Logik & Semantik
8. Vorlesung
Prädikatenlogik – 2

Uniforme Notation: Quantoren
- Expansionsmöglichkeiten (Korrektheit)

Konsistente Formelmengen (Vollständigkeit)
- Hintikka-Mengen
- Erfüllbarkeit in Herbrand-Modellen

Weiteres

Definition eines logischen Systems: Generelles Schema

Spezifikation

- einer formalen Sprache (zur Repräsentation)
- von Evaluations- / Interpretationsprinzipien
- semantischer Kategorisierungen und Beziehungen
- Ableitungs-, Beweisverfahren
  - Ziel: Tableau-Verfahren

Vorgehen

Ziel

- Spezifikation eines Tableau-Verfahrens für Prädikatenlogik
  - Regeln, Korrektheit, Vollständigkeit

Vorarbeiten (in Analogie zur Aussagenlogik)

- Uniforme Notation für quantifizierte Formeln
- Korrektheit: Erweiterungsmöglichkeiten für Formelmengen unter Erhalt der Erfüllbarkeit
- Vollständigkeit: prädikatenlogische Hintikka-Mengen, Beweis ihrer Erfüllbarkeit, dazu Definition von Herbrandmodellen
- Unentscheidbarkeit der Prädikatenlogik

Tableau-Verfahren

Uniforme Notation – Quantifikation

Zwei Typen quantifizierter Formeln γ bzw. δ

- Für beliebige Variablen *v*, Formeln Φ und für jeden beliebigen Term *t* gilt folgende Klassifikation und sind *Instanzen* $\gamma(t)$ bzw $\delta(t)$ definiert.

Universell		Existentiell (Partikular)	
γ	$\gamma(t)$	δ	$\delta(t)$
$(\forall v)\ \Phi$	$\Phi\{v / t\}$	$(\exists v)\ \Phi$	$\Phi\{v / t\}$
$\neg(\exists v)\ \Phi$	$\neg\Phi\{v / t\}$	$\neg(\forall v)\ \Phi$	$\neg\Phi\{v / t\}$
quantifizierte Formel	Instanz	quantifizierte Formel	Instanz

- Die Uniforme Notation zur Quantifikation liefert nicht eindeutige Komponenten der Formel, sondern beliebig viele (sogar unendlich viele) Instanzen.
- Die Instanzen bei der universellen und der existentiellen Quantifikation unterscheiden sich syntaktisch nicht. Der Unterschied liegt in der Nutzung der Instanzen.

Uniforme Notation – Quantifikation (2)

Universell		Existentiell (Partikular)	
γ	$\gamma(t)$	δ	$\delta(t)$
$(\forall v)\ \Phi$	$\Phi\{v\ /\ t\}$	$(\exists v)\ \Phi$	$\Phi\{v\ /\ t\}$
$\neg(\exists v)\ \Phi$	$\neg\Phi\{v\ /\ t\}$	$\neg(\forall v)\ \Phi$	$\neg\Phi\{v\ /\ t\}$
quantifizierte Formel	Instanz	quantifizierte Formel	Instanz

Beispiele

$(\forall x)\ \mathrm{P}(x)$	$\mathrm{P(c)}$	$(\exists x)\ \mathrm{P}(x)$	$\mathrm{P(c)}$
$(\forall x)\ \mathrm{P(c)}$	$\mathrm{P(c)}$	$\neg(\forall x)\ \neg\mathrm{P}(x)$	$\neg\neg\mathrm{P(c)}$
$\neg(\exists y)\ (\forall x)\ \mathrm{R}(x, y)$	$\neg(\forall x)\ \mathrm{R}(x, \mathrm{c})$	$\neg(\forall x)\ \mathrm{R}(x, \mathrm{f(d)})$	$\neg\mathrm{R(c, f(d))}$

Uniforme Notation – Quantifikation (3)

- Wenn die Variable y nicht in γ bzw. δ vorkommt, dann
  - sind die Formeln γ und $(\forall y)\ \gamma(y)$ äquivalent,
  - ist $\gamma(t) = \gamma(y)\{y / t\}$,
  - sind die Formeln δ und $(\exists y)\ \delta(y)$ äquivalent,
  - ist $\delta(t) = \delta(y)\{y / t\}$.

Universell		Existentiell (Partikular)	
γ	$\gamma(t)$	δ	$\delta(t)$
$(\forall v)\ \Phi$	$\Phi\{v / t\}$	$(\exists v)\ \Phi$	$\Phi\{v / t\}$
$\neg(\exists v)\ \Phi$	$\neg\Phi\{v / t\}$	$\neg(\forall v)\ \Phi$	$\neg\Phi\{v / t\}$
quantifizierte Formel	Instanz	quantifizierte Formel	Instanz

Uniforme Notation – Quantifikation (4)

Beispiele

- Wenn die Variable y nicht in γ bzw. δ vorkommt, dann
  - $\gamma = (\forall v)\ \Phi$ und $(\forall y)\ \Phi\{v / y\} = (\forall y)\ \gamma(y)$ sind wegen der gebundenen Umbenennung äquivalent,
  - $\gamma(t) = \Phi\{v / t\} = \Phi\{v / y\}\ \{y / t\} = \gamma(y)\{y / t\}$

Universell		Existentiell (Partikular)	
γ	$\gamma(t)$	δ	$\delta(t)$
$(\forall v)\ \Phi$	$\Phi\{v / t\}$	$(\exists v)\ \Phi$	$\Phi\{v / t\}$
$\neg(\exists v)\ \Phi$	$\neg\Phi\{v / t\}$	$\neg(\forall v)\ \Phi$	$\neg\Phi\{v / t\}$
quantifizierte Formel	Instanz	quantifizierte Formel	Instanz

- Wenn die Variable y nicht in γ bzw. δ vorkommt, dann
  - $\gamma = (\forall v)\ \Phi$ und $(\forall y)\ \Phi\{v / y\} = (\forall y)\ \gamma(y)$ sind wegen der gebundenen Umbenennung äquivalent,
  - $\gamma = \neg(\exists v)\ \Phi$ und $(\forall y)\ \neg\Phi\{v / y\} = (\forall y)\ \gamma(y)$ sind wegen der gebundenen Umbenennung und der Dualität der Quantoren äquivalent,
  - $\gamma(t) = \Phi\{v / t\} = \Phi\{v / y\}\ \{y / t\} = \gamma(y)\{y / t\}$
  - $\gamma(t) = \neg\Phi\{v / t\} = \neg\Phi\{v / y\}\ \{y / t\} = \gamma(y)\{y / t\}$
  - $\delta = (\exists v)\ \Phi$ und $(\exists y)\ \Phi\{v / y\} = (\exists y)\ \delta(y)$ sind wegen der gebundenen Umbenennung äquivalent,
  - $\delta = \neg(\forall v)\ \Phi$ und $(\exists y)\ \neg\Phi\{v / y\} = (\exists y)\ \delta(y)$ sind wegen der gebundenen Umbenennung und der Dualität der Quantoren äquivalent,
  - $\delta(t) = \Phi\{v / t\} = \Phi\{v / y\}\ \{y / t\} = \delta(y)\{y / t\}$
  - $\delta(t) = \neg\Phi\{v / t\} = \neg\Phi\{v / y\}\ \{y / t\} = \delta(y)\{y / t\}$

Prinzip der Strukturellen Induktion [UN, Prädikatenlogik]

Theorem 5.5.3

Eine Eigenschaft ***Q*** gilt für alle Formeln der Prädikatenlogik gdw. gilt:

- Induktionsbasis$_{UN}$
  Jede atomare Formel X und deren Negation besitzen die Eigenschaft ***Q***.
- Induktionsschritte$_{UN}$
  - Falls Z die Eigenschaft ***Q*** hat, dann hat auch $\neg\neg Z$.
  - Falls α_1 und α_2 die Eigenschaft ***Q*** haben, dann auch α.
  - Falls β_1 und β_2 die Eigenschaft ***Q*** haben, dann auch β.
  - Wenn für jeden Term t die Formel $\gamma(t)$ die Eigenschaft ***Q*** besitzt, dann auch γ.
  - Wenn für jeden Term t die Formel $\delta(t)$ die Eigenschaft ***Q*** besitzt, dann auch δ.

