Technische Universität Clausthal

Institut für Informatik

Sommersemester 2004

Seminarvortrag „Axiomatische Theorien in der Logik“

im Themenkomplex II: „Information und Logik“

Hauptseminar „Theoretische Informatik“

bei Herrn Professor Kupka

Robert Hartmann

Zitat (unbekannt): „Die Kunst des Vortragens, ist die Kunst des Weglassens“
Zitat (Blaise Pascal): „Die wahre Methode […Beweise zu führen…] wäre […]
alle Begriffe zu definieren und alle Behauptungen zu beweisen.“

Inhalt(1)

Inhalt(2)

1) Begriffsdefinitionen

A: (formale) Aussagenlogik

Definition (Formel oder Aussagensatz):

Jedes (aussagenlogische) Symbol, das für eine Aussage steht, ist ein Aussagensatz. Die Wahrheitssymbole sowie jede Aussage selbst sind Aussagensätze.
Aussagen lassen sich mit Verknüpfungssymbolen zu einer neuen Aussage verschmelzen.

Wahrheitssymbole:	*true*	richtig, wahr
	false	falsch, unwahr
Verknüpfungssymbole:	*not*, $\neg$	Negation
	and, $\wedge$	Konjunktion
	or, $\vee$	Disjunktion
	if-then	Bedingung (oder Folgerung, Implikation)
	$\equiv$	Äquivalenz
	if-then-else	Bedingung mit Alternative

Normaler Weise werden auch $\Rightarrow$ für Implikation, $\Leftrightarrow$ für Äquivalenz benutzt.
In diesem Text werden diese Zeichen als metasprachliche Elemente benutzt, welche metasprachliche Implikation bzw. metasprachliche Äquivalenz bedeuten.

Definition (Interpretation einer Formel):

Die Zuweisung von Wahrheitswerten (*true* oder *false*) zu den aussagenlogischen Symbolen in einer Formel heißt Interpretation einer Formel.

Definition (Wert einer Formel):

Der (Wahrheits-)Wert einer Aussage ist *true* oder *false*, nie beides gleichzeitig.
Der Wert ermittelt sich während des Auswertens der Interpretation.

> **Anmerkung:** Im Folgenden setze ich Kenntnis über die Art, wie mit Formeln umgegangen werden kann, voraus.

Definition (Gültigkeit einer Formel):

Eine Formel F ist gültig [valid], falls der Wert von F unter jeder Interpretation *true* ist.
F wird dann auch Tautologie genannt.

B: Prädikatenlogik (erster Ordnung)

Definition (Symbole):

Zu den Symbolen der Aussagenlogik kommen folgende hinzu:

Konstanten: $a,\ b,\ c,\ a',\ b',\ c',\ a_1,\ b_1,\ c_1\ \ldots$

Variablen: $u,\ v,\ w,\ x,\ y,\ z,\ u_1,\ v_1,\ w_1,\ x_1,\ y_1,\ z_1\ \ldots$

Funktionssymbole [Funktionen]: $f,\ g,\ h,\ f_1,\ g_1,\ h_1\ \ldots$

Prädikatsymbole [Prädikate, Relationen]: $p,\ q,\ r,\ p_1,\ q_1,\ r_1\ \ldots$

Existenzquantor: $\exists$ „Es existiert“

Allquantor: $\forall$ „Für alle“

Konstanten und Variablen beschreiben Objekte, Funktionssymbole und Prädikatssymbole beschreiben Funktionen und Relationen auf diesen Objekten.

Definition (Term):

Konstanten und Variablen sind Terme,
die Anwendung von f auf n Terme ergibt einen Term, d.h: $f(t_1,\ldots,t_n)$ ist ein Term.

Definition (Aussage):

Aussagen in der Prädikatenlogik sind dafür gedacht,
Relationen (Beziehungen) zwischen Objekten zu beschreiben.
Die Wahrheitssymbole sind Aussagen,
$p(t_1,...,t_n)$ ist eine Aussage, wenn $t_1,...,t_n$ n Terme sind.

Definition (Satz):

Jede Aussage ist ein Satz.
Sätze lassen sich mit den gleichen Verknüpfungssymbolen wie Formeln der Aussagenlogik zu einem neuen Satz verschmelzen.
Zusätzlich: $(\exists x)F$, $(\forall x)F$ sind Sätze, wenn F ein Satz ist.

