Grundbegriffe der mathematischen Logik

Vorlesung WS 2005/2006

Jakob Kellner

http://www.logic.univie.ac.at/~kellner

Kurt Gödel Research Center for Mathematical Logic

6. Vorlesung, 2005-11-23

Grundlegende Begriffe der Rekursionstheorie

- $f : \mathbb{N} \to \mathbb{N}$ ist eine partielle Funktion, wenn (klassisch) $f : A \to \mathbb{N}$ für ein $A \subseteq \mathbb{N}$. Wir setzen $\operatorname{dom}(f) := A$.
- $f : \mathbb{N} \to \mathbb{N}$ ist eine totale Funktion, wenn $\operatorname{dom}(f) = \mathbb{N}$.
- Eine partielle Funktion $f : \mathbb{N} \to \mathbb{N}$ ist p.r. (partiell rekursiv) oder rekursiv, wenn es ein URM Programm P gibt das f entspricht.
- Eine partielle Funktion $f : \mathbb{N} \to \mathbb{N}$ ist t.r. wenn sie p.r. und total ist.
- Eine totale Funktion ist also p.r. gdw sie t.r. ist.
- Eine Menge $A \subseteq \mathbb{N}$ ist rekursiv, wenn χ_A p.r. (d.h. t.r.).
- Eine Menge $A \subseteq \mathbb{N}$ ist r.e., wenn A Bild (oder äquivalent: Definitionsbereich) einer p.r. Funktion ist.
- A ist rekursiv gdw A r.e. und $\mathbb{N} \setminus A$ r.e.

De Morgan etc

Die folgenden Sätze sind Tautologien

- KG: $A \wedge B \quad \leftrightarrow \quad B \wedge A, \qquad A \vee B \quad \leftrightarrow \quad B \vee A$
- AG: $(A \wedge B) \wedge C \quad \leftrightarrow \quad A \wedge (B \wedge C), \qquad (A \vee B) \vee C \quad \leftrightarrow \quad A \vee (B \vee C)$
- DG: $(A \wedge B) \vee C \quad \leftrightarrow \quad (A \vee C) \wedge (B \vee C),$
  $(A \vee B) \wedge C \quad \leftrightarrow \quad (A \wedge C) \vee (B \wedge C),$
- De Morgan: $\neg(A \wedge B) \quad \leftrightarrow \quad (\neg A \vee \neg B), \qquad \neg(A \vee B) \quad \leftrightarrow \quad (\neg A \wedge \neg B)$
- $A \wedge (A \vee B) \quad \leftrightarrow \quad A, \qquad A \vee (A \wedge B) \quad \leftrightarrow \quad A$
- $A \vee \neg A, \qquad \neg(A \wedge \neg A)$

Daher kann man z.B. $A \vee B \vee C$ schreiben.
Bemerkung: $(\{w, f\}, \vee, \wedge, \neg)$ ist eine Boolesche Algebra.
Hier bezeichnet $\vee$ nicht ein Junktoren-Symbol, sondern die Wahrheitstheoretische Funktion $\{w, f\}^2 \to \{w, f\}$, analog für $\wedge$ und $\neg$.

Symbole und Metasymbole

Sätze der Aussagenlogik sind (bzw. kann man auffassen als) Zeichenketten aus einem Alphabet mit unendlich vielen Symbolen: $A_0, A_1, \ldots, (,), \wedge, \vee, \rightarrow, \neg$.

Im Unterschied dazu:

“Wenn φ ein Satz ist, dann auch $\neg\varphi$.”

φ ist hier ein Metasymbol, d.h. keine Zeichenkette sondern ein Platzhalter für eine beliebige Zeichenkette.

Prädikatenlogik

Aussagenlogik kann nur wenig ausdrücken.
Mehr Möglichkeiten bietet Prädikatenlogik
(oder: Logik erster Stufe, oder: first order logic, f.o.).