Prinzip der Strukturellen Rekursion [UN, Prädikatenlogik]

Theorem

Es existiert genau eine Funktion f definiert über der Menge aller Formeln von $\mathcal{L}_{PL}$, so dass gilt:

- Rekursionsbasis$_{UN}$
  Der Wert von f ist explizit spezifiziert auf den atomaren Formeln und ihren Negationen.
- Rekursionsschritt$_{UN}$
  - Der Wert $f(\neg\neg X)$ ist spezifiziert über den Wert von f bzgl. X.
  - Der Wert $f(\alpha)$ ist spezifiziert über $f(\alpha_1)$ und $f(\alpha_2)$.
  - Der Wert $f(\beta)$ ist spezifiziert über $f(\beta_1)$ und $f(\beta_2)$.
  - Der Wert $f(\gamma)$ ist spezifiziert über Werte von $f(\gamma(t))$.
  - Der Wert $f(\delta)$ ist spezifiziert über Werte von $f(\delta(t))$.

- Der Wert $f(\gamma)$ ist spezifiziert über Werte von $f(\gamma(t))$.
- Der Wert $f(\delta)$ ist spezifiziert über Werte von $f(\delta(t))$.

- Diese Spezifikation kann beinhalten, dass der Term t variiert wird, d.h. verschiedene oder sogar alle Instanzen berücksichtigt werden.

Uniforme Notation – Erfüllbarkeit mit γ- und δ-Formeln

Satz 5.5.1

Sei ***S*** eine Menge von geschlossenen Formeln und γ und δ ebenfalls geschlossene Formeln. Weiterhin sei
t ein (beliebiger) geschlossener Term und
p eine Konstante, die nicht in ***S*** oder δ vorkommt.
Dann gilt:

1. Falls ***S*** ∪ {γ} erfüllbar ist, so ist ***S*** ∪ {γ, γ(*t*)} erfüllbar.
2. Falls ***S*** ∪ {δ} erfüllbar ist, so ist ***S*** ∪ {δ, δ(*p*)} erfüllbar.

γ	γ(*t*)	δ	δ(*p*)
(∀*v*) Φ	Φ{*v* / *t*}	(∃*v*) Φ	Φ{*v* / *p*}
¬(∃*v*) Φ	¬Φ{*v* / *t*}	¬(∀*v*) Φ	¬Φ{*v* / *p*}

- Der zweite Teil des Satzes stellt den semantischen Sachverhalt dar, der die Skolemisierung rechtfertigt.

- Dieser Satz zielt natürlich auf das prädikatenlogische Tableau-Verfahren ab. Hiermit kann man sich vielleicht auch schon vorstellen, wie es aussehen wird.

- Aufgabe (ohne Nummer)
- Formulieren Sie Tableau-Expansionsregeln für quantifizierte Formeln unter Berücksichtigung der Bedingungen dieses Satzes. Schlagen Sie erst danach im entsprechenden Kapitel nach, wie die Regel lauten und vergleichen Sie Ihren Vorschlag damit.

Uniforme Notation – Beweis von Satz 5.5.1

Teil 1: Falls $\boldsymbol{S} \cup \{\gamma\}$ erfüllbar ist, so ist $\boldsymbol{S} \cup \{\gamma, \gamma(t)\}$ erfüllbar.

Angenommen $\boldsymbol{S} \cup \{ \gamma \}$ ist erfüllbar in $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$.

Wir zeigen, dass dann $\mathcal{M}$ auch $\gamma(t)$ wahr macht.

- Es sei x eine Variable, die nicht in γ vorkommt.
- Dann ist γ äquivalent zu $(\forall x)\ \gamma(x)$ und $\gamma(t) = \gamma(x)\{ x / t \}$.
- Da $(\forall x)\ \gamma(x)$ in $\mathcal{M}$ erfüllbar und geschlossen ist, ist $(\forall x)\ \gamma(x)$ auch wahr in $\mathcal{M}$ [Lemma, Fol. 7-27]
- Deswegen: $[\gamma(x)]^{\mathcal{I},\mathcal{A}} = \mathbf{t}$ für alle Zuweisungen $\mathcal{A}$ in $\mathcal{M}$. [Def.]
- Sei $\mathcal{A}$ eine Zuweisung in $\mathcal{M}$ mit $x^{\mathcal{A}} = t^{\mathcal{I}}$.

  Dann gilt: $[\gamma(t)]^{\mathcal{I},\mathcal{A}} = [\gamma(x)\{ x / t \}]^{\mathcal{I},\mathcal{A}} = [\gamma(x)]^{\mathcal{I},\mathcal{A}} = \mathbf{t}$ [Satz 5.3.7; Überf.]

Also:

$$\boldsymbol{S} \cup \{\gamma, \gamma(t)\} \text{ erfüllbar in } \mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle.$$

Uniforme Notation – Beweis von Satz 5.5.1 (Forts.)

Teil 2: Falls $\boldsymbol{S} \cup \{\delta\}$ erfüllbar ist, so ist $\boldsymbol{S} \cup \{\delta, \delta(p)\}$ erfüllbar.

Angenommen $\boldsymbol{S} \cup \{\delta\}$ ist erfüllbar in $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$ und p ist eine Konstante, die nicht in $\boldsymbol{S}$ und δ vorkommt.

- Es sei x eine Variable, die nicht in δ vorkommt.
- Dann ist δ äquivalent zu $(\exists x)\ \delta(x)$ und $\delta(p) = \delta(x)\{ x / p \}$.
- Da $(\exists x)\ \delta(x)$ erfüllbar in $\mathcal{M}$ ist, gibt es eine Zuweisung $\mathcal{A}$ in $\mathcal{M}$, so dass $[\delta(x)]^{\mathcal{I},\mathcal{A}} = \mathbf{t}$.
- Wir bilden ein neues Modell: $\mathcal{M}^* = \langle \mathcal{D}, \mathcal{J} \rangle$
  $\mathcal{J}$ und $\mathcal{I}$ stimmen überein, mit Ausnahme von $p^{\mathcal{J}} = \mathcal{J}(p) := x^{\mathcal{A}}$
- Formeln ohne p verhalten sich in $\mathcal{M}$ und $\mathcal{M}^*$ gleich.
- Daher ist $\boldsymbol{S} \cup \{\delta\}$ erfüllbar in $\mathcal{M}^*$ und $[\delta(x)]^{\mathcal{J},\mathcal{A}} = \mathbf{t}$.
- Wegen $x^{\mathcal{A}} = p^{\mathcal{J}}$ gilt:
  $[\delta(p)]^{\mathcal{J},\mathcal{A}} = [\delta(x)\{x/p\}]^{\mathcal{J},\mathcal{A}} = [\delta(x)]^{\mathcal{J},\mathcal{A}} = [\delta(x)]^{\mathcal{I},\mathcal{A}} = \mathbf{t}$

Also: $\boldsymbol{S} \cup \{\delta, \delta(p)\}$ erfüllbar in $\mathcal{M}^* = \langle \mathcal{D}, \mathcal{J} \rangle$.