Definition (freie und gebundene Variable):

Variablen, die von Quantoren (Allquantoren oder Existenzquantoren) gebunden werden, heißen gebundene Variablen. Alle anderen heißen freie oder ungebundene Variablen.

Beispiel:
Sei F ein Satz mit $F = (\exists x)(\forall z)\, p(x,\ f(z),\ y)$.
So sind x und z in F gebundene Variablen,
da sie jeweils durch $(\exists x)$ bzw. $(\forall z)$ gebunden sind.
y in F ist freie Variable.

Definition (Bereinigung):

Ein prädikatenlogischer Satz F heißt bereinigt, falls keine Variable in F sowohl gebunden als auch frei vorkommt und falls keine Variable als gebundene Variable in mehreren Quantoren auftritt. Durch Umbenennung von gebundenen Variablen lässt sich jeder Satz F in eine bereinigte Form $\tilde{F}$ überführen, die zu F logisch äquivalent ist.

Definition (Pränexform, pränexe Normalform):

Ein Satz F ist in Pränexform, falls er die Bauart $Q_1 x_1 ... Q_n x_n E$ hat, wobei die Q_i Quantoren sind und in E kein Quantor mehr vorkommt.

Definition (geschlossener Satz):

Ein Satz, in dem keine freien Variablen vorkommen, heißt geschlossener Satz.

Beispiel:
Der Satz $(\forall x)p(x,y)$ ist nicht geschlossen, hingegen $(\forall x)(\exists y)p(x,y)$ wohl.

Definition (Interpretation eines Satzes):

Sei D eine beliebige nicht leere Menge, D heiße Domain.
Eine Interpretation I über einer Domain D verbindet Werte mit jeder Konstanten, Variablen, sowie jedem Funktions- und Prädikatssymbol in folgender Weise:

- Zu jeder Konstanten a, ein Element $a_I \in D$
- Zu jeder Variablen x, ein Element $x_I \in D$
- Zu jedem Funktionssymbol f mit n-Argumenten, eine n-äre Funktion $f_I(d_1,...,d_n)$, wobei die $d_j \in D$ und der Wert von $f_I(d_1,...,d_n)$ zu D gehört.
- Zu jedem Prädikatensymbol p mit n-Argumenten, eine n-äre Relation $p_I(d_1,...,d_n)$, wobei die $d_j \in D$ und der Wert von $p_I(d_1,...,d_n)$ ist entweder *true* oder *false*.

Definition (Gültigkeit eines Satzes):

In der Prädikatenlogik ist die Gültigkeit eines Satzes nur für geschlossene Sätze definiert.
Ein geschlossener Satz F ist gültig [valid], falls der Wert von F unter jeder Interpretation *true* ist.

Definition (Allgemeinster Unifikator, most general unifier)

Sei Γ eine Menge von Literalen, das sind Formeln oder Teilformeln, Sätze oder Teilsätze.

q heißt Unifikator (Vereinheitlicher) von Γ, wenn q alle Elemente aus Γ durch simultane Substitution gleich macht.
Dies bedeutet für $F \neq G, F \in \Gamma, G \in \Gamma$ ist $Fq = Gq$.

Anmerkung: Der Unifikator wird unter anderem bei den später eingeführten Resolutions- und Skolemisierungsregeln angewendet.

C: Axiomatische Theorien

Definition (Axiome):

Eine Theorie wird durch ihre Axiome, das ist eine Menge von geschlossenen Sätzen, definiert. Ein Axiom wird dann erfüllt, wenn seine Interpretation *true* liefert.

Definition (Modell):

Eine Interpretation I ist genau dann ein Modell für eine Theorie T mit den Axiomen A_i, wenn jedes der Axiome A_i der Theorie unter dieser Interpretation I erfüllt ist.

Definition (Theorieerweiterung):

Unter der Erweiterung einer Theorie versteht man das Hinzufügen von geschlossenen Sätzen zu der Menge der Axiome.
Anmerkung: Durch Theorieerweiterung kann sich die Menge der Modelle verringern. Theorien, die <u>keine Modelle</u> besitzen, heißen <u>inkonsistente Theorien</u>.