Beispiele für Sätze der Prädikatenlogik

- $\mathcal{L} = \{\}$ $\quad x = x$
- $\mathcal{L} = \{\cdot, e\}$ $\quad \forall x \, \exists y \, (x \cdot y = e \wedge y \cdot x = e)$
- $\mathcal{L} = \{\in\}$ $\quad \exists x \, \forall y \, \neg y \in x$

Ausblick

- Syntax: Definition der Sätze (als Zeichenketten), freie Variablen, Substitution.
- Beschränkungen der Prädikatenlogik.
- Semantik: Bedeutung eines Satzes (in einer konkreten Struktur), Begriff der semantischen Folgerung.
- Kalkül: Ableitungs- bzw. Beweissystem (syntaktisch, d.h. Manipulation von Zeichenketten), Begriff der formalen Ableitbarkeit bzw. Beweisbarkeit.
- Vollständigkeitssatz: Semantischen Folgerung und formalen Ableitbarkeit ist das selbe.
- Folgerungen: Kompaktheitssatz, nonstandard Modelle, Unvollständigkeitssatz.

Syntax der Prädikatenlogik: $\mathcal{L}$

$\mathcal{L}$

Fixiere eine Menge $\mathcal{L}$ von Konstanten-, Relations- und Funktionssymbolen (mit Stelligkeiten).

Bsp: $\mathcal{L}$ besteht aus:
den Konstantenssymbolen $0, 1$,
den Funktionssymbolen $+, \cdot$ (2-stellig) und ln (1-stellig), und
dem Relationssymbol $<$ (2-stellig).
Kurz (aber unexakt): $\mathcal{L} = \{0, 1, +, \cdot, \ln, <\}$.

Wichtige andere Sprachen:

Beispiele für $\mathcal{L}$

- Gruppentheorie: $\mathcal{L} = \{e, \cdot\}$,
- Ordnung: $\mathcal{L} = \{<\}$,
- Mengenlehre: $\mathcal{L} = \{\in\}$,
- Elementare reelle Algebra: $\mathcal{L} = \{0, 1, +, \cdot, <\}$.

Syntax der Prädikatenlogik: Terme

Terme

Die Menge der $\mathcal{L}$-Terme ist induktiv definiert:

- Ein Variablensymbol x_i ($i \in \mathbb{N}$) ist ein $\mathcal{L}$-Term.
- Jedes $\mathcal{L}$-Konstantensymbol ist ein $\mathcal{L}$-Term.
- Wenn $t_1, \dots t_n$ $\mathcal{L}$-Terme sind und f ein n-stelliges $\mathcal{L}$-Funktionssymbol, dann ist $f(t_1, \dots t_n)$ ein $\mathcal{L}$-Term.

Bsp:

- $\mathcal{L} = \{e, \cdot\}$: $e \cdot e$ und $x_0 \cdot x_1$ sind Terme.
  Eigentlich: $\cdot(e, e)$ etc.
- $\mathcal{L} = \{\in\}$ oder $\{<\}$: Nur die x_i sind Terme.
- $\mathcal{L} = \{0, 1, +, \cdot, <\}$: $x_1 \cdot x_2 + (1 + 1 + 1) \cdot x_3$ und $1 + 1$ sind Terme.

Syntax der Prädikatenlogik: Formeln

Formeln

Die Menge der $\mathcal{L}$-Formeln ist induktiv definiert:

- Atomformeln:
  - Wenn t_1 und t_2 $\mathcal{L}$-Terme sind, dann ist $t_1 = t_2$ eine $\mathcal{L}$-Formel.
  - Wenn $t_1, \dots t_n$ $\mathcal{L}$-Terme sind und R ein n-stelliges $\mathcal{L}$-Relationssymbol, dann ist $R(t_1, \dots t_n)$ eine $\mathcal{L}$-Formel.
- Abschluß unter Aussagenlogischen Junktoren:
  Wenn φ und ψ $\mathcal{L}$-Formeln sind, dann auch $\neg\varphi$, $(\varphi \vee \psi)$, $(\varphi \wedge \psi)$ und $(\varphi \rightarrow \psi)$.
- Abschluß unter Quantifikation:
  Sei $i \in \mathbb{N}$. Wenn φ eine $\mathcal{L}$-Formel ist, dann auch $(\forall x_i \varphi)$ und $(\exists x_i \varphi)$.

