Vorlesung Logik

Prof. Dr. Gerhard Brewka

Gebraucht die Zeit, sie geht so schnell von hinnen,
Doch Ordnung lehrt Euch Zeit gewinnen.
Mein teurer Freund, ich rat' Euch drum
Zuerst Collegium logicum.
Da wird der Geist Euch wohl dressiert,
In spanische Stiefeln eingeschnürt,
Dass er bedächtiger so fortan
Hinschleiche die Gedankenbahn,
Und nicht etwa, die Kreuz und Quer',
Irrlichteliere hin und her

Mephisto, Faust

1. Einführung

1.1 Teilgebiete der Informatik und Theoretische Informatik

Die Informatik wird oft in folgende 4 Gebiete eingeteilt: Technische, Praktische, Angewandte und Theoretische Informatik.
Die Theoretische Informatik untersucht grundlegende Konzepte, die für das gesamte Gebiet von Bedeutung sind. Die Vorlesung Logik gehört zu einem Zyklus von 4 Vorlesungen des Bachelorstudiums. Wir geben hier zunächst einen kurzen Überblick über relevante Themen dieser Vorlesungen:

1. Diskrete Strukturen:

    Hier werden die wichtigsten Grundbegriffe der theoretischen Informatik eingeführt, sozusagen das Handwerkszeug, das man in diesem Teilgebiet benötigt.

2. Logik:

    Logik untersucht Folgerungsbeziehungen. Sie entwickelt dazu präzise Sprachen, in denen exakte Spezifikationen vorgenommen werden können. Von besonderem Interesse sind auch automatisierbare Schlussverfahren. Zur Logik gleich mehr.

3. Formale Sprachen:

    Formale Sprachen sind Kunstsprachen, wie sie z.B. zur Kommunikation mit Rechnern entwickelt werden (Programmiersprachen). Untersucht werden verschiedene Klassen solcher Sprachen, ihre Eigenschaften, Beschreibungsmöglichkeiten (Grammatiken) und entsprechende Automatenmodelle, durch die diese Sprachen erkannt werden können.

4. Berechenbarkeit und Komplexität:

Die Berechenbarkeitstheorie untersucht, wie der Begriff der Berechenbarkeit präzisiert werden kann. Verschiedene Modelle (Turing-Berechenbarkeit, While-Berechenbarkeit, ...) erweisen sich als äquivalent. Man kann zeigen, dass es nicht berechenbare, mathematisch präzise beschreibbare Funktionen gibt.

Die Komplexitätstheorie untersucht, wie die Komplexität von Algorithmen (Rechenvorschriften) beschrieben werden kann. Dazu werden verschiedene Komplexitätsklassen und Beschreibungsmittel eingeführt.

1.2 Was ist Logik?

Lehre von den formalen Beziehungen zwischen Sätzen
(insbesondere Folgerungsbeziehungen)

als eigenständige Wissenschaft begründet von Aristoteles. Er unterscheidet:

Lehre vom Begriff (Klassifizierung von Begriffen, Definitionslehre)
Lehre vom Urteil (Struktur, Klassifikation von Aussagesätzen)
Lehre vom Schluss (Folgerungsbeziehungen aufgrund der Struktur der Sätze)

Beiträge von Stoikern (Theorien der Implikation, logische Antinomien)
mittelalterl. Scholastik (Arbeiten zu Sprachphilosophie und log. Semantik)
Leibniz Vorläufer der modernen Logik: log. Symbolsprache für alle Wissenschaften
Entwicklung der modernen mathematischen Logik ab Mitte 19. Jh. (Frege, Boole, Russell)

Charakteristika:
formale Kunstsprache, modelltheoretische Semantik, korrekte und vollständige Kalküle

Bemerkung: es gibt viele verschiedene math. Logiken (mehrwertige, modale, deontische, dynamische, lineare, nichtmonotone, fuzzy, temporale Logik etc.)

Wenn wir von "der" Logik sprechen, ist die klassische Aussagen- oder Prädikatenlogik gemeint.

Warum ist Logik relevant für Informatiker?

Beschreibungsmittel für formale Sachverhalte	Wissensrepräsentation
Semantik von Programmiersprachen	Schaltalgebra
Logisches Programmieren (PROLOG)	Automatisches Beweisen
Programmverifikation	usw.

