Hochschule Darmstadt, FB Informatik, Wintersemester 2017/18

Logik

baumgarten_bernd@web.de
http://bernd-baumgarten.de/

Was ist und wozu nützt Logik?

Logik ist die Wissenschaft von den

- Regeln,
- Methoden und
- Grenzen

des Schlussfolgerns.

Anwendung:

geisteswissenschaftlich:

- argumentieren,
- folgern,
- beweisen,
- widerlegen.

technisch:

- berechnen,
- entwerfen,
- prüfen.

Anwendungsweisen:

- produktiv oder
- nachprüfend.

Schwerpunkte der Vorlesung

Themenbereiche	im Skript ab …
• Mathematische Werkzeuge	Seite 1
• Aussagenlogik	Seite 5
• Modallogiken	Seite 22
• Prädikatenlogik	Seite 31

Aspekte

- Grundlagen,
- Algorithmen,
- Anwendungen.

Metasprachliche Symbole

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

Metasprache: „Hallo" hat 6 Buchstaben.
$A \to \neg A$ 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 / deswegen*
Die Erde ist eine Scheibe. $\Rightarrow$ Ich fresse einen Besen.

$:\Leftrightarrow$ *ist dadurch definiert, dass / gilt 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

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

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

$\{a, b, c, \ldots, z\} :=$ 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)

Wichtige Mengen:

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

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

Achtung: Manche Autoren verwenden $\mathbb{N} = \{0, 1, 2, \ldots\}$!

$\mathbb{R}$ **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**

$\mathsf{P}(A) := \{M \mid M \subseteq A\}$ (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**

$\prod_{i=1}^{n} A_i := \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } i = 1,\ldots,n\}$ bzw.
$A_1 \times \ldots \times A_n$ **(kartesisches) Produkt**

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

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

Ein Paradoxon (innerer Widerspruch) der **Naiven Mengenlehre,** entdeckt von Bertrand Russell 1903): Komprehensionsaxiom auf $P(x) :\Leftrightarrow x \notin x$ anwenden. Sei $N := \{x \mid P(x)\}$. Dann ist $N \in N \Leftrightarrow P(N) \Leftrightarrow N \notin N$.

Aber: *Aus dem Paradies, das uns Cantor geschaffen, soll uns niemand vertreiben können.* (David Hilbert 1926)

Wie daran festhalten? → **Axiomatische Mengenlehre**
oder praktisch meist: „vorsichtige Verwendung".

Relationen

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

$R(a_1, \ldots, a_n)$ Schreibweise für $(a_1, \ldots, a_n) \in R$

aRb Schreibweise für $R(a,b)$

Ein $R \subseteq A \times A$, (zweistellige Relation **auf** A) ist ...

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

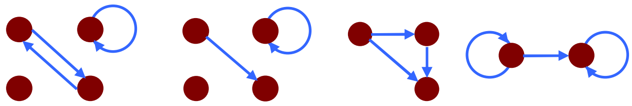
antisymmetrisch
:⇔ für alle $a,b \in A$ gilt: aRb und $bRa \Rightarrow a{=}b$;

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

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

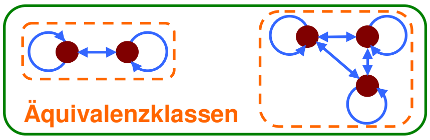
Beispiele

symmetrisch antisymm. transitiv reflexiv



Äquivalenzrelation
:⇔ R symmetrisch, transitiv und reflexiv

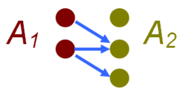
Jeder Äquivalenzrelation entspricht eine **Partition**:



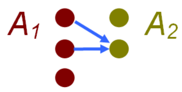
R **Halbordnung** :⇔ antisymmetrisch, transitiv und reflexiv, z.B. ≤ auf den erwähnten Zahlenbereichen.

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

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



R **rechtseindeutig** :⇔ für alle $a \in A_1$, $b_1, b_2 \in A_2$ gilt: $aR\,b_1$ und $aR\,b_2 \Rightarrow b_1 = b_2$



Funktionen

f ist (**totale**) **Funktion** oder **Abbildung** von A in B, kurz $f: A \to B$, :⇔ $f \subseteq A \times B$, linkstotal und rechtseindeut.

$B^A :=$ Menge aller Abbildungen $f: A \to B$

$f: A \to B$ ist **partielle** Funktion oder Abbildung :⇔
$f \subseteq A \times B$, rechtseindeutig, nicht unbedingt linkstotal.

Totale Funktionen sind <u>spezielle partielle</u> Funktionen!

