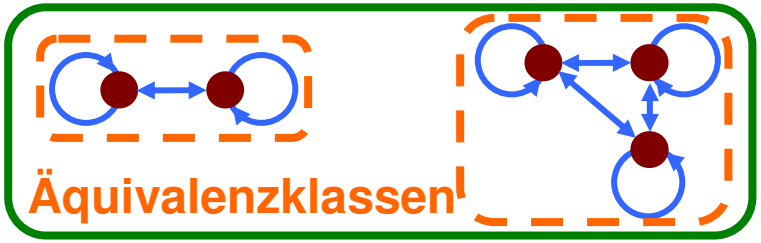
transitiv  $:\Leftrightarrow$ für alle $a,b,c \in A$ gilt: (aRb und bRc) $\Rightarrow aRc$;

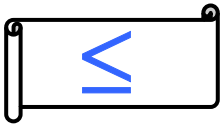
reflexiv  $:\Leftrightarrow$ für alle $a \in A$ gilt: aRa.

Relationen (2)

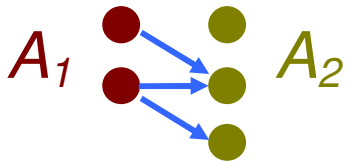
Eine zweistellige Relation R auf einer Menge ist …

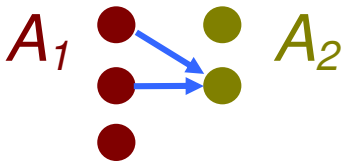
Äquivalenzrelation $:\Leftrightarrow$ R symmetrisch, transitiv und reflexiv
(entspricht **Partition**)



Halbordnung  $:\Leftrightarrow R$ antisymmetrisch, transitiv und reflexiv

Sei $R \subseteq A_1 \times A_2$ zweistellige Relation ...

R **linkstotal**  $:\Leftrightarrow$ für jedes $a \in A_1$ existiert ein $b \in A_2$ mit aRb

R **rechtseindeutig**  $:\Leftrightarrow$ für alle $a \in A_1$, $b_1, b_2 \in A_2$ gilt:
aRb_1 und $aRb_2 \Rightarrow b_1 = b_2$

Funktionen (1)

f (**totale**) **Funktion** oder **Abbildung von** A **in** B, kurz

$f : A \to B :\Leftrightarrow$ $f \subseteq A \times B$, f linkstotal und rechtseindeutig

$B^A :=$ Menge aller Abbildungen von A in B

(Eine **partielle** Funktion / Abbildung ist ... nicht unbedingt linkstotal.) ⇦Ü2

Totale Funktionen sind spezielle partielle Funktionen!

$\text{Def}_f := \{a \in A \mid \text{es ex. } b \in B : (a,b) \in f\}$ **Definitionsbereich** partielles $f : A \to B$

$f : A \to B$ total $\Rightarrow \text{Def}_f = A.$)

$f[M], M \subseteq A := \{f(x) \mid x \in M\} = \{b \in B \mid \text{es ex. } a \in A : (a,b) \in f\}$ **Bildmenge**

Ü3⇨

Funktionsbeschreibung (total), Beispiel:

$$f : \begin{cases} \mathbb{Z} & \to & \mathbb{N}_0 \\ x & \mapsto & x^2 \end{cases}$$

Funktionen (2)

Für $f : A \to B$, $g : B \to C$ ist ...

$g \circ f : A \to C$:= die Abbildung mit $g \circ f(a) := g(f(a))$, die

Hintereinanderausführung von f und g

f **injektiv** :$\Leftrightarrow$ f **linkseindeutig**, für alle $a, b \in A$ gilt: $f(a) = f(b) \Rightarrow a = b$,

f **surjektiv** :$\Leftrightarrow$

f **rechtstotal**, bzw. $f[A] = B$, für alle $b \in B$ existiert ein $a \in A$ mit $f(a) = b$

f **bijektiv** :$\Leftrightarrow$ f sowohl injektiv als auch surjektiv

Ü4

$$id_A : \begin{cases} A & \to & A \\ x & \mapsto & x \end{cases}$$

identische Abbildung

$f^{-1} : B \to A$:= **Umkehrabbildung** zu bijektivem $f : A \to B$

$f^{-1}(b) = a :\Leftrightarrow f(a) = b$, und $\Rightarrow f^{-1} \circ f = id_A, f \circ f^{-1} = id_B$