- Ein neues Modell wird gebildet, denn wir können nicht davon ausgehen, dass $x^{\mathcal{A}} = p^{\mathcal{I}}$.

- Erfüllung ist gesichert, aber nicht unbedingt im gleichen Modell.
- Entsprechendes gilt für Erfüllbarkeit und Skolemisierung.

- man beachte: $(\exists x)\ \delta(x)$ ist genau dann erfüllbar in $\mathcal{M}$, wenn $\delta(x)$ in $\mathcal{M}$ erfüllbar ist.

Nutzbarkeit von Satz 5.5.1

Die Voraussetzungen besagen

- *p* eine Konstante, die nicht in ***S*** oder δ vorkommt

Tableau-Expansion könnte eine entsprechende Bedingung stellen !

- Was, wenn es keine entsprechende Konstante gibt?

Spracherweiterungen sind zulässig !

- denn es gilt allgemein: Wenn es zwei prädikatenlogische Sprachen $\mathcal{L}_{PL}$ und $\mathcal{L}'_{PL}$ gibt (die nur in den verfügbaren Symbolen voneinander abweichen), so dass $\boldsymbol{S} \subset \mathcal{L}_{PL}$ und $\boldsymbol{S} \subset \mathcal{L}'_{PL}$, dann ist die Erfüllbarkeit von ***S*** unabhängig von der Zuordnung zu einer der beiden Sprachen.

- Entsprechendes gilt dann natürlich für Gültigkeit, Falsifizierbarkeit, Äquivalenz, Folgerung.

Parameter – Die Einführung neuer Konstanten

Definition (5.7.2)

Sei $\mathcal{L}_{PL}$ eine prädikatenlogische Sprache. Und sei **par** eine abzählbare Menge von Konstanten, die disjunkt ist zu $\mathcal{Kon}(\mathcal{L}_{PL})$. Wir nennen die Elemente von **par** *Parameter*.

$\mathcal{L}_{PL}(\boldsymbol{R}, \boldsymbol{F}, \boldsymbol{C})^{\mathbf{par}} := \mathcal{L}_{PL}(\boldsymbol{R}, \boldsymbol{F}, \boldsymbol{C} \cup \mathbf{par})$

also: $\mathcal{Kon}(\mathcal{L}_{PL}{}^{\mathbf{par}}) = \mathcal{Kon}(\mathcal{L}_{PL}) \cup \mathbf{par}$

$\mathcal{Fun}_n(\mathcal{L}_{PL}{}^{\mathbf{par}}) = \mathcal{Fun}_n(\mathcal{L}_{PL})$ $\qquad \mathcal{Rel}_n(\mathcal{L}_{PL}{}^{\mathbf{par}}) = \mathcal{Rel}_n(\mathcal{L}_{PL})$

$\mathcal{Var}(\mathcal{L}_{PL}{}^{\mathbf{par}}) = \mathcal{Var}(\mathcal{L}_{PL})$

$\mathcal{L}_P{}^{\mathbf{par}}$ ist eine Spracherweiterung zu $\mathcal{L}_{PL}$:

$\mathcal{Ter}(\mathcal{L}_{PL}) \subseteq \mathcal{Ter}(\mathcal{L}_{PL}{}^{\mathbf{par}})$ $\qquad \mathcal{For}(\mathcal{L}_{PL}) \subseteq \mathcal{For}(\mathcal{L}_{PL}{}^{\mathbf{par}})$

- Parameter entsprechen einer weitverbreiteten und bewährten Praxis der mathematischen Sprache.
  Sie treten in Wendungen der Art auf:
  „Sei k eine Entität mit der Eigenschaft Φ."
  Was für Entitäten sind das aber?
- Wir betrachten das an einem Beispiel: Wenn wir formulieren
  „Sei p eine natürliche Zahl mit der Eigenschaft,
  eine Primzahl zu sein und ausserdem gerade zu sein."

  so wollen wir vermutlich gerade nicht die Konstante 2 verwenden, denn der Zweck der ganzen Angelegenheit ist vermutlich, zu zeigen, dass es nur eine Zahl mit dieser Eigenschaft gibt.

Also ist es nicht zweckmässig p als Konstante aus *C*, der Menge der Konstanten anzusehen. Andererseits ist es auch keine Variable, denn diese würde syntaktisch und semantisch anders behandelt werden. Es ist eben genau das, was hinter der Idee der Parameter steckt, eine *neue Konstante*.

Vorgehen

Ziel

- Spezifikation eines Tableau-Verfahrens für Prädikatenlogik
  - Regeln, Korrektheit, Vollständigkeit

Vorarbeiten (in Analogie zur Aussagenlogik)

- Uniforme Notation für quantifizierte Formeln
- Korrektheit: Erweiterungsmöglichkeiten für Formelmengen unter Erhalt der Erfüllbarkeit
- Vollständigkeit: prädikatenlogische Hintikka-Mengen, Beweis ihrer Erfüllbarkeit, dazu Definition von Herbrandmodellen
- Unentscheidbarkeit der Prädikatenlogik

Tableau-Verfahren

Prädikatenlogische Hintikka-Mengen

Definition 5.6.1 (*Hintikka-Menge*)

Eine Menge ***H*** von geschlossenen Formeln aus $\mathcal{L}_{PL}$ (mit mindestens einer Konstanten) heißt prädikatenlogische *Hintikka-Menge* bzgl. $\mathcal{L}_{PL}$, falls gilt:

- ***H*** ist eine aussagenlogische Hintikka-Menge (Def. 3.5.1) und

- Falls $\gamma \in H$,
  dann $\gamma(t) \in H$ für alle geschlossenen Terme t in $\mathcal{L}_{PL}$.
- Falls $\delta \in H$,
  dann $\delta(t) \in H$ für mindestens einen geschlossenen Term t in $\mathcal{L}_{PL}$.

- Vgl. Ben-Ari (2001), Def. 5.31

- Falls $\mathcal{L}_{PL}$ eine nicht-endliche Menge geschlossener Terme besitzt, dann sind alle Hintikka-Mengen zu $\mathcal{L}_{PL}$, die eine γ-Formel enthalten, nicht endlich.
- Wenn $\mathcal{L}_{PL}$ eine Konstante und ein Funktionssymbol besitzt, dann gibt es in $\mathcal{L}_{PL}$ eine nicht-endliche Menge geschlossener Terme.

Unendliche Hintikka-Mengen

Lemma

Es gibt erfüllbare Formeln der Prädikatenlogik, so dass jede Hintikka-Menge, in der sie enthalten sind, unendlich ist.