Syntax der Prädikatenlogik: Beispiele für Formeln

- $\mathcal{L} = \{e, \cdot\}$: $e \cdot x = y$ ist Atomformel. $\forall x\, e \cdot x = y$ ist Formel.
- $\mathcal{L} = \{\in\}$: $x \in y$ ist Atomformel. $\exists x\, \forall y\, \neg x \in y$ ist Formel.
- $\mathcal{L} = \{<\}$: $x < y$ ist Atomformel. $\exists x\, \forall y\, \neg x < y$ ist Formel.
- $\mathcal{L} = \{0, 1, +, \cdot, <\}$: $x > 0$ und $y \cdot y = x$ sind Atomformeln.
  $\forall x\, (x > 0 \rightarrow (\exists y\, y \cdot y = x))$ ist Formel.

Freie und gebundene Variablen: Beispiele

Beispiele für freie und gebundene Variablen:

- In $f(x) > 1$ ist x eine freie Variable.
- In $\forall x(f(x) > 1)$ ist x eine gebundene Variable.
- In $g(x) = 1 \wedge (\forall x(f(x) > 1))$ tritt x zuerst frei, dann gebunden auf.

Also exakter: Nich freie/gebundene Variable, sondern freies/gebundenes Vorkommnis eine Variable.

Freie und gebundene Variablen: Definition

Freie und Gebundene Variablen

Ein Vorkommnis vom Variablensymbol v in der Formel φ heißt frei, wenn

- φ ist Atomformel, oder
- φ ist $\psi_1 \vee \psi_2$ und das entsprechende Vorkommnis von v in ψ_1 (bzw. ψ_2) ist frei, oder
- die analoge Situation für $\neg, \wedge, \rightarrow$, oder
- φ ist $(\exists w \psi)$ und $v \neq w$ und das entsprechende Vorkommnis von v in ψ ist frei.

Andernfalls ist das Vorkommnis von v gebunden.

Wir interessieren uns eigentlich nur für Formeln ohne freie Variable:

Satz

Eine Formel ohne freie Vorkommnisse von Variablen heißt Satz.

Freie und gebunden Variablen: Substitution

Substitution

Wenn v ein Variablensymbol, t ein Term und φ eine Formel ist, dann ist $\varphi[v \mapsto t]$ die Formel, die entsteht wenn man alle freien Vorkommnisse von v durch t ersetzt.

Beispiel: φ sei $x + 1 > y \wedge \exists x(x < y)$.
In φ kommen also x und y frei vor.
Beispiele für $\varphi[v \mapsto t]$:

v	t	$\varphi[v \mapsto t]$
x	0	$0 + 1 > y \wedge \exists x(x < y)$
y	0	$x + 1 > 0 \wedge \exists x(x < 0)$
y	x	$x + 1 > x \wedge \exists x(x < x)$ (Problem!)

Es kann Probleme machen, wenn der substituierte Term eine Variable enthält, die im Ergebnis gebunden ist.
Wenn der substituierte Term ein Konstantensymbol ist, gibt es solche Probleme nicht.

Syntaktische Abkürzungen

Wir verwenden einige Abkürzungen:

- $\varphi \leftrightarrow \psi$ steht für $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.
- $t_1 \neq t_2$ steht für $\neg t_1 = t_2$
- Klammern werden oft weggelassen, wenn Eindeutigkeit garantiert ist.
- Bei manchen 2stelligen Funktionssymbolen schreiben wir $t_1\, f\, t_2$ statt $f(t_1, t_2)$, z.B. $x_0 + x_2$ statt $+(x_0, x_2)$.
- Wir verwenden manchmal andere Variablensymbole, z.B. x, y, z statt x_0, x_1, x_2.
- $(\forall x < t)\varphi$ steht für $\forall x(x < t \rightarrow \varphi)$, und analog für andere 2stellige Relationssymbole (z.B. $\in$).
- $(\exists x < t)\varphi$ steht für $\exists x(x < t \wedge \varphi)$ etc.
- Eine Formel wird manchmal als $\varphi(x)$ geschrieben. Das betont daß x frei in φ vorkommen kann. $\varphi(t)$ bezeichnet dann $\varphi[x \mapsto t]$.
  Beispiel: $\varphi(x)$ ist $x < 2 \wedge x > y$. Dann ist $\varphi(0)$ die Zeichenkette $0 < 2 \wedge 0 > y$.
- $(\exists! x)\varphi(x)$ steht für: $\exists x(\varphi(x) \wedge (\forall y(\varphi(y) \rightarrow y = x)))$.
  D.h.: Es gibt genau ein x mit $\varphi(x)$.

Semantik: Einfache Beispiele

Bevor wir die Semantik (Bedeutung) eines Satzes definieren, einige Beispiele:

Sei $\mathcal{L} = \{e, \cdot\}$ (Sprache der Gruppentheorie.)

Sowohl $\mathcal{N} = (\mathbb{N}, +, 0)$ als auch $\mathcal{Z} = (\mathbb{Z}, +, 0)$ sind $\mathcal{L}$-Strukturen.

Der Satz $\forall x\, \exists y\; x \cdot y = e$ ist wahr in $\mathcal{Z}$, aber nicht in $\mathcal{N}$. $(\mathbb{Z}, +, 0)$ erfüllt dieses Gruppenaxiom, aber $(\mathbb{N}, +, 0)$ nicht. (Das inverse zu 1, -1, liegt nicht in $\mathbb{N}$.)

Es gibt also eine Grundmenge (Universum), und die Quantoren $\forall$ und $\exists$ erstrecken sich über Elemente des Universums.

Der Satz "Das Universum ist eine Gruppe" ist der Satz AG$\wedge$NE$\wedge$Inv, wobei
AG: $\forall x\, \forall y\, \forall z\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
NE: $\forall x\, (x \cdot e = x \ \wedge\ e \cdot x = x)$
Inv: $\forall x\, \exists y\, (x \cdot y = e \ \wedge\ y \cdot x = e)$

Wir können also in der Prädikatenlogik formulieren, daß das Universum eine Gruppe ist.

Beschränkungen der Prädikatenlogik

Bevor wir die Semantik exakt definieren, noch einige wichtige Einschränkungen der Prädikatenlogik:

Sei $\mathcal{L} = \{e, \cdot\}$.

- $\exists x_0 \, \exists x_1 \; x_0 \neq x_1$ besagt: Das Universum hat mindestens 2 Elemente.
- Genauso gibt es Sätze, die besagen daß das Universum mindestens n Elemente hat.
- Es gibt also eine unendliche Satzmenge, die besagt: “Das Universum ist unendlich.” Es gibt aber keinen einzelnen Satz, der das besagt.
- Es gibt einen Satz, der besagt: “Das Universum hat 2 Elemente,” nämlich $\exists x_0 \, \exists x_1 \, (x_0 \neq x_1 \; \wedge \forall y \, (y = x_0 \vee y = x_1))$.
- Es gibt keine Satzmenge, die besagt “Das Universum ist endlich.” (Das wird aus dem Kompaktheitssatz folgen.)
- $(\forall x \neq e) \, x \cdot x \neq e$ sagt: e ist kein Quadrat.
- Es gibt also eine Satzmenge, die besagt “Das Universum ist torsionsfrei”. Es gibt aber keinen einzelnen Satz, der das besagt.
- Keine Satzmenge sagt daß G nichttrivialen Normalteiler hat (das benötigt Quantor über Teilmengen von G).

Beschränkungen der Prädikatenlogik: Auswege

Man kann natürlich Quantoren über Teilmengen des Universums in die Sprache aufnehmen. Das führt zur Sprache zweiter Stufe.