Sprachen

Alphabet: $A = \{a_1, \ldots, a_n\}$, auch unendlich möglich (z.B. zweistufige Sprachen)

Zeichen: $a_i \in A$ (auch „**Symbol**“)

Wort: $w \in A^*, \quad A^* = \{(z_1, \ldots, z_k) \mid k \in \mathbb{N}_0, \forall 1 \le i \le k : z_i \in A\}$,
meist ohne Komma und Klammern geschrieben als $z_1 \ldots z_k$

Sprache (über A): eine Menge von Wörtern, $L \subseteq A^*$

leeres Wort: ε $(=(z_1, \ldots, z_k)$ mit $k = 0)$ ■

Verkettung: $u \circ v$:= „uv“ (hintereinandergeschrieben)

Wiederholung: a^k := $a \ldots a$ (k-mal) ■

Kleene-Stern: * “null-■, ein- oder mehrmals”

Spezialfälle

L Sprache $L^* := \{ w_1 \ldots w_n \mid n \in \mathbb{N}_0, \ \forall 1 \le i \le n: w_i \in L \}$ ■

w Wort $w^* := \{w\}^*$

a Zeichen $a^* := \{a\}^* \ (= \{a^k \mid k = 0,1,...\})$ ■

■) $z_1 \ldots z_0 = a^0 = w_1 \ldots w_0 = \varepsilon$ (weil **kein** z_i bzw. a bzw. w_i darin steht)

Induktion (1)

Induktion dient ...

- zur Definition
- zum Beweis von Eigenschaften *P* aller Elemente

} gewisser, meist unendlicher, Mengen

Definitionsbeispiel:

Neandertaler-Zahlen NZ

1. | ist eine NZ.
2. Ist *n* eine NZ, dann auch *n*| (**Nachfolger** von *n, succ*(*n*), "$n+1$").
3. Jede NZ entsteht durch endlich häufige Anwendung der Regeln (1) und (2).

Induktion (2)

Neandertaler-Zahlen NZ ...

Heutige Schreibweise | = 1, || = 2, ..., ||||||||| = 10, usw.

→ **natürliche Zahlen,** $\mathbb{N}$

Ferner: kein Strich = 0; 1 ist Nachfolger von 0; $\mathbb{N}_0$

Wozu braucht man Regel (3)?

- Auch { |, O }* erfüllt die Regeln (1)+(2) !
  Wir wollen aber nur nach Regeln (1) und (2) Gebildetes zulassen!
- Unendlichfache Anwendung der Regel (2) → |||... (unendliche Folge)?
  Wir wollen aber nur endlich häufige Anwendung!

Regel (3) gehört stillschweigend zu „**induktiv**“.

Induktive Mengendefinition

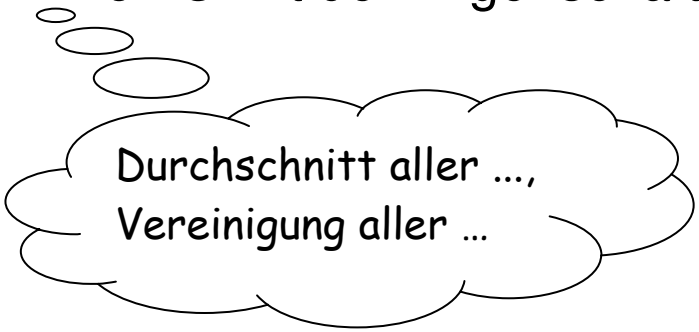
Induktive Definition bestimmter **Teilmengen einer (Grund-)Menge *U***

Seien $M_0 \subseteq U$ Basis- bzw. Ausgangsmenge,

$f_k : U^{m_k} \to U$ ($k = 1,2, ...,$ evtl. partiell) Induktionsschritte.

Dann existiert eine kleinste Teilmenge M von U mit den Eigenschaften

1. $M_0 \subseteq M$
2. $f_k[M^{m_k}] \subseteq M$



Beispiele

Arithmetische Terme, Minibeispiel:

(1) a,b sind **(ab+·)-Terme**.