Beweisskizze

- Betrachte die Formel $F = A_1 \wedge A_2 \wedge A_3$, mit

$A_1 = (\forall x)\ (\exists y)\ P(x, y)$

$A_2 = (\forall x)\ \neg P(x, x)$

$A_3 = (\forall x)\ (\forall y)\ (\forall z)\ ((P(x, y) \wedge P(y, z)) \supset P(x, z))$

- Es sei M eine Hintikka Menge, die F enthält. Dann enthält M auch A1, A2, A3.
- Für Hintikka-Mengen war vorausgesetzt, dass die Bezugssprache mindestens eine Konstante enthält.
- Ausgehend von einer Konstanten t1 führt die Anwesenheit von A2 in M dazu, dass es eine unendliche Folge von Termen t1 .. ti .. gibt, so dass jeweils P(ti, ti+1) in M enthalten sind. (Jetzt ist noch zu zeigen, dass es in dieser Folge keine Wiederholungen oder Schleifen gibt.)
- Die Anwesenheit von A3 in M führt weiter dazu, dass auch für jedes n > 0 P(ti, ti+n) in M enthalten ist.
- Dagegen führt die Anwesenheit von A2 in M dazu, dass alle ¬P(ti, ti) in M enthalten sind.
- Aufgrund der Konsistenzbedingung kann damit für keinen Term P(ti, ti) in M enthalten sein (Also: wenn i ≠ j, dann auch ti ≠ tj) und deshalb kann auch kein Term mehrfach in der Folge von Termen auftauchen.
- Also ist M unendlich.

Prädikatenlogisches Hintikka-Lemma

Satz 5.6.2* (*Hintikka-Lemma*)

Sei $\mathcal{L}_{PL}$ eine prädikatenlogische Sprache mit einer nicht-leeren Menge von geschlossenen Termen.

Falls ***H*** eine prädikatenlogische Hintikka-Menge bzgl. $\mathcal{L}_{PL}$ ist, so ist ***H*** erfüllbar.

Spezialisierung

- Dieser Satz kann sogar noch spezieller gefasst werden: unter den gegebenen Voraussetzungen gibt es nicht nur irgendein Modell, in dem ***H*** erfüllt wird, sondern es gibt ein Herbrand-Modell.

- Ben-Ari (2001) Lemma 5.33
- Eine Sprache mit leerer Menge geschlossener Terme kann z.B. dann auftreten, wenn in $\mathcal{L}_{PL}$ keine Konstante existiert.

Herbrand-Modelle

Motivation

- Eine prädikatenlogische Formel ist erfüllbar, wenn es eine Interpretation gibt, die sie wahr macht.
- Zu jeder logischen Sprache gibt es unendlich viele unterschiedliche Interpretationen.
- Wie kann es in systematischer Weise gelingen, zu zeigen, dass es keine Interpretation gibt, die die Formel wahr macht?
- Wie kann man (unter Berücksichtigung der Formel) systematisch eine Interpretation spezifizieren, die die Formel wahr macht?

Herbrands Idee

- Standardisierte Modelle auf Basis der Terme der Logiksprache, bei Bedarf Ergänzung um weitere Konstanten (Parameter)

Definition eines logischen Systems: Generelles Schema

Spezifikation

- einer formalen Sprache (zur Repräsentation)
- von Evaluations- / Interpretationsprinzipien
  - Herbrand-Modelle
- semantischer Kategorisierungen und Beziehungen
  - Herbrand-Theorem: Jede erfüllbare Formelmenge ist in einem Herbrand-Modell erfüllbar
- Ableitungs-, Beweisverfahren

Zuweisungen & Substitutionen: Herbrand-Modelle

Zuweisungen: $\mathcal{A}: \mathcal{V}ar(\mathcal{L}_{PL}) \to \mathcal{D}$ Abbildung ins Modell
Substitutionen: $\sigma: \mathcal{V}ar(\mathcal{L}_{PL}) \to \mathcal{T}er(\mathcal{L}_{PL})$ Abbildung in die Sprache

- Herbrands Idee: Auch Sprachen können als Domänen für die Interpretation verwendet werden.

Definition 5.4.1

Ein Modell $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$ für die Sprache $\mathcal{L}_{PL}$ ist ein *Herbrand-Modell* für $\mathcal{L}_{PL}$ wenn gilt:

1. $\mathcal{D} = g\mathcal{T}er(\mathcal{L}_{PL})$ ist die Menge der geschlossenen Terme zu $\mathcal{L}_{PL}$.
2. Für jeden geschlossenen Term t gilt: $t^{\mathcal{I}} = t$

Beobachtung

Wenn $\mathcal{M}$ ein Herbrand-Modell für $\mathcal{L}_{PL}$ ist und $\mathcal{A}$ eine Zuweisung in $\mathcal{M}$, dann ist $\mathcal{A}$ eine Substitution $\mathcal{V}ar(\mathcal{L}_{PL}) \to g\mathcal{T}er(\mathcal{L}_{PL})$.

- Unser Farbcode macht deutlich, dass durch Herbrand-Modelle die Unterscheidung von Syntax und Semantik in sich zusammenbricht. Dieses gilt aber im wesentlichen für die Interpretation der Terme. Den Formeln werden durch die Modelle weiterhin Wahrheitswerte zugeordnet, die nicht Teil der Sprache selbst sind.

- Die Zuweisungen in Herbrand Modelle sind Substitutionen, die jeder Variable einen geschlossenen Term zuordnen.

- Da wir schon früher verlangt haben, dass $\mathcal{D}$ nicht die leere Menge ist, gibt es Herbrand-Modelle nur für solche Logiksprachen, die mindestens einen geschlossenen Term, also mindestens eine Konstante haben. Gegebenenfalls muss man eine Spracherweiterung vornehmen, um diese Bedngung zu erfüllen.

Herbrand Modelle – 1

Herbrand-Modelle

- sind spezifische Modelle, da sie über der Sprache $\mathcal{L}_{PL}$ selbst interpretieren,
- sind daher als semantische Basis für Beweisverfahren gut einsetzbar (und „einsehbar“),
- sind aber – wg. des Herbrand Theorems – hinreichen allgemein, um alle denkbaren Modelle in gewisser Weise simulieren oder repräsentieren zu können.

Terme in Herbrand-Modellen

Satz 5.4.2

Sei $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$ ein Herbrand-Modell für $\mathcal{L}_{PL}$, $\mathcal{A}$ eine Zuweisung in $\mathcal{M}$ und t ein beliebiger Term aus $\mathcal{L}_{PL}$.