Logik untersucht Folgerungen aufgrund der Struktur der Sätze:

Wenn es regnet, dann ist die Straße nass.
Es regnet.
Die Straße ist nass

Schluss unabhängig von Bedeutung von "es regnet", "die Straße ist nass":

Wenn es grubelt, dann brabelt es.
Es grubelt.
Es brabelt

Folgender Schluss ist nicht-logisch, da er Wissen über die Bedeutung der Sätze voraussetzt:

Peter ist mein Bruder
Peter ist mit mir verwandt

Ein logischer Schluss liegt erst vor, wenn das zusätzliche Wissen explizit gemacht wird:

Wenn Peter mein Bruder ist, ist er mit mir verwandt.
Peter ist mein Bruder.
Peter ist mit mir verwandt.

Logik abstrahiert von der Bedeutung der in Schlüssen verwendeten Sätze.

Relevant ist nur (im Falle der klassischen Logik)

1) der Aufbau komplexer Sätze (wenn ... dann, und, oder, ...)

2) dass Sätze entweder wahr oder falsch sind

Da die natürlicher Sprache vage, mehrdeutig und kontextabhängig ist, verwendet die Logik eine Kunstsprache:

Eine festgelegte Menge von Symbolen (etwa A, B, C, A1, A2, ...) repräsentiert elementare Aussagen, andere Symbole ($\wedge$, v, $\rightarrow$, $\neg$) Verknüpfungen von solchen Aussagen.

math. Exaktheit, auf Kosten von Ausdrucksfähigkeit, Flexibilität, Nuancenreichtum

Bsp.: $A \wedge B$ in der Aussagenlogik äquivalent zu $B \wedge A$, aber:

Peter bekam Fieber und der Arzt verschrieb ein Medikament.
Der Arzt verschrieb ein Medikament und Peter bekam Fieber.

Grundlage dieser Vorlesung:

Uwe Schöning, Logik für Informatiker, 5. Auflage, Spektrum Akademischer Verlag, 2000, Euro 20.00 (gebraucht bei Amazon ab 9.90).

Grobgliederung:

1. Einführung
2. Aussagenlogik
   - 2.1 Syntax
   - 2.2 Semantik
   - 2.3 Äquivalenz und Normalformen
   - 2.4 Hornformeln
   - 2.5 Endlichkeitssatz
   - 2.6 Resolution
   - 2.7 Das Davis-Putnam- Verfahren
   - 2.8 Tableauverfahren
3. Prädikatenlogik
   - 3.1 Syntax und Semantik; Normalformen
   - 3.2 Entscheidbarkeit
   - 3.3 Herbrand-Theorie und Resolution
4. Logik-Programmierung
   - 4.1 Definite Programme und minimale Modelle
   - 4.2 Default Negation und stabile Modelle
   - 4.3 Answer-Set-Programmierung

Zur Einstimmung:

Wenn ich kein Bier zum Essen trinke, dann esse ich immer Fisch.

Wenn ich Eis esse oder kein Bier trinke, dann esse ich nie Fisch.

Vereinfachung? Immer Bier und entweder kein Fisch oder kein Eis.

(kann man anhand des Durchspielens aller Möglichkeiten sehen)

Appendix: Mathematische Grundbegriffe

Die hier beschriebenen Begriffe sind elementare Grundbegriffe der theoretischen Informatik. Sie sind nicht Gegenstand der Vorlesung, werden aber der Vollständigkeit halber hier benannt.

a) Mengen

Cantor (1845-1918) gilt als Begründer der Mengenlehre. Er charakterisiert Mengen folgendermaßen:

Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen; diese Objekte heißen die Elemente der Menge

Notation: a Element von M: $a \in M$
a nicht Element von M: $a \notin M$

endliche Mengen lassen sich aufzählen: {2,8,12,13}, {Peter, Hans, Fritz}

unendliche Mengen können durch Angabe der Eigenschaften ihrer Elemente definiert werden

$$\{x \mid x \text{ ist Primzahl}\}$$

oder induktiv, z.B.:

M_1 ist die kleinste Menge für die gilt:

1) $aa \in M_1$ und $bb \in M_1$ (Basisfälle)
2) wenn $w \in M_1$, dann gilt $awa \in M_1$ und $bwb \in M_1$ (abgeleitete Fälle).

Beispiele für Elemente in M_1: abbaabba, baab, nicht in M_1: babab

Induktive Definitionen erlauben Induktionsbeweise:
eine Eigenschaft E gilt für alle Elemente einer induktiv definierten Menge, wenn
1) E für die Basisfälle gilt (hier aa und bb), und
2) E für die abgeleiteten Fälle gilt, vorausgesetzt E gilt für die Elemente, aus denen sie abgeleitet werden (hier w).

Beispiel: zeige, dass jedes Element von M_1 eine gerade Anzahl von a's und b's besitzt.