Diese Sprache ist enorm mächtig, hat aber keine effektive (r.e.) Axiomatisierung, daher erfüllt sie nicht die eigentliche Grundaufgabe der Logik in der Mathematik.

Anderer Ausweg: Die Sprache der Mengenlehre $\mathcal{L} = \{\in\}$ erlaubt es, diese Beschränkungen zu umgehen.

Semantik der Prädikatenlogik: $\mathcal{L}$-Strukturen

Eine $\mathcal{L}$-Struktur $\mathcal{M}$

Eine $\mathcal{L}$-Struktur $\mathcal{M}$ besteht aus einer Grundmenge (Universum) M zusammen mit:

- Für jedes Konstantensymbol c ein Element $c^{\mathcal{M}}$,
- Für jedes n-stelliges Funktionssymbol f eine Funktion $f^{\mathcal{M}} : M^n \to M$,
- Für jedes n-stelliges Relationssymbol R eine Relation $R^{\mathcal{M}} \subseteq M^n$.

Beispiele:

- $(\mathbb{Z}, 0, +)$ ist eine $\{e, \cdot\}$-Struktur.
- $(\mathbb{N}, 0, \cdot)$ ist eine $\{e, \cdot\}$-Struktur.
- $(\mathbb{Z}, <)$ ist eine $\{<\}$-Struktur.
- $(\mathbb{Q}, <)$ ist eine $\{<\}$-Struktur.
- $(\mathbb{Q}, <)$ ist eine $\{\in\}$-Struktur.
- $(\mathbb{R}, 0, 1, +, \cdot, <)$ ist eine $\{0, 1, +, \cdot, <\}$-Struktur.

Semantik der Prädikatenlogik: $(\mathcal{L}, \mathcal{M})$-Formeln

$(\mathcal{L}, \mathcal{M})$-Formeln

Sei $\mathcal{M}$ eine $\mathcal{L}$-Struktur. Eine $(\mathcal{L}, \mathcal{M})$-Formel ist eine Formel der Sprache $\mathcal{L}$ mit zusätzlich allen Elementen von M als Konstanten.

Beispiele:

- $\mathcal{L} = \{e, \cdot\}$, $\mathcal{M} = (\mathbb{Z}, 0, +)$. Eine $(\mathcal{L}, \mathcal{M})$-Formel ist z.B. $\exists x(x \cdot -3 = e)$.
  Das Element $-3 \in \mathbb{Z}$ ist ein neues Konstantensymbol!
- $\mathcal{L} = \{<\}$, $\mathcal{M} = (\mathbb{Q}, <)$. $\frac{3}{4} < x$ ist eine $(\mathcal{L}, \mathcal{M})$-Formel.
- $\mathcal{L} = \{0, 1, +, \cdot, <\}$, $\mathcal{M} = (\mathbb{R}, 0, 1, +, \cdot, <)$. Eine $(\mathcal{L}, \mathcal{M})$-Formel ist z.B.
  $\forall x_0(x_0 > \sqrt{3} \rightarrow x_0 > e)$.
  (Das Element $\sqrt{3} \in \mathbb{R}$ ist ein neues Konstantensymbol.)

$(\mathcal{L}, \mathcal{M})$-Satz

Ein $(\mathcal{L}, \mathcal{M})$-Satz ist eine $(\mathcal{L}, \mathcal{M})$-Formel ohne freie Variable.

Semantik der Prädikatenlogik: Term-Auswertung

Terme

Wenn t ein $(\mathcal{L}, \mathcal{M})$-Term ohne Variablen ist, dann ist $t^{\mathcal{M}} \in M$ folgendermaßen induktiv definiert:

- Wenn t ein Konstantensymbol c ist, dann ist $t^{\mathcal{M}} = c^{\mathcal{M}}$.
- Wenn t die Form $f(t_1, \ldots, t_n)$ hat, dann ist $t^{\mathcal{M}} = f^{\mathcal{M}}(t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}})$.