Dann ist $t\mathcal{A}$ (= Das Resultat der Anwendung der Substitution $\mathcal{A}$ auf t) ein geschlossener Term und $t^{\mathcal{I}, \mathcal{A}} = [t\mathcal{A}]^{\mathcal{I}}$

Beweisidee

Induktion über Termaufbau mit

$[x\mathcal{A}]^{\mathcal{I}} = x\mathcal{A}$ (da $x\mathcal{A}$ geschlossener Term) und $x^{\mathcal{I}, \mathcal{A}} = x^{\mathcal{A}} = x\mathcal{A}$

$[c\mathcal{A}]^{\mathcal{I}} = c^{\mathcal{I}} = c$ (da c geschlossener Term) und $c^{\mathcal{I}, \mathcal{A}} = c^{\mathcal{I}} = c$

$[f(t_1, \ldots t_n)\mathcal{A}]^{\mathcal{I}} = f(t_1\mathcal{A}, \ldots t_n\mathcal{A})^{\mathcal{I}} = f^{\mathcal{I}}([t_1\mathcal{A}]^{\mathcal{I}}, \ldots [t_n\mathcal{A}]^{\mathcal{I}})$
und $f(t_1, \ldots t_n)^{\mathcal{I}, \mathcal{A}} = f^{\mathcal{I}}(t_1{}^{\mathcal{I}, \mathcal{A}}, \ldots t_n{}^{\mathcal{I}, \mathcal{A}})$

Formeln in Herbrand-Modellen

Satz 5.4.3

Seien $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$ ein Herbrand-Modell für $\mathcal{L}_{PL}$, $\mathcal{A}$ eine Zuweisung in $\mathcal{M}$ und Φ eine beliebige Formel aus $\mathcal{L}_{PL}$.

Dann ist $\Phi\mathcal{A}$ (= Das Resultat der Anwendung der Substitution $\mathcal{A}$ auf Φ) eine geschlossene Formel und $\Phi^{\mathcal{I}, \mathcal{A}} = [\Phi\mathcal{A}]^{\mathcal{I}}$

Beweisidee

Induktion über Formelaufbau mit

$[P(t_1, \ldots t_n)\mathcal{A}]^{\mathcal{I}} = P(t_1\mathcal{A}, \ldots t_n\mathcal{A})^{\mathcal{I}} = P^{\mathcal{I}}([t_1\mathcal{A}]^{\mathcal{I}}, \ldots [t_n\mathcal{A}]^{\mathcal{I}})$

und $P(t_1, \ldots t_n)^{\mathcal{I}, \mathcal{A}} = P^{\mathcal{I}}(t_1^{\mathcal{I}, \mathcal{A}}, \ldots t_n^{\mathcal{I}, \mathcal{A}})$

und: Substitutionen betreffen gebundene Variablen nicht

Uniforme Notation – Herbrand Modelle

Satz 5.4.4

Sei Φ eine Formel aus $\mathcal{L}_{PL}$ und $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$ ein Herbrand-Modell für $\mathcal{L}_{PL}$. Dann gilt:

1. $(\forall x)\ \Phi$ ist wahr in $\mathcal{M}$ gdw. $\Phi\{x/t\}$ ist wahr in $\mathcal{M}$ für alle $t \in \mathcal{D}$.
2. $(\exists x)\ \Phi$ ist wahr in $\mathcal{M}$ gdw. $\Phi\{x/t\}$ ist wahr in $\mathcal{M}$ für irgendein $t \in \mathcal{D}$.

Satz 5.5.2

Sei $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$ ein Herbrand-Modell für $\mathcal{L}_{PL}$. Dann gilt:

1. Falls γ eine Formel aus $\mathcal{L}_{PL}$, so gilt:
   γ ist wahr in $\mathcal{M}$ gdw. $\gamma(t)$ wahr in $\mathcal{M}$ für alle $t \in \mathcal{D}$.
2. Falls δ eine Formel aus $\mathcal{L}_{PL}$, so gilt:
   δ ist wahr in $\mathcal{M}$ gdw. $\delta(t)$ wahr in $\mathcal{M}$ für irgendein $t \in \mathcal{D}$.

- Satz 5.4.4 (Dies ist nicht das Herbrand-Theorem) zeigt, wie sich die Interpretation in der Sprache im Hinblick auf die Auswertung von Formeln mit Quantifikation auswirkt.
- Durch die Herbrand-Interpretationen werden die Quantoren substitutionell interpretiert: Die All-Formeln ist wahr, wenn alle Substitutionsinstanzen wahr sind, die Existenz-Formel ist wahr, wenn eine Substitutionsinstanz wahr ist.
- Damit diese Interpretationen sinnvoll sind, müssen die Herbrand-Universen (d.h. die Menge der geschlossenen Terme) zu den Sprachen hinreichend komplex sein. Dazu muss die Menge der Konstanten oder der Funktionssymbole auf Anforderung hin erweiterbar sein (⇒ Parameter, Skolemfunktionen).
- Die ‚Konsequenz' zeigt auf, dass es möglich ist, das Verhalten quantifizierter Formeln durch Mengen von Formeln mit weniger Quantoren nachzubilden. (⇒ Skolemisierung, Herbrand-Expansion: F1-Vorlesung)
- Im Endeffekt bedeutet dies, dass es zu jeder geschlossenen prädikatenlogischen Formel Φ eine Menge von geschlossenen Formeln S ohne Quantoren gibt, so dass Φ genau dann erfüllbar ist, wenn S erfüllbar ist. Da die Formeln aus S auch keine Variablen mehr enthalten, kann man S wie eine Menge aussagenlogischer Formeln behandeln. Das heißt, dass das

Prädikatenlogisches Hintikka-Lemma

Satz 5.6.2 (*Hintikka-Lemma*)

Sei $\mathcal{L}_{\mathrm{PL}}$ eine prädikatenlogische Sprache mit einer nicht-leeren Menge von geschlossenen Termen.

Falls ***H*** eine prädikatenlogische Hintikka-Menge bzgl. $\mathcal{L}_{\mathrm{PL}}$ ist, so ist ***H*** in einem Herbrand-Modell für $\mathcal{L}_{\mathrm{PL}}$ erfüllbar.

Beweisstruktur

1. Definition eines Herbrand-Modells $\mathcal{M}$ für $\mathcal{L}_{\mathrm{PL}}$ unter Rückgriff auf ***H***.
2. Beweis, dass jede Formeln aus ***H*** in $\mathcal{M}$ wahr ist.

- Eine Sprache mit leerer Menge geschlossener Terme kann z.B. dann auftreten, wenn in $\mathcal{L}_{\mathrm{PL}}$ keine Konstante existiert.

Prädikatenlogisches Hintikka-Lemma: Modellkonstruktion

1. Modellkonstruktion $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$

$\mathcal{D} = g\mathcal{T}er(\mathcal{L}_{PL})$

$\mathcal{I}$ ist die folgende Abbildung:

- für jedes $c \in \mathcal{K}on(\mathcal{L}_{PL})$ ist $\mathcal{I}(c) = c$
- für jedes $f \in \mathcal{F}un_n(\mathcal{L}_{PL})$ ist $\mathcal{I}(f)(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$

Für jeden geschlossenen Term t gilt dann: $t^{\mathcal{I}} = t$

- für jedes $R \in \mathcal{R}el_n(\mathcal{L}_{PL})$ sei
  $\mathcal{I}(R) = \{(t_1, \ldots, t_n) \in \mathcal{D}^n \mid R(t_1, \ldots, t_n) \in \boldsymbol{H}\}$

Prinzip der Strukturellen Induktion [UN, Prädikatenlogik]

Theorem 5.5.3

Eine Eigenschaft ***Q*** gilt für alle Formeln der Prädikatenlogik gdw. gilt:

- Induktionsbasis$_{UN}$
  Jede atomare Formel X und deren Negation besitzen die Eigenschaft ***Q***.
- Induktionsschritte$_{UN}$
  - Falls Z die Eigenschaft ***Q*** hat, dann hat auch $\neg\neg Z$.
  - Falls α_1 und α_2 die Eigenschaft ***Q*** haben, dann auch α.
  - Falls β_1 und β_2 die Eigenschaft ***Q*** haben, dann auch β.
  - Wenn für jeden Term t die Formel $\gamma(t)$ die Eigenschaft ***Q*** besitzt, dann auch γ.
  - Wenn für jeden Term t die Formel $\delta(t)$ die Eigenschaft ***Q*** besitzt, dann auch δ.