1) aa besitzt 2 a's und 0 b's, bb besitzt 0 a's und 2 b's
2) Angenommen w besitzt m a's und n b's, wobei m und n gerade.
   awa besitzt m+2 a's und n b's, beide gerade.
   bwb besitzt m a's und n+2 b's, beide gerade. QED

Extensionalitätsprinzip: Mengen sind gleich, wenn sie dieselben Elemente haben:

$$M = N \text{ gdw. für alle } x \text{ gilt: } (x \in M \text{ gdw. } x \in N)$$

Vorsicht: es sind nicht beliebige Mengenkonstruktionen durch Aussagen möglich:

Russellsche Antinomie: es gibt sicherlich Mengen, die sich nicht selbst als Element enthalten. Gibt es auch die Menge all dieser Mengen:

$$\{ M \mid M \notin M\}$$

Angenommen, es gäbe diese Menge. Enthält sie sich selbst? 2 Möglichkeiten:
a) sie enthält sich nicht selbst: dann enthält sie sich nach Definition.
b) sie enthält sich selbst: dann enthält sie sich nicht nach Definition.

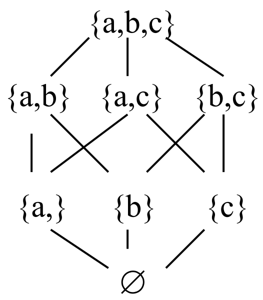
Sätze wie „x ist Primzahl" nennt man auch Aussageformen.
Nicht jede beliebige Aussageform ist also geeignet für die Definition von Mengen verschiedene Ansätze, die Antinomien ausschließen, wurden entwickelt.

hier: naiver Mengenbegriff ausreichend.

Grundbegriffe der Mengenlehre:

Teilmenge: $N \subseteq M$ gdw. für alle x: $x \in N$ impliziert $x \in M$.
echte Teilm.: $N \subset M$ gdw. $N \subseteq M$ und nicht $M \subseteq N$.
leere Menge: $\varnothing$
Potenzmenge einer Menge M: $P(M) = \{ X \mid X \subseteq M\}$

Beispiel: P({a,b,c})



Für alle Mengen M, N, P gilt:

$M \subseteq M$ (Reflexivität)
$N \subseteq M$ und $M \subseteq P$ impliziert $N \subseteq P$ (Transitivität)
$N \subseteq M$ und $M \subseteq N$ impliziert $M = N$ (Antisymmetrie)

Mengenalgebra:

$M \cap N = \{x \mid x \in M \text{ und } x \in N\}$	Schnitt von M und N
$M \cup N = \{x \mid x \in M \text{ oder } x \in N\}$	Vereinigung von M und N
$M \setminus N = \{x \mid x \in M \text{ und } x \notin N\}$	Differenz von M und N

falls $M \cap N = \emptyset$ nennt man M und N disjunkt.

Eigenschaften der Operationen:

Kommutativität:	$M \cap N = N \cap M$ $M \cup N = N \cup M$
Assoziativität:	$M \cap (N \cap P) = (M \cap N) \cap P$ $M \cup (N \cup P) = (M \cup N) \cup P$
Distributivität:	$M \cap (N \cup P) = (M \cap N) \cup (M \cap P)$ $M \cup (N \cap P) = (M \cup N) \cap (M \cup P)$
Idempotenz:	$M \cap M = M$ $M \cup M = M$

Ist M Teilmenge einer (Grund)-Menge G, so heißt $C_G(M) = G \setminus M$ Komplement von M bezüglich G.
Häufig ist aus Kontext klar, welches G gemeint ist, und man spricht einfach vom Komplement von M und notiert es C(M)

de Morgansche Gesetze:

$$C(M \cap N) = C(M) \cup C(N)$$
$$C(M \cup N) = C(M) \cap C(N)$$

Seien M und N Mengen, das kartesische Produkt (auch: Kreuzprodukt) von M und N ist die Menge

$$M \times N = \{(a,b) \mid a \in M, b \in N\}$$

(a,b) bezeichnet man als geordnetes Paar

Seien $M_1, \ldots, M_n$ Mengen

$$M_1 \times \ldots \times M_n = \{(x_1, \ldots, x_n) \mid x_i \in M_i\}$$

ist die Menge der n-Tupel über Mengen $M_1, \ldots, M_n$.