$\mathrm{Def}_f := \{a \in A \mid$ es ex. $b \in B : (a,b) \in f\}$ ist der **Definitionsbereich** und

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

die **Bildmenge** einer partiellen Funktion $f: A \to B$.

Ist f totale Funktionen, gilt $\mathrm{Def}_f = A$.

Beispiel einer **Funktionsbeschreibung**: $f: \begin{cases} \mathbb{Z} \to \mathbb{N}_0 \\ x \mapsto x^2 \end{cases}$

Für $f: A \to B$ und $g: B \to C$ ist $g \circ f: A \to C$ mit $g \circ f(a) := g(f(a))$ deren **Hintereinanderausführung**.

f **injektiv** :⇔ f **linkseindeutig**
d.h. für alle $a,b \in A$ gilt: $f(a) = f(b) \Rightarrow a = b$,

f **surjektiv** :⇔ f **rechtstotal**
d.h. $f[A] = B$, für alle $b \in B$ ex. ein $a \in A$ mit $f(a) = b$

f **bijektiv** :⇔ f sowohl injektiv als auch surjektiv

$id_A: \begin{cases} A \to A \\ x \mapsto x \end{cases}$ **identische Abbildung**

$f^{-1}: B \to A$:= **Umkehrabbildung** zu bijektivem $f: A \to B$, d.h. $f^{-1}(b) = a$:⇔ $f(a) = b$

$\Rightarrow f^{-1} \circ f = id_A$, $f \circ f^{-1} = id_B$

Sprachen

Alphabet: $A = \{a_1, \ldots, a_n\}$

auch unendliches A möglich (z.B. zweistufige Sprachen)

Zeichen (auch **Symbol**) $a_i \in A$

Wort $w \in A^*$,

$A^* := \{(z_1, \ldots, z_k) \mid k \in \mathbb{N}_0, \forall 1 \le i \le k : z_i \in A\}$,

meist ohne Komma/Klammer geschrieben als $z_1 \ldots z_k$

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

leeres Wort: $\varepsilon = (z_1, \ldots, z_k)$ mit $k = 0$, also ( )

Verkettung: $u \circ v$:= u und v hintereinander o. Lücke

Wiederholung: $a^k := a \ldots a$ (k-mal) [1]

Kleene-Stern * "null[1]-, ein- oder mehrmals"

Spezialfälle

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

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

a Zeichen $a^* := \{a\}^*$ $(= \{a^k \mid k \in \mathbb{N}_0\}$ [1])

[1]) $z_1 z_2 \ldots z_0 = a^0 = w_1 w_2 \ldots w_0 = \varepsilon$ (weil kein z_i bzw. a bzw. w_i darin).

Induktion und Rekursion

Induktion dient ...

- zur Definition
- zum Beweis von Eigenschaften P aller Elemente … gewisser unendlicher Mengen

Induktive Definitionen – Beispiel

Neandertaler-Zahlen NZ

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

Moderne Schreibweise I = 1, II = 2, ..., IIIIIIIIII = 10, usw.

→ **natürliche Zahlen,** $\mathbb{N}$

Ferner „heutzutage" (seit 4. Jahrhundert n.Chr.): kein Strich =: 0; 1 ist Nachfolger von 0; $\mathbb{N}_0$

Wozu braucht man Regel (3)?

- Weil z.B. auch {I,O}* die Regeln 1+2 erfüllt – Wir wollen aber <u>nur</u> nach Regeln (1) und (2) Gebildetes zulassen!
- Hartgesottene Mengentheoretiker ziehen auch unendlichfache Anwendung der Regel (2) in Betracht, wir hier aber nur <u>endlich</u> häufige!

Regel (3) wird oft nicht besonders erwähnt, also stillschweigend benutzt, wenn von „**induktiv**" die Rede ist.

Induktive Definition bestimmter Teilmengen einer Menge U **allgemein**

Seien $M_0 \subseteq U$, $f_k : U^{m_k} \to U$ (k=1,2, ..., evtl. partiell).
Dann existiert eine kleinste Teilmenge M von U (nämlich der „Durchschnitt von allen") mit den Eigenschaften

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

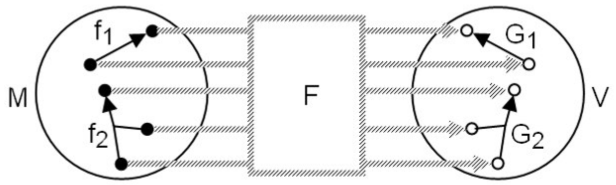
Beispiel 1 (neu)
$U = \{a, b, +, \cdot\}^*$
(1) a,b sind „(ab+ ·)-Terme".
(2) x,y (ab+ ·)-Terme $\Rightarrow$ (x+y) und (x·y) (ab+ ·)-Terme
– z.B. ((a+(b+a))·b) $\boxed{f_1 / f_2(x, y)}$

Beispiel 2 (alt)
Neandertaler-Zahlen, $U = \{|\}^* . f(x) = x|$

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 $f_k(x_1, ..., x_{m_k})$
… so gilt P auf ganz M.