Prädikatenlogisches Hintikka-Lemma: Induktionsbasis

2. Jede Formel aus *H* ist wahr in $\mathcal{M}$

UN-Induktion mit: Wenn $\Phi \in H$, dann $\nu_H(\Phi) = \mathbf{t}$.

Induktionsbasis$_{\mathbf{UN}}$

Ist $\Phi = R(t_1, \ldots, t_n) \in \boldsymbol{H}$, dann ist

$\Phi^{\mathcal{I}} = R^{\mathcal{I}}(t_1^{\mathcal{I}}, \ldots, t_n^{\mathcal{I}}) = R^{\mathcal{I}}(t_1, \ldots, t_n) = \mathbf{t}$, nach Def. von $R^{\mathcal{I}}$

Ist $\Phi = \neg R(t_1, \ldots, t_n) \in \boldsymbol{H}$, dann ist

$\Phi^{\mathcal{I}} = \neg R^{\mathcal{I}}(t_1^{\mathcal{I}}, \ldots, t_n^{\mathcal{I}}) = \neg R^{\mathcal{I}}(t_1, \ldots, t_n) = \mathbf{t}$, da $R(t_1, \ldots, t_n) \notin \boldsymbol{H}$

Logische Konstanten $\Rightarrow$ Satz 3.5.2

Also ist die Behauptung für alle atomaren Formeln und deren Negation bewiesen.

- Hier erkennt man leicht: Die Konstruktion ist genau so vorgenommen worden, dass die Induktionsbasis sich ganz einfach ergibt.

Prädikatenlogisches Hintikka-Lemma: Induktionsschritte

Induktionsannahme$_{\text{UN}}$

- Es sei γ eine γ-Formel und δ eine δ-Formel, so dass für alle $F \in \{\gamma(t), \delta(t) \mid t \in g\mathcal{T}er(\mathcal{L}_{\text{PL}})\}$ gilt: Wenn $F \in \boldsymbol{H}$, dann $v_H(F) = \mathbf{t}$.

Induktionsschritt$_{\text{UN}}$ γ

Wenn $\gamma \in \boldsymbol{H}$, dann sind alle $\gamma(t) \in \boldsymbol{H}$. [Def. Hintikka-Menge]
Dann sind alle $\gamma(t)$ wahr in $\mathcal{M}$. [Induktionsannahme]
Also ist γ wahr in $\mathcal{M}$. [Satz 5.5.2]

Induktionsschritt$_{\text{UN}}$ δ

Wenn $\delta \in \boldsymbol{H}$, dann ist ein $\delta(t) \in \boldsymbol{H}$. [Def. Hintikka-Menge]
Dieses $\delta(t)$ ist wahr in $\mathcal{M}$. [Induktionsannahme]
Also ist δ wahr in $\mathcal{M}$. [Satz 5.5.2]

Weitere Induktionsschritte $\Rightarrow$ Satz 3.5.2

Herbrand-Theorem

Theorem (5.9.4*)

Es sei **par** eine abzählbar unendliche Menge neuer Parameter.

$\boldsymbol{S} \subseteq g\mathcal{F}or(\mathcal{L}_{\mathrm{PL}})$ ist genau dann erfüllbar, wenn $\boldsymbol{S}$ in einem Herbrand-Modell für $\mathcal{L}_{\mathrm{PL}}{}^{\mathbf{par}}$ erfüllbar ist.

$X \in g\mathcal{F}or(\mathcal{L}_{\mathrm{PL}})$ ist genau dann gültig, wenn X in allen Herbrand-Modellen für $\mathcal{L}_{\mathrm{PL}}{}^{\mathbf{par}}$ wahr ist.

Beweisskizze

Da das Hintikka-Lemma (5.6.2) bereits bewiesen ist, reicht es, folgendes Lemma zu beweisen.

Lemma

Es sei $\mathcal{L}_{\mathrm{PL}}$ eine prädikatenlogische Sprache und **par** eine abzählbar unendliche Menge (bzgl. $\mathcal{L}_{\mathrm{PL}}$) neuer Parameter.

$\boldsymbol{S} \subseteq g\mathcal{F}or(\mathcal{L}_{\mathrm{PL}})$ ist genau dann erfüllbar, wenn $\boldsymbol{S}$ Teilmenge einer Hintikka-Menge bzgl. $\mathcal{L}_{\mathrm{PL}}{}^{\mathbf{par}}$ ist.

- Weitere Beweise sind in vielen Logik-Büchern zu finden, in ähnlicher Form auch in den F1-Unterlagen

- Das Herbrand-Theorem stellt die besondere Rolle der Interpretation bzgl. sprachlicher Ausdrücke logischen Sprache $\mathcal{L}_{\mathrm{PL}}$ heraus. Damit wird ein Weg aufgezeigt, wie Modelle systematisch konstruiert und getestet werden können.
- Genau dies ist die semantische Fundierung von Beweisverfahren. Nur leider sind auch Herbrand-Modelle in der Regel nicht endlich.

Selbststudium:
Beweisskizze: Existenz einer Hintikka-Menge

Behauptung

Es sei $\mathcal{L}_{PL}$ eine prädikatenlogische Sprache, **par** eine abzählbar unendliche Menge (bzgl. $\mathcal{L}_{PL}$) neuer Parameter und $\boldsymbol{S} \subseteq g\mathcal{F}or(\mathcal{L}_{PL})$ erfüllbar.

Dann ist $\boldsymbol{S}$ Teilmenge einer Hintikka-Menge bzgl. $\mathcal{L}_{PL}^{\mathbf{par}}$.

Beweisskizze

- Da $\mathcal{L}_{PL}^{\mathbf{par}}$ eine abzählbare Menge ist, können wir annehmen, dass eine Folge $F_1, \ldots, F_i, \ldots$ von Formeln aus $\mathcal{L}_{PL}^{\mathbf{par}}$ gegeben ist, so dass jede Formel aus $\mathcal{L}_{PL}^{\mathbf{par}}$ auch vorkommt.
- Da in endlichen Formelmengen auch nur endlich viele Parameter vorkommen können und $\boldsymbol{S}$ keinen Parameter enthält, gibt es zu jedem i unendlich viele Parameter, die nicht in $\boldsymbol{S} \cup \{F_1, \ldots, F_i\}$ vorkommen.

Die andere Richtung des Lemmas ist schon durch das Hintikka-Theorem bewiesen.

Das im Folgenden angegebene ‚Konstruktionsverfahren' für die Hintikka-Menge ist formal sinnvoll, um zu zeigen, dass es so eine Menge gibt. Da die resultierende Menge aber unendlich sein kann, ist es natürlich nicht praktikabel.

Die Menge **par** garantiert uns dabei, dass wir genügend Bezeichnungen für Objekte haben, die aus $\boldsymbol{S}$ über die Quantoren erschließbar sind.