(2) x,y (ab+·)-Terme ⇒ (x+y) und (x·y) (ab+·)-Terme – z.B. ((a+(b+a))·b)

Neandertalerzahlen als Strichlisten:

(1) | ist natürliche Zahl (2) *n* natürliche Zahl ⇒ *n*| ist natürliche Zahl

– Was sind hier jeweils die U, M_0, f_k? –

Ü5

Induktiver Beweis

Induktionsprinzip (für induktive Beweise) auf induktiv definiertem *M*:

Gilt Eigenschaft *P*

(1) „**auf** M_0“ (d.h. für alle Elemente von M_0) und

(2) wenn auf $\{x_1, ..., x_{m_k}\}$, dann auch für $f_k(x_1, ..., x_{m_k})$ (sofern def.),

so gilt *P* **auf ganz *M***.

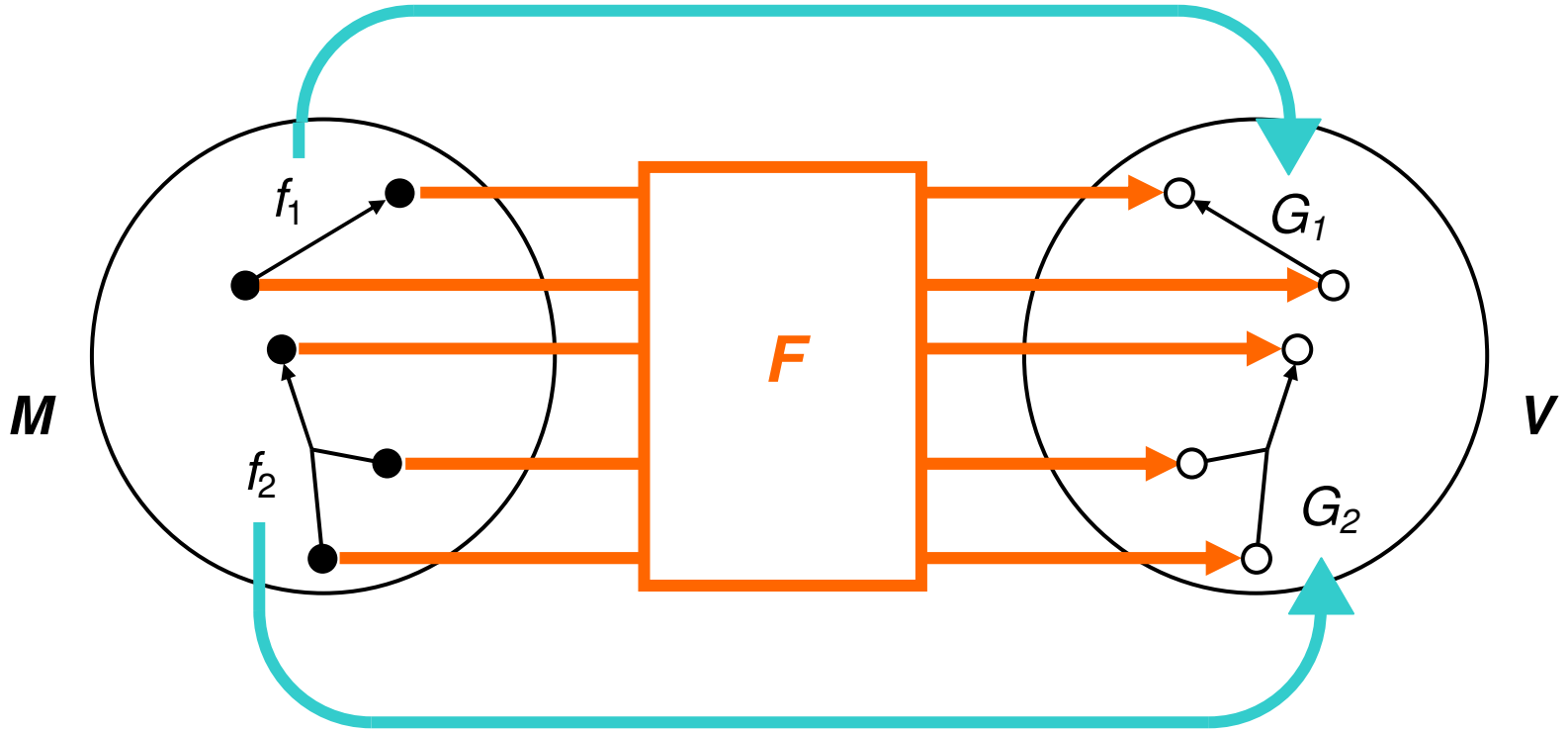
… weil jedes Element

- entweder „von vornherein“ die Eigenschaft *P* hat (da es aus M_0 ist)
- oder von seinen „Bausteinen“ aus der vorigen „Generation“ bei seiner Entstehung die Eigenschaft *P* „erbt“.

Ü6ad

Rekursive Definition von Funktionen – Idee

... auf induktiv definiertem *M*:



Man baut quasi das **Bild parallel mit den Aufbauschritten des Urbilds** auf**.**

Rekursive Definition von Funktionen (1)

... auf induktiv definiertem M:

Seien

- ein Wertebereich V und
- für jede Erweiterungsregel k ein $G_k : V^{m_k} \to V$

gegeben.

Dann definiert man durch

- $F(x) \in V$ für alle $x \in M_0$ festlegen. – **Basisfälle**