3-Tupel heißen auch Tripel, 4-Tupel Quadrupel, 5-Tupel Quintupel
falls $M_1 = \ldots = M_n = M$, so heißt $M_1 \times \ldots \times M_n$ auch M^n.

b) Relationen

Grundlegende Definitionen

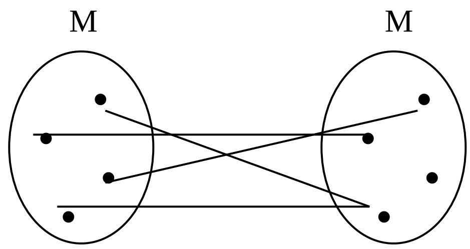
Relation R in einer Menge M: Beziehung zwischen je 2 Elementen von M.
Beispiel <-Relation auf natürlichen Zahlen Nat: $a < b$ gdw es gibt $r \in$ Nat, so dass $a + r = b$.
Falls $a < b$ sagt man auch: $<$ trifft auf (a,b) zu.
Relation $<$ kann durch alle Paare, auf die sie zutrifft, charakterisiert werden:

> Eine Relation R in einer Menge M ist eine Teilmenge von M x M.
> Statt $(a,b) \in R$ schreibt man auch aRb.

Beispiele: x ist Teiler von y, x ist Vater von y, x ist Chef von y, ...

Entsprechend: Relation zwischen Mengen M und N: Teilmenge von M x N

Graphische Veranschaulichung endlicher Relationen:



zu R inverse Relation $R^{-1} = \{(y,x) \mid (x,y) \in R\}$

Wichtige Eigenschaften von Relationen:

R ist:	falls für alle x, y, z ∈ M gilt:	Beispiel:
reflexiv:	xRx	$\subseteq$ (Teilmengenrelation)
irreflexiv:	nicht xRx	$\subset$ (echte Teilmengenrelation)
symmetrisch:	wenn xRy, dann yRx	$\equiv$ (Äquivalenz von Formeln)
asymmetrisch:	xRy impliziert nicht yRx	$\subset$
antisymmetrisch:	xRy und yRx impliziert x = y	$\subseteq$
transitiv:	xRy und yRz impliziert xRz	$\models$
linear:	xRy oder yRx	$\geq$ (z.B. auf Nat)
voreindeutig:	yRx und zRx impliziert y = z	nur 1 Kante zu Knoten in Nb
eindeutig:	xRy und xRz impliziert y = z	nur 1 Kante zu Knoten in Vb
eineindeutig:	eindeutig und voreindeutig	

Verknüpfung von Relationen: Seien R und S Relationen in M. Die Verknüpfung von R und S, $R \circ S$, ist die Menge von Paaren $\{(x,z) \mid$ es gibt ein y mit xRy und ySz$\}$.

(Analog für Relationen $R \subseteq M \times N$, $S \subseteq N \times P$; $R \circ S$ ist dann Relation zwischen M und P)

Beispiel: Sei M = {Peter, Franz, Fritz, ...} eine Menge von Personen,
$V = \{(x,y) \mid x, y \in M$, x verwandt mit y$\}$
$F = \{(x,y) \mid x, y \in M$, x befreundet mit y$\}$
Dann ist
$(x,y) \in V \circ F$ gdw. y ist Freund eines Verwandten von x
$(x,y) \in F \circ V$ gdw. y ist Verwandter eines Freundes von x

Sei R eine Relation in M. Die transitive Hülle von R, R^t, ist die kleinste Relation, für die gilt:

a) $R \subseteq R^t$
b) wenn $(x,y) \in R^t$ und $(y,z) \in R$, dann $(x,z) \in R^t$.

Beispiele:
a) Sei $R = \{(x,x+1) \mid x \in Nat\}$ die direkte Nachfolgerrelation auf Nat, dann ist R^t die <-Relation
b) Sei $R = \{(x,y) \mid$ x Kind von y$\}$, dann ist $(v,w) \in R^t$ gdw v Nachkomme von w.

Äquivalenzrelationen

Eine Relation R in M heißt Äquivalenzrelation, wenn R reflexiv, symmetrisch und transitiv ist. Man sagt dann: a ist äquivalent zu b bzgl. R falls aRb.

Beispiele:
$R = \{(x,y) \mid$ x, y Studierende im selben Semester$\}$
$R_n = \{(x,y) \mid$ x,y aus Nat, es gibt z aus Nat, so dass x-z und y-z teilbar durch n$\}$

Eine Zerlegung (Partition) einer Menge M ist eine Menge K von nichtleeren Teilmengen von M, so dass gilt:
1. die Elemente von K sind paarweise disjunkt,
2. jedes Element von M ist Element eines Elementes von K.

Jede Äquivalenzrelation R in M induziert eine Zerlegung K von M in Äquivalenzklassen, wobei a und b zu einer Klasse gehören gdw aRb.