Selbststudium: Beweisskizze: Existenz einer Hintikka-Menge (2)

- Da $\boldsymbol{S}$ erfüllbar ist, gibt es ein Modell $\mathcal{M} = \langle \mathcal{D}, \mathcal{I} \rangle$ und eine Zuweisung $\mathcal{A}$ in $\mathcal{M}$, so dass alle Elemente von $\boldsymbol{S}$ wahr gemacht werden.
- Wir definieren nun Folgen $\boldsymbol{S}_\mathbf{i} \subseteq \mathcal{L}_{PL}{}^{\mathbf{par}}$ und $\mathcal{M}_\mathbf{i} = \langle \mathcal{D}, \mathcal{I}_\mathbf{i} \rangle$, so dass $\boldsymbol{S} \subseteq \boldsymbol{S}^* = \cup_{i \geq 0} \boldsymbol{S}_\mathbf{i}$ und $\boldsymbol{S}^* \subseteq \mathcal{L}_{PL}{}^{\mathbf{par}}$ eine Hintikka-Menge ist.
- Die Folgen $\boldsymbol{S}_\mathbf{i}$ und $\mathcal{M}_\mathbf{i} = \langle \mathcal{D}, \mathcal{I}_\mathbf{i} \rangle$ (und zur Unterstützung $\mathcal{I}_\mathbf{i}'$) sind wie folgt definiert:
- $\boldsymbol{S}_\mathbf{0} = \boldsymbol{S}$, $\mathcal{I}_\mathbf{0} = \mathcal{I}$

Selbststudium: Beweisskizze: Existenz einer Hintikka-Menge (3)

- Für jedes $i \geq 0$
  - Wenn F_{i+1} Parameter enthält, die nicht in $\boldsymbol{S} \cup \{F_1, \ldots, F_i\}$ vorkommen, dann sei $\mathcal{I}_i'$ eine Erweiterung von $\mathcal{I}_i$ so, dass alle neuen Parameter auf Elemente von $\mathcal{D}$ abgebildet werden, ansonsten sei $\mathcal{I}_i' = \mathcal{I}_i$.
  - Wenn F_{i+1} von $\mathcal{I}_i'$ und $\mathcal{A}$ nicht wahr gemacht wird, dann $\boldsymbol{S}_{i+1} = \boldsymbol{S}_i$ und $\mathcal{I}_{i+1} = \mathcal{I}_i'$.
  - Wenn F_{i+1} von $\mathcal{I}_i'$ und $\mathcal{A}$ wahr gemacht wird und keine δ-Formel ist, dann $\boldsymbol{S}_{i+1} = \boldsymbol{S}_i \cup \{F_{i+1}\}$ und $\mathcal{I}_{i+1} = \mathcal{I}_i'$.
  - Wenn F_{i+1} eine δ-Formel ist, die von $\mathcal{I}_i'$ und $\mathcal{A}$ wahr gemacht wird, dann sei p ein Parameter, der nicht in $\boldsymbol{S} \cup \{F_1, \ldots, F_{i+1}\}$ vorkommt, $\delta(p)$ Instanz von F_{i+1} und $\boldsymbol{S}_{i+1} = \boldsymbol{S}_i \cup \{F_{i+1}, \delta(p)\}$. $\mathcal{I}_{i+1}$ sei eine Erweiterung von $\mathcal{I}_i'$ so, dass $\delta(p)$ wahr wird.

- Jetzt müsste man eigentlich noch folgendes zeigen:
  - Die Erweiterungen der Interpretationen sind in jedem Schritt möglich.
  - In jedem Schritt gilt: Si+1 ist erfüllbar in Mi+1
  - Es gilt so gar für j ≤ i: jede Teilmenge von Sj ist erfüllbar in Mi. (Dabei ist auch wichtig, dass die Menge D über alle Schritte konstant bleibt, auch wenn die Menge der Terme, die in D interpretiert werden, anwachsen kann.)
  - S* erfüllt alle Bedingungen, die an Hintikka-Mengen gestellt werden. Dabei kann man darauf zurückgreifen, dass es für jede Menge Si auch immer ein Modell gibt, in dem sie erfüllbar ist.

Vorgehen

Ziel

- Spezifikation eines Tableau-Verfahrens für Prädikatenlogik
  - Regeln, Korrektheit, Vollständigkeit

Vorarbeiten (in Analogie zur Aussagenlogik)

- Uniforme Notation für quantifizierte Formeln
- Korrektheit: Erweiterungsmöglichkeiten für Formelmengen unter Erhalt der Erfüllbarkeit
- Vollständigkeit: prädikatenlogische Hintikka-Mengen, Beweis ihrer Erfüllbarkeit, dazu Definition von Herbrandmodellen
- Unentscheidbarkeit der Prädikatenlogik

Tableau-Verfahren

Unentscheidbarkeit der Prädikatenlogik

Churchs Theorem (hier nach Ben-Ari 5.43)

- Gültigkeit von Formeln ist in der Prädikatenlogik unentscheidbar.
- Es gibt keine allgemeine Prozedur, die bei Eingabe einer beliebigen prädikatenlogischen Formel nach endlicher Zeit hält und (verlässlich) ausgibt, ob die Formel gültig ist.
- Durch die enge Verbindung von Gültigkeit, Erfüllbarkeit, Folgerbarkeit, ... gelten dann entsprechende Aussagen auch für diese semantischen Begriffe.

Beweisskizze zu Churchs Theorem

Reduktion des Halteproblems für 2-Registermaschinen auf Gültigkeit in der Prädikatenlogik.

- Definition 2-Register-Maschinen
- Übersetzung eines Programms in PL
- Übersetzung des Halteproblems in ein Gültigkeitsproblem
- Beweis, dass die Übersetzung korrekt ist

(Ben-Ari, 2001, S. 122f.)

- Programme für 2-Registermaschinen sind sehr einfach strukturiert, deshalb lassen sie sich auch sehr einfach in die Prädikatenlogik übersetzten.
- Andererseits sind sie aber mächtig genug, so dass sich das Halteproblem für Turingmaschinen auf ihr Halteproblem reduzieren lässt. (Hopkroft Ullman, 1979 Section 7.8).

2-Register-Maschine: Definition (Ben-Ari 5.41)

Eine 2-Register-Maschine M

- besteht aus zwei Registern x und y, die natürliche Zahlen enthalten können,
- und einem Programm P = $L_0, \ldots, L_n$, das aus einer Liste von n Instruktionen besteht, wobei L_n die Instruktion `'halt'` ist, und für $0 \leq i < n$ L_i eine der folgenden Instruktionen ist:
  - `x := x + 1;`
  - `y := y + 1;`
  - `wenn x > 0, dann x := x - 1 und gehe zu Lj;`
  - `wenn y > 0, dann y := y - 1 und gehe zu Lj;`

- Ben-Ari spezifiziert die Befehle etwas anders. Die obige Spezifikation ist aber in verschiedenen anderen Aufsätzen zu finden und ich habe den Eindruck, dass diese korrekt sind.

2-Register-Maschine: Ausführungssequenz (Ben-Ari 5.41)

- Sei M eine 2-Register-Maschine.