Definition (Gültigkeit eines Satzes):

Ein geschlossener Satz F ist gültig [valid], falls der Wert von F unter jedem Modell der Theorie *true* ist.

Anmerkung: Beachte den feinen Unterschied zur Prädikatenlogik: Ein geschlossener Satz F ist gültig [valid], falls der Wert von F unter jeder Interpretation *true* ist.

Definition (Relativierende Quantoren):

Für jedes unäre Prädikatensymbol p und jeden Satz F

$$(\forall px)F \Leftrightarrow (\forall x)[\mathit{if}\ \ p(x)\ \mathit{then}\ F]$$

$$(\exists px)F \Leftrightarrow (\exists x)[\,p(x)\ \mathit{and}\ \ F]$$

Beispiel:

In der Theorie T_1 bestehe die Menge der Axiome aus genau:

$F_1 : (\forall x)\, p\big(x, f(x)\big)$

$F_2 : (\forall x)\, p\big(x, m(x)\big)$

$F_3 : (\forall x, y)[\mathit{if}\ \ p(x, y)\ \mathit{then}\ gf(x, f(y))]$

$F_4 : (\forall x, y)[\mathit{if}\ \ p(x, y)\ \mathit{then}\ gm(x, m(y))]$

Die Interpretation I der Theorie T_1 bekomme den Namen „Familieninterpretation“, J hingegen heiße „Integerinterpretation“.

I sei eine Interpretation für T_1, in der gilt:

$f(x) \Leftrightarrow$ Vater von x

$m(x) \Leftrightarrow$ Mutter von x

$p(x, y) \Leftrightarrow$ y ist Elternteil von x

$gf(x, y) \Leftrightarrow$ y ist Großvater von x

$gm(x, y) \Leftrightarrow$ y ist Großmutter von x

J sei eine Interpretation für T_1, in der gilt:

$f(x) \Leftrightarrow 2x$

$m(x) \Leftrightarrow 3x$

$p(x, y) \Leftrightarrow y = 2x$ oder $y = 3x$

$gf(x, y) \Leftrightarrow y = 4x$ oder $y = 6x$

$gm(x, y) \Leftrightarrow y = 6x$ oder $y = 9x$

Vorschlag für Bedingungen an ein axiomatisches System (Karl Popper):

Karl Popper schlägt diese allgemeinen Bedingungen vor:
„Wir sagen, dass ein theoretisches System axiomatisiert ist,
wenn eine Anzahl von Sätzen, Axiomen, aufgestellt wird, die folgenden vier Grundbedingungen genügen:
Das System der Axiome muss, für sich betrachtet,

(a) widerspruchsfrei sein, was mit der Forderung äquivalent ist, dass nicht jeder beliebige Satz aus dem Axiomensystem ableitbar sein soll;
(b) unabhängig sein, d.h. keine Aussage enthalten, die aus den übrigen Axiomen ableitbar ist („Axiom“ soll nur ein innerhalb des Systems nichtableitbarer Grundsatz heißen.)

Was ihr logisches Verhältnis zu den übrigen Sätzen des axiomatisierten Systems betrifft, so sollen die Axiome überdies

(c) zur Deduktion aller Sätze dieses Gebietes hinreichen und
(d) notwendig sein, d.h. keine überflüssigen Bestandteil enthalten.“

(Logik der Forschung, S. 41)

2) Polarität des Vorkommens

- Entscheidungshilfe beim Tabellenverfahren
- Zwei Arten der Polarität: positive und negative
- Es gibt verschiedene Regeln, wie Polaritäten auf Literale verteilt werden. [Eine Liste der Regeln ist in der Ausarbeitung nachzulesen]

Definition (Kraft von Quantoren [=force of quantifiers]):

Ein Quantor hat **universelle Kraft** (kenntlich gemacht durch das Superscript $(...x)^{\forall}$) in einem Satz, wenn

- er ein Allquantor mit positiver Polarität ist $[(\forall x)F]^{+} \Rightarrow (\forall x)^{\forall} F$
- er ein Existenzquantor mit negativer Polarität ist $[(\exists x)F]^{-} \Rightarrow (\exists x)^{\forall} F$

Ein Quantor hat **existenzielle Kraft** (kenntlich gemacht durch das Superscript $(...x)^{\exists}$) in einem Satz, wenn

- er ein Allquantor mit negativer Polarität ist $[(\forall x)F]^{-} \Rightarrow (\forall x)^{\exists} F$
- er ein Existenzquantor mit positiver Polarität ist $[(\exists x)F]^{+} \Rightarrow (\exists x)^{\exists} F$

Ein Quantor mit **dualer Kraft** (kenntlich gemacht durch das Superscript $(...x)^{\forall\exists}$) kann nur im direkten Wirkungsbereich von Äquivalenzverbindung $\equiv$ oder bei *if-then-else* Konstrukten vorkommen.