… weil jedes Element
- entweder „von vornherein" die Eigenschaft P hat (da es aus M_0 ist)
- oder die Eigenschaft P von seinen „Bausteinen" aus der vorigen „Generation" bei seiner Entstehung „erbt".

Rekursive Definition
von Abbildungen auf induktiv definiertem M – Idee:



Man baut quasi das Bild parallel mit den Aufbauschritten des Urbilds auf.
Seien
- ein Wertebereich V und
- für jede Erweiterungsregel (k) ein $G_k : V^{m_k} \to V$ gegeben.

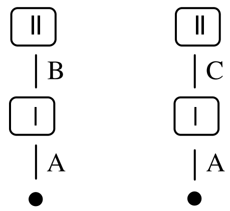
Dann definiert man durch
- $F(x) \in V$ für alle $x \in M_0$ festlegen. – **Basisfälle**
- $F(f_k(x_1, ..., x_{m_k})) := G_k(F(x_1), ..., F(x_{m_k}))$ – **Rekursion**

eine Abbildung $F : M \to V$, zumindest **sofern** jedes Element von M eine „**eindeutige Entstehungsgeschichte**" hat, (d.h. interferenzfrei, ambivalenzfrei, eindeutig **parsebar** ist) – **oder** ein Beweis der **Wohldefiniertheit** gelingt.

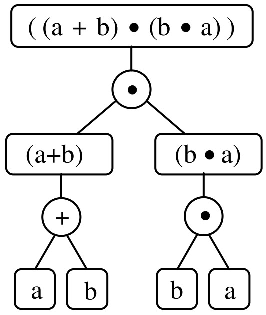
Gegenbeispiel:
keine eindeutige Entstehungsgeschichte
Australopithecus-Zahlen:
(A) | ist APZ.
(B) n APZ $\Rightarrow$ $n|$ ist APZ.
(C) n nat. Z. $\Rightarrow$ $|n$ ist APZ.

→ Einschub: **Entstehungsgeschichten** …

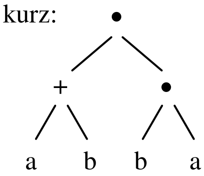
sind i.a. Bäume, ähnlich den *parse trees*. Im Problembeispiel APZ hat || die (unverzweigten) Entstehungsgeschichten (Wurzel = || oben):



Verzweigtes Beispiel
(ab+ ·)-Terme, gebildet aus
2 Basisfällen: ‚a' und ‚b'
2 Erweiterungsregeln: ‚+'-Regel und ‚•'-Regel



oder kurz:



← Einschub Ende

Beispiel und Gegenbeispiel zur Wohldefiniertheit von Funktionen (genauer: Definitionsversuchen) – APZ

Links(|) := 0;	*LorR*(|) := 0;
Links(n|) := *Links*(n);	*LorR*(n|) := *LorR*(n) +1;
Links(|n) := *Links*(n)+1;	*LorR*(|n) := *LorR*(n)+1;
nicht wohldefiniert:	wohldefiniert!
$\boxed{0 = Links(||) = 1 \text{ ??}}$	$\boxed{\text{Beweis?}}$

Spezialfall rekursiv definierter Abbildungen:
rekursive Definitionen von Eigenschaften:
Eigenschaften sind Abbildungen in {W,F}.

Beispiel: mögliche Eigenschaft von Neandertalerzahlen
Gerade(|) := F
Gerade($n|$):= Wenn *Gerade*(n)=W, dann F, sonst W

Grammatiken

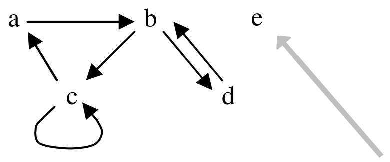
Eine **Grammatik** ist ein Quadrupel G = (N, T, S, R) mit
- einem Alphabet N von **Nichtterminalzeichen**,
- einem Alphabet T v. **Terminalzeichen**, $N \cap T = \varnothing$,
- einen **Startzeichen** $S \in N$,
- einer endlichen Menge $R \subseteq (N \cup T)^* \times (N \cup T)^*$ von **Regeln**.

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 $H(G) \subseteq (N \times T)^*$ **induktiv** gegeben ist durch
$S \in H(G)$ und $r\,v\,s \in H(G) \wedge v \to w \Rightarrow r\,w\,s \in H(G)$.