- $F(f_k(x_1, ..., x_{m_k})) := G_k(F(x_1), ..., F(x_{m_k}))$ – **Rekursion**

(**rekursiv**) eine **Abbildung** $F : M \to V$,

Geht das immer gut?

Rekursive Definition von Funktionen (2)

... auf induktiv definiertem M:

Seien

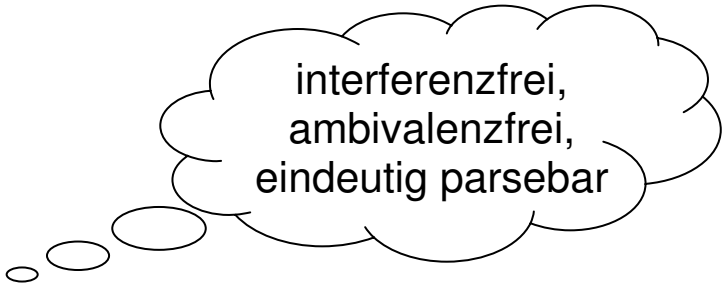
- ein Wertebereich V und
- für jede Erweiterungsregel k ein $G_k : V^{m_k} \to V$

gegeben.

Dann definiert man durch

- $F(x) \in V$ für alle $x \in M_0$ festlegen. – **Basisfälle**
- $F(f_k(x_1, ..., x_{m_k})) := G_k(F(x_1), ..., F(x_{m_k}))$ – **Rekursion**

(**rekursiv**) eine **Abbildung** $F : M \to V$,



Aber das geht nur dann sicher gut, wenn ...

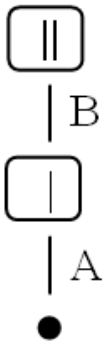
- jedes Element von M eine „**eindeutige Entstehungsgeschichte**“ hat,
- **oder** ein Beweis der **Wohldefiniertheit** gelingt.

Entstehungsgeschichten

Eindeutige Entstehungsgeschichte – Beispiel ☺

Neandertaler-Zahlen NZ

(A) | ist NZ.
(B) *n* ist NZ ⇒ *n*| ist NZ-Z.

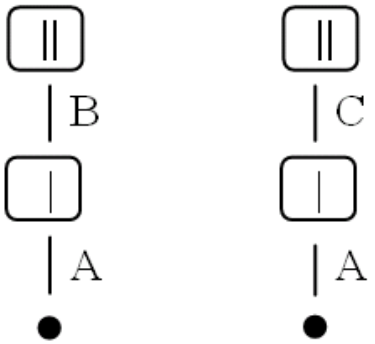


Eindeutige Entstehungsgeschichte – **Gegenbeispiel ☹**

Australopithecus-Zahlen:

(A) | ist APZ.
(B) *n* APZ ⇒ *n*| APZ.
(C) *n* APZ ⇒ |*n* APZ.

|| hat 2 Entstehungsgeschichten:

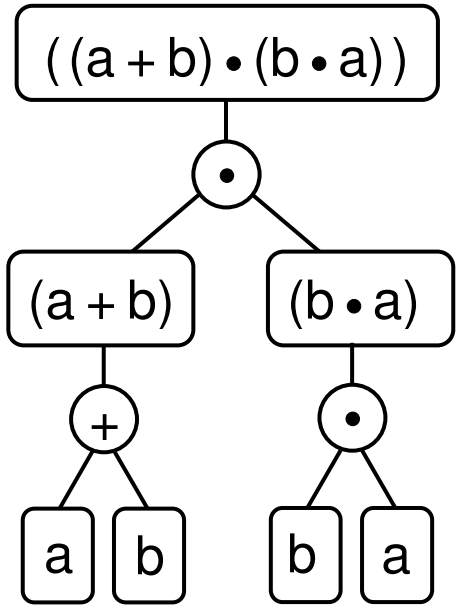


Entstehungsgeschichten sind Bäume

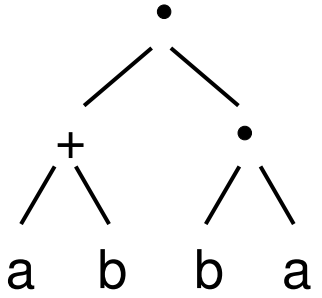
z.B. (ab+ ·)-Terme, gebildet aus

- 2 Basisfällen: ‚a' und ‚b'
- 2 Erweiterungsregeln: ‚+'-Regel und ‚•'-Regel

Beispiel:



oder kurz:



Rekursive Definition von Funktionen (3)

Wie kann rekursive Abbildungsdefinition bei Australopithecus-Zahlen schiefgehen?

Gegenbeispiel zur Wohldefiniertheit:
Links(|) := 0;
Links(*n*|) := *Links*(*n*);
Links(|*n*) := *Links*(*n*)+1;
nicht wohldefiniert, d.h. führt zu widersprüchlichen Zuweisungen:

0 = *Links*(|/) = 1 ??

keine eindeutige Entstehungsgeschichte …
… aber wohldefiniert auf Australopithecus-Zahlen

LorR(|) := 0;
LorR(*n*|) := *LorR*(*n*) +1;
LorR(|*n*) := *LorR*(*n*)+1;

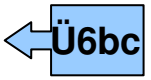
Übung: Beweis der Wohldefiniertheit

Rekursive Definition von Eigenschaften

Eigenschaft = Spezialfall von Abbildung, nämlich → {W,F} !

Beispiel: Eigenschaft *Gerade* auf Neandertalerzahlen

Gerade(|)	:= F
Gerade(*n*|)	:= Wenn *Gerade*(*n*)=W, dann F, sonst W
	= ¬*Gerade*(*n*)



Grammatiken

Eine **Grammatik** ist ein Quadrupel $G = (N, T, S, R)$ mit

- einem Alphabet N von **Nichtterminalzeichen**,
- einem Alphabet T von **Terminalzeichen**, $N \cap T = \varnothing$,
- einen **Startzeichen** $S \in N$,
- einer endlichen Menge $R \subseteq (N \cup T)^* \times (N \cup T)^*$ von **Regeln**.

Schreibweisen $(v,w) \in R$: $v \to w$

$(v,w),(v,w') \in R$: $v \to w \mid w'$.

G **definiert** („erzeugt“) eine **Sprache von Terminalzeichenwörtern**,
$L(G) := H(G) \cap T^*$,
wobei die Hilfssprache $H(G) \subseteq (N \cup T)^*$ **induktiv** gegeben ist durch

- $S \in H(G)$
- $r\ v\ s \in H(G) \wedge v \to w \Rightarrow r\ w\ s \in H(G)$.