3) Skolemisierung

Beim deduktiven Tableaux-Verfahren für Prädikatenlogik (und axiomatische Theorien) spielt die Skolemisierung von Sätzen eine Rolle.

- Das Entfernen von Quantoren
- Äquivalente Umformung ist die Entfernung von Quantoren mit existenzieller Kraft
- Nicht äquivalente Umformung ist die Entfernung von Quantoren mit universeller Kraft, jedoch wird die Gültigkeit beibehalten.

Die fünf Regeln der (vollen) Skolemisierung:

Schritt 1: Beseitigung der Quantoren mit dualer Kraft.

- Äquivalenz Elimination:
  $F \equiv G \Leftrightarrow (if\ F\ then\ G)\ and\ (if\ G\ then\ F)$

  $F \equiv G \Leftrightarrow (F\ and\ G)\ or\ ((not\ F)\ and\ (not\ G))$
- Elimination der bedingten Verbindung:
  $if\ F\ then\ G\ else\ H \Leftrightarrow (if\ F\ then\ G)\ and\ (if\ (not\ F)\ then\ H)$

  $if\ F\ then\ G\ else\ H \Leftrightarrow (F\ and\ G)\ or\ ((not\ F)\ then\ H)$
- Elimination der bedingten Relation/Funktion
  $p(\overline{r}, if\ F\ then\ t_1\ else\ t_2, \overline{s}) \Leftrightarrow if\ F\ then\ p(\overline{r}, t_1, \overline{s})\ else\ p(\overline{r}, t_2, \overline{s})$

  $f(\overline{r}, if\ F\ then\ t_1\ else\ t_2, \overline{s}) \Leftrightarrow if\ F\ then\ f(\overline{r}, t_1, \overline{s})\ else\ f(\overline{r}, t_2, \overline{s})$

Schritt 2: Falls nötig, bereinigen des Satzes.

Schritt 3: Bringe den Satz in Pränexform.

Führe die Schritte 4 und 5, von rechts nach links auf einen Satz angewendet, aus.

Schritt 4: Entfernung von Quantoren strikter universeller Kraft durch Hinzufügen einer Skolem-Konstanten oder Skolem-Funktion.
So lange, bis keine Quantoren strikter universeller Kraft mehr vorhanden.

Schritt 5: Entfernung von Quantoren strikter existenzieller Kraft durch einfaches Weglassen des Quantors.
Domain-Element für entsprechende Variablen einsetzen.
So lange, bis keine Quantoren strikter existenzieller Kraft mehr vorhanden.

4) Deduktives Tableaux-Verfahren für die Prädikatenlogik

Bemerkung: Das Verfahren für die Aussagenlogik, sowie ein Beispiel „aussagenlogischer Beweis mit Polaritätsstrategie" kann in der Ausarbeitung nachgelesen werden.

Die Tabelle besteht aus zwei Spalten:

Annahmen (Assertions)	Ziele (Goals)

Pro Annahme und Ziel eine Zeile, d.h. Annahmen und Ziele dürfen nicht in einer Zeile stehen, wobei es egal ist in welcher Reihenfolge eingetragen wird.

Zum Beispiel $If\ (A_1\ and\ A_2\ and\ A_3)\ then\ (G_1\ or\ G_2\ or\ G_3)$ kann in folgender Tabelle notiert sein.

Annahmen (Assertions)	Ziele (Goals)
	G_3
A_2	
A_3	
	G_1
A_1	
	G_2

Sowohl die Annahmen als auch die Ziele werden nur in simplifizierter Form in die Tabelle eingetragen.

$not(not\ F) \Rightarrow F;\ F\ and\ true \Rightarrow F;\ F\ or\ false \Rightarrow F;\ if\ F\ then\ false \Rightarrow not\ F$
sind solche Vereinfachungen.