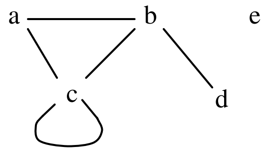
Graphen und Bäume

Gerichteter Graph := zweistellige Relation über einer Menge (i.a. graphisch dargestellt). Beispiel:



{(a,b), (b,c), (c,a), (b,d), (c,c), (d,b)} über {a,b,c,d,e}.
a, b, ..., e sind **Knoten**, (a,b), (b,c), usw. sind **Kanten**.

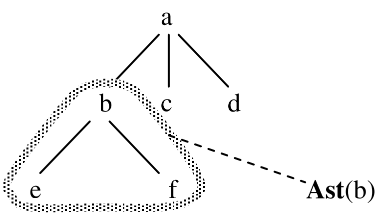
Ungerichteter Graph :=
Paar- und Singlemengenmenge (bzw. symmetrische Relation) über einer Menge, z.B.



{{a,b}, {b,c}, {c}, {c,a}, {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}

Baum: zahlreiche Definitionsmöglichkeiten wegen

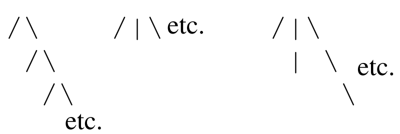
- **echter** Unterschiede: (**geordnet** (d.h. Kinder haben Reihenfolge) oder **ungeordnet, endlich** oder **unendlich** viel Knoten, **endlich verzweigt** oder **nicht**)
- unterschiedlicher Definitions**werkzeuge** (z.B. als spezieller ungerichteter oder gerichteter Graph, als spezielle Halbordnung).



- a ist die **Wurzel**.
- b, c, d sind die Kinder von a.
- **Grad** ist die Anzahl der Kinder, Grad(a)=3.
- c, d, e, f sind die **Blätter**
- a – b – e ist ein **Zweig** (Pfad Wurzel–Blatt)
- Ast siehe Bsp.: **Ast**(b)

Königs Lemma

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

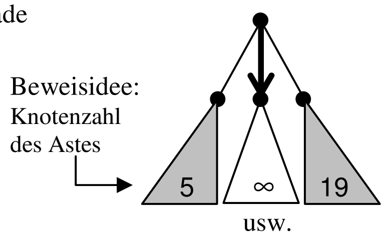


- Pfade sind immer endlich lang.
- Jeder Baum mit unendlich vielen Knoten hat einen unendlichen Pfad.
- Jeder Baum mit unendlich vielen Knoten hat endliche Pfade „beliebiger Länge.“
- Sind in einem Baum alle Pfade endlich, so ex. eine maximale Pfadlänge.
- Sind in einem Baum alle Pfade endlich, so hat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

Lemma von König

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

Gilt auch wenn die Grade unbeschränkt sind!



Anwendungen:

<u>A. Ein Solitaire-Spiel</u>

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 nachlieferbar).

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***.

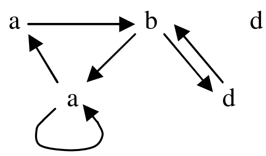
Ziel: **Spiele unendlich lange** (unendlich oft Spielzug 2)!

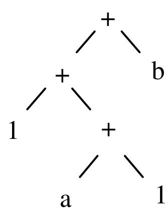
Geht das? König's Lemma → **nein!**

<u>B. Anwendung in der Logik</u>: Kompaktheitssätze

Beschriftete Graphen und Bäume

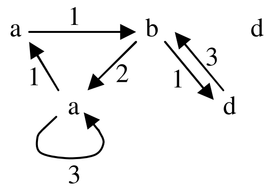
In gewöhnlichen Graphen und Bäumen gibt es jeden Knotennamen nur einmal, **der Name identifiziert den Knoten**.
In **knotenbeschrifteten** Graphen und Bäumen zeigt man meist nur die **Knotenanschriften**, die sich auch wiederholen dürfen. Die Namen werden meist ignoriert.
Mathematisch:
... + Abbildung Knotenmenge → Anschriftenmenge





Anwendung: **Syntaxbäume** (endlich, geordnet) von Termen Beispiel: ((1+(a+1))+b) s.o.rechts

Es gibt auch **kantenbeschriftete** sowie **gleichzeitig knoten- und kantenbeschriftete***) Graphen und Bäume
(+ Abbildung Kantenmenge → Anschriftenmenge)



***)** Spezialfall: **Automaten** (→ Theor. Informatik, aber mit zusätzlichen Komponenten, z.B. Anfangszustand).