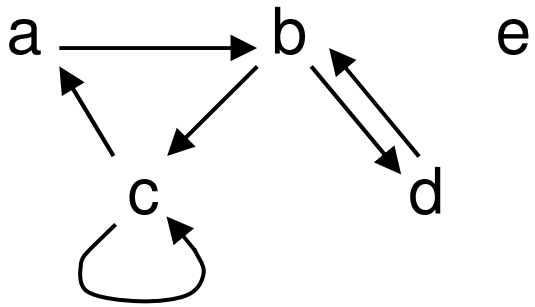
Ü7

Graphen (1)

Gerichteter Graph :=

zweistellige Relation über einer Menge

(i.a. graphisch dargestellt).



entspricht {(a,b), (b,c), (c,a), (b,d), (c,c), (d,b)}
über {a,b,c,d,e}.

a, b, ..., e sind **Knoten** (mit angeben! Sonst e unbekannt.)
(a,b), (b,c), usw. sind **Kanten**.

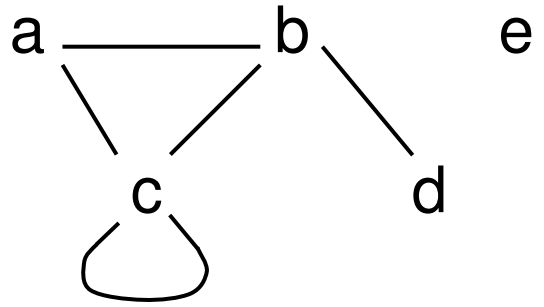
Graphen (2)

Ungerichteter Graph

1. Definitionsmöglichkeit: Paar-&Single(!)mengenmenge

2. Definitionsmöglichkeit: symmetrische Relation

über einer Menge (mit angeben! Sonst e unklar.)



entspricht { {a,b}, {b,c}, {c,a}, {c}, {b,d} }

bzw. { (a,b), (b,a), (a,c), (c,a), (b,c), (c,b), (b,d), (d,b), (c,c) } .

über {a,b,c,d,e}

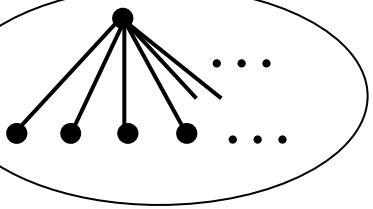
Bäume

Baum zahlreiche Definitionsmöglichkeiten

Kinder haben Reihenfolge?

unterschiedl. Bäume

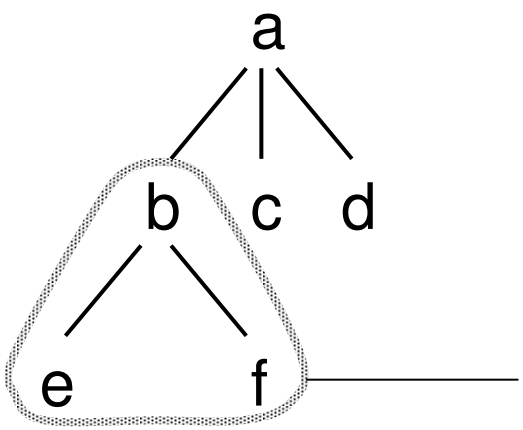
geordnet / **ungeordnet**
endlich / **unendlich viele Knoten**
endlich verzweigt / **nicht**



untersch. Ansätze*

als spezielle ungerichtete/gerichtete Graphen, spezielle Halbordnungen usw.

*) vgl. Äquiv.-Relation ~ Partition



Kinderzahl

a ist die **Wurzel**

b, c, d sind **Kinder** von a (**Grad** von a ist 3)

c, d, e, f sind die **Blätter**

a – b – e ist ein **Zweig** (Pfad Wurzel–Blatt)

Ast(b)

Ü8

Kőnigs Lemma

Welche dieser 3 Bäume mit **unendlich vielen Knoten** sind als **Gegenbeispiel** für welche Hypothese geeignet?

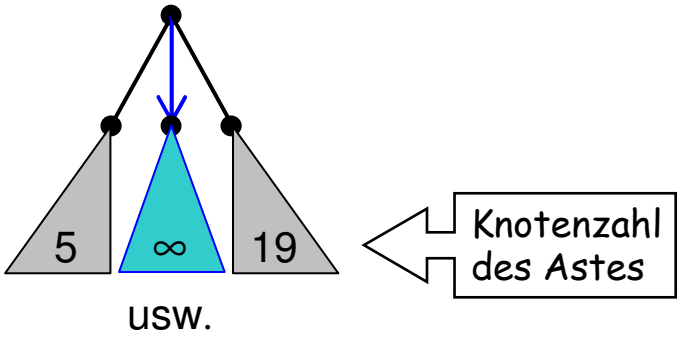
- Pfade sind immer endlich lang.
- Jeder Baum mit unendlich vielen Knoten hat einen unendlichen Pfad.
- Jeder Baum mit unendlich vielen Knoten hat endliche Pfade „beliebiger Länge."
- Sind in einem Baum alle Pfade endlich so ex. eine maximale Pfadlänge.
- Sind in einem Baum alle Pfade endlich so hat er endlich viele Knoten.
- Sind in einem Baum die Grade beschränkt, hat er endlich viel Knoten.