Eine größere Liste mit Simplifizierungen findet man in der Ausarbeitung.

Definition (Semantische Bedeutung einer Tabelle)

Eine Tabelle mit den Annahmen $A_1, A_2, ..., A_m$ und den Zielen $G_1, G_2, ..., G_n$ ist wahr unter einer Interpretation I, falls folgendes erfüllt ist:

Falls der Universalschluss $(\forall *) A_i$ jeder Annahme A_i unter I wahr ist,
dann ist mindestens ein Existenzschluss $(\exists *) G_j$ für ein Ziel G_j unter I wahr.

Unwahr unter einer Interpretation I wird eine Tabelle, falls folgendes erfüllt ist:

Der Universalschluss $(\forall *) A_i$ jeder Annahme A_i unter I ist wahr und der Existenzschluss $(\exists *) G_j$ ist unwahr für jedes Ziel G_j unter I

Nach logischer Umformung der Definition gilt:

Eine <u>Tabelle</u> ist unter einer Interpretation I genau dann <u>wahr</u>,
<u>wenn</u> mindestens ein <u>Universalschluss</u> $(\forall *) A_i$ <u>einer</u> <u>Annahme</u> A_i <u>unwahr</u> unter I ist
<u>oder</u> mindestens ein <u>Existenzschluss</u> $(\exists *) G_j$ <u>eines</u> <u>Ziel</u> G_j unter I <u>wahr</u> ist.

Definition (Gültigkeit einer Tabelle)

Eine Tabelle ist gültig wenn ihre semantische Bedeutung wahr ist für jede Interpretation.

Definition (Positionswechsel, Dualitätseigenschaft)

Unter einem Positionswechsel versteht man das Verschieben eines Ziels in die Annahme-Spalte, bzw. das Verschieben einer Annahme in die Ziel-Spalte.

Annahmen (Assertions)	Ziele (Goals)
	F

Wird dann zu:

Annahmen (Assertions)	Ziele (Goals)
(not F)	

Definition (Polarität)

Für Tabellen wird eine Anfangspolarität wie folgt gesetzt:

- Jedes Ziel hat positive Polarität
- Jede Annahme hat negative Polarität
- Die Polarität von Teilformeln in Annahmen oder Zielen ist abhängig von den vorher eingeführten Polaritätsregeln.

Beispiel:

Annahmen (Assertions)	Ziele (Goals)
	$[F]^{+}$

Wird dann zu:

Annahmen (Assertions)	Ziele (Goals)
$[not[F]^{+}]^{-}$	

Deduktionsregeln

1. Ersetzungsregel (rewriting rule)
2. Trennungsregel (splitting rule)
3. Schlussregel (resolution rule)
4. Regeln zur Äquivalenzbehandlung (equivalence rule)
5. Skolemisierungsregeln (Quantifier-elimination rule)

Polaritätsstrategie bei der Deduktion

Sei q der allgemeinste Unifikator (most general-unifier) wie oben eingeführt.
Es besagt die Polaritätsstrategie für Prädikatenlogik:

1. Ersetze $\overline{Pq}$ in $F_1q[\overline{Pq}]$ durch $\overline{false}$, wenn mindestens ein Vorkommen von $\overline{Pq}$ in $F_1q[\overline{Pq}]$ negative Polarität besitzt.
2. Ersetze $\overline{Pq}$ in $F_2q[\overline{Pq}]$ durch $\overline{true}$, wenn mindestens ein Vorkommen von $\overline{Pq}$ in $F_2q[\overline{Pq}]$ positive Polarität besitzt.

Beachte dabei, dass es egal ist in welchen Zeilen in der Tabelle F_1 und F_2 stehen.
Auch die relative Position zueinander ist nicht von Bedeutung.
Möchte man mit den oben genannten Regeln Äquivalenzen behandeln, so besagt die Strategie:

In $Fq[\overline{Pq \equiv Qq}]$ wird $(\overline{Pq \equiv Qq})$ durch $\overline{false}$ ersetzt, wenn mindestens ein Vorkommen von $(\overline{Pq \equiv Qq})$ negative Polarität besitzt.