Jeder Baum mit **unendlich vielen Knoten allesamt endlichen Grades** besitzt einen **unendlichen Pfad**.

Dénes Kőnig (1936)

→ Gilt auch wenn die Grade unbeschränkt sind!

Beweisidee



Anwendungen von Königs Lemma

A. Ein Solitaire-Spiel

Voraussetzung:
Du bist unsterblich.

Material:
Du hast einen Kartenvorrat, der zu jeder natürlichen Zahl n beliebig viele Karten enthält, auf denen „n“ steht (bzw. sie sind grenzenlos lieferbar).

Spielablauf:
1. Nimm **eine** Karte „n“ nach Wunsch aus dem Vorrat.
2. Wiederhole, solange möglich:
   Lege **eine** Deiner Karten, „**m**“, ab und ersetze sie aus dem Vorrat durch **beliebig** aber **endlich viele** Karten mit (evtl. unterschiedlichen) „**k**“, **k<m**.

Ziel:
Spiele unendlich lange (d.h. unendlich oft Spielzug 2)!

Geht das? **König's Lemma** ⇒ **nein!**

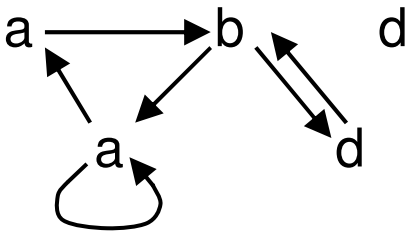
B. Anwendung in der Logik

Kompaktheitssätze (→ später)

Beschriftete Graphen und Bäume (1)

In gewöhnlichen Graphen und Bäumen gibt es jeden Knotennamen nur einmal, der Name **identifiziert** den Knoten.

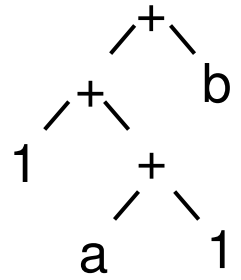
In **knotenbeschrifteten** Graphen und Bäumen sieht man nur die Knoten**anschriften**, die sich auch wiederholen dürfen.
Die Namen werden meist ignoriert, so wie hier ⇨



Mathematisch: + **Abbildung** Knotenmenge → Anschriftenmenge

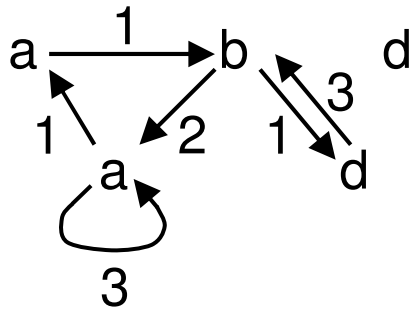
Anwendung: **Syntaxbäume** (geordnet) von Termen
Beispiel: ((1+(a+1))+b)

(vgl. Entstehungsgeschichten bei Induktion)



Beschriftete Graphen und Bäume (2)

Es gibt auch **kantenbeschriftete** sowie **gleichzeitig** knoten- und kantenbeschriftete Graphen und Bäume.



Mathematisch: + **Abbildung** Kantenmenge → Anschriftenmenge

Spezialfall: **Automaten (deterministisch/nicht-deterministisch)**

Mathematisch: kantenbeschrifteter Graph
+ spezielle Eigenschaft der Kantenbeschriftung (falls determ.)
+ ausgezeichnete(r) Anfangsknoten
+ ausgezeichnete Menge akzeptierender Knoten
→ *Theoretische Informatik: Anwendung auf formale Sprachen*