5) Deduktives Tableaux-Verfahren für axiomatischen Theorien

1. Alle Definitionen aus den vorherigen Verfahren werden übernommen, auch für die Polarstrategie.
2. Alle Axiome der jeweiligen Theorie, werden so wie sie sind in die Spalte der Annahmen eingetragen.

6) Ausblick: Axiomatische Theorien mit Induktion

Die wichtigsten axiomatische Theorien werden durch Axiome definiert, welche das Prinzip der mathematischen Induktion benutzen.

Zum Beispiel:
Die natürlichen Zahlen werden durch die Peano-Axiome definiert.
P1: 0 ist eine natürliche Zahl
P2: Jede natürliche Zahl n besitzt einen Nachfolger n_+.
P3: Es gibt keine natürliche Zahl n mit $n_+ = 0$
P4: Gilt für m und n die Beziehung $m_+ = n_+$, dann ist $m = n$.
P5: Eine Aussage, die für 0 und auch für jeden Nachfolger n_+ jeder natürlichen Zahl, für die sie richtig ist, gilt, ist richtig für alle natürlichen Zahlen.

Die Peano-Axiome lassen sich mit

- der Konstenten 0 [Interpretation: Null]
- dem unären Funktionssymbol x_+ [Interpretation: Nachfolger]
- dem unären Prädikatensymbol $integer(x)$ [Interpretation:x ist natürliche Zahl]

wie folgt darstellen:

$$P1:\ integer(0)$$

$$P2:\ (\forall\ integer\ \ x)[integer(x_+)]$$

$$P3:\ (\forall\ integer\ \ x)[not(x_+ = 0)]$$

$$P4:\ (\forall\ integer\ \ x,y)\begin{bmatrix} if\ \ x_+ = y_+ \\ then\ \ x = y \end{bmatrix}$$

$$P5:(\forall\ \ F[x])\begin{bmatrix} if \begin{bmatrix} F[0]\ \ and \\ (\forall\ \ integer\ \ z)\begin{bmatrix} if\ \ F[z] \\ then\ \ F[z_+] \end{bmatrix} \end{bmatrix} \\ then\ \ (\forall\ \ integer\ \ x)\big[F[x]\big] \end{bmatrix}$$

7) Zum Schluss: Fragen aus der Philosophie der Mathematik

1. Die ontologische Frage: Worauf referieren mathematische Ausdrücke, d.h. wovon handelt eigentlich Mathematik?
   Oder mit anderen Worten:
   Falls eine mathematische Aussage wahr ist, was macht sie wahr?
2. Die erkenntnistheoretische Frage: Wie können wir unsere Überzeugung, dass eine mathematische Theorie wahr ist, rechtfertigen (begründen)?
   Inwiefern ist es rational, eine bestimmte mathematische Überzeugung zu haben?

Literaturhinweise:

- **Immanuel Kants (1724-1804):** „Kritik der reinen Vernunft“ (1781/1787)
- **Gottfried Wilhelm Leibniz (1646-1716):**
  „Elemente des Kalküls [Elementa calculi]“, (1679)
  „Zur Characteristica“, (nach 1690)

8) Quellenverzeichnis

- Karl Vorländer: „Geschichte der Philosophie, Band 4, Philosophie der Neuzeit“; Rowohlt Taschenbuchverlag Band 261/62, München 1966
- Rechenberg, Pomberger: „Informatik-Handbuch“ 2.Auflage; Hanser Verlag, München 1999 [ISBN 3-446-19601-3]
- Z.Manna, R.Waldinger: „the deductive Foundations of computer programming , a one-Volume Version of THE LOGICAL BASIS FOR COMPUTER PROGRAMMING“; Addison-Wesley 1993 [ISBN 0-201-54886-0]
- http://www.ifi.unizh.ch/groups/ailab/teaching/NAISemi01/Presentations/Philosophie_Mathematik.htm
- http://www.michael-giesecke.de/theorie/dokumente/01_objektbereich/fliesstext/01_axiomatische_grundlegung.htm [→Popper, „Logik der Forschung“ Tübingen 1973, 5. Aufl., S. 41.]
- Hsg. Peter Sloterdijk: „Leibniz, Ausgewählt und vorgestellt von Thomas Leinkauf“ in der Reihe „Philosophie Jetzt!“; Diederichs, München 1996 [ISBN 3-424-01280-7]