Eine Ausführungssequenz von M

- ist eine Folge von Zuständen $s_k = (L_i, x, y)$, wobei L_i eine Instruktion im Programm und x und y der Inhalt der Register `x` und `y` vor der Ausführung von L_i ist.
- Der initiale Zustand ist $s_0 = (L_0, m, 0)$ für eine Zahl m.
- s_{k+1} ergibt sich aus $s_k = (L_i, x, y)$ durch Ausführung von L_i.
- Wenn es ein k gibt, so dass $s_k = (L_n, x, y)$, dann hält die Berechung von M und M hat y = f(m) berechnet.

Beispiel: Programm einer 2-Register-Maschine

Funktion: f(m) = 2 + 3m

```
L0: x := x + 1;
L1: wenn x > 0, dann x := x - 1 und gehe zu L3;
L2: y := y + 1;
L3: y := y + 1;
L4: y := y + 1;
L5: wenn x > 0, dann x := x - 1 und gehe zu L2;
L6: halt;
```

Ausführungssequenz

(L_0, 2, 0), (L_1, 3, 0), (L_3, 2, 0), (L_4, 2, 1), (L_5, 2, 2), (L_2, 1, 2), (L_3, 1, 3), (L_4, 1, 4), (L_5, 1, 5), (L_2, 0, 5), (L_3, 0, 6), (L_4, 0, 7), (L_5, 0, 8), (L_6, 0, 8)

Turing-Maschinen und 2-Register-Maschinen

Theorem (Minsky, hier nach Ben-Ari 5.42)

- Für jede Turing-Maschine T, die eine Funktion f berechnet, kann eine 2-Register-Maschine M konstruiert werden, die dieselbe Funktion f berechnet.

2-Register-Maschinen

- sind noch unpraktischer als Turingmaschinen, wenn es um die Programmierung geht,
- sind aber sehr praktisch für den angestrebten Beweis, denn die Maschinen lassen sich recht einfach mit der Prädikatenlogik beschreiben.

- Beweis : Hopcroft & Ullman (1979, Section 7.8) und andere Auflagen, z.B. Hopcroft, Motwani & Ullman 2002, Abschnitt 8.5)
- Minsky, M. (1967). Computation: Finite and Infinite Machines. Prentice-Hall.

2-Register-Maschinen und Logik

Lemma

- Für jede 2-Register-Maschine M kann eine Formel S_M konstruiert werden, so dass S_M genau dann gültig ist, wenn M ausgehend vom Zustand (L_0, 0, 0) hält.

Beweisidee

- Kodierung der natürlichen Zahlen durch Terme:
  $0 \rightarrow a$, $n+1 \rightarrow s(n)$
- Kodierung der Zustände (L_i, m, n) durch atomare Formeln $p_i(m, n)$, Anfangszustand: $p_0(a, a)$
- Kodierung der Zustandsübergänge bei Ausführung von L_i durch S_i
- Kodierung des Halteproblems als Gültigkeit von
  $(\bigwedge_{i<n} S_i \wedge p_0(a, a)) \supset \exists z_1 \exists z_2\, p_n(z_1, z_2)$

2-Register-Maschinen und Logik (2)

Beweisidee

- Kodierung des Halteproblems als Gültigkeit von

  $(\bigwedge_{i<n} S_i \wedge p_0(a, a)) \supset \exists z_1 \exists z_2\, p_n(z_1, z_2)$

  - Die Formel soll eine Interpretation besitzen, bei der $p_i(m, n)$ genau dann wahr ist, wenn sich M irgendwann im Zustand (L_i, m, n) befindet.
- Kodierung der Zustandsübergänge bei Ausführung von L_i durch S_i
  - Demnach soll S_i ausdrücken, in welchem Zustand sich M befindet, nachdem Programmschritt L_i auf einem beliebigen Zustand ausgeführt wurde.

2-Register-Maschinen und Logik (3)

Beweisidee

- Kodierung der Zustandsübergänge bei Ausführung von L_i durch S_i
  - Demnach soll S_i ausdrücken, in welchem Zustand sich M befindet, nachdem Programmschritt L_i auf einem beliebigen Zustand ausgeführt wurde.

L_i	S_i
`x := x + 1;`	$\forall x\, \forall y\, (p_i(x, y) \supset p_{i+1}(s(x), y))$
`y := y + 1;`	$\forall x\, \forall y\, (p_i(x, y) \supset p_{i+1}(x, s(y)))$
`wenn x > 0, dann x := x - 1 und gehe zu Lj;`	$\forall y\, (p_i(a, y) \supset p_{i+1}(a, y)) \wedge$ $\forall x\, \forall y\, (p_i(s(x), y) \supset p_j(x, y))$
`wenn y > 0, dann y := y - 1 und gehe zu Lj;`	$\forall x\, (p_i(x, a) \supset p_{i+1}(x, a)) \wedge$ $\forall x\, \forall y\, (p_i(x, s(y)) \supset p_j(x, y))$

- Nun ist noch zu zeigen: Gegeben eine beliebige 2-Register-Maschine M, dann ist die entsprechende Formel $(\bigwedge_{i<n} S_i \wedge p_0(a, a)) \supset \exists z_1\, \exists z_2\, p_n(z_1, z_2)$ genau dann gültig, wenn die Maschine bei der Eingabe x = 0 und y = 0 nach endlich vielen Schritten anhält. Details bei Ben-Ari 2002.

Beispiel: Kodierung des Programms

$\forall x\ \forall y\ (p_0(x, y) \supset p_1(s(x), y)) \wedge$
$\forall y\ (p_1(a, y) \supset p_2(a, y)) \wedge \forall x\ \forall y\ (p_1(s(x), y) \supset p_3(x, y)) \wedge$
$\forall x\ \forall y\ (p_2(x, y) \supset p_3(x, s(y))) \wedge$
$\forall x\ \forall y\ (p_3(x, y) \supset p_4(x, s(y))) \wedge$
$\forall x\ \forall y\ (p_4(x, y) \supset p_5(x, s(y))) \wedge$
$\forall y\ (p_5(a, y) \supset p_6(a, y)) \wedge \forall x\ \forall y\ (p_5(s(x), y) \supset p_2(x, y)) \wedge$

Startzustand

$p_0(a, a)$

"Berechnung": Folgende Formel sind folgerbar

$p_1(s(a), a)$ $p_3(a, a)$ $p_4(a, s(a))$ $p_5(a, s(s(a)))$ $p_6(a, s(s(a)))$
$\exists z_1\ \exists z_2\ p_6(z_1, z_2)$

Ch. Habel / C. Eschenbach: Logik & Semantik 8 – 45

- In diesem Fall ist offensichtlich, dass die Maschine hält und entsprechend, die Kodierung des Halteproblems zu einer gültigen Formel führt.

Unentscheidbarkeit der Prädikatenlogik

Churchs Theorem

- Gültigkeit von Formeln ist in der Prädikatenlogik unentscheidbar.

Wie man am Beweis sieht: Churchs Theorem gilt auch,

- wenn man das Inventar der verfügbaren Symbole stark einschränkt (mind. zweistellige Relationssymbole sind aber erforderlich).
- wenn man die Struktur der Formeln stark einschränkt (Kodierung entspricht einem Prolog-Programm mit einer Anfrage)

Was tun?

- Mit Unentscheidbarkeit leben (allein Korrektheit gewährleisten) und Notbremsen einbauen
- Nach entscheidbaren Fragmenten suchen.

Uniforme Notation – Beweis von Satz 5.5.1: Detail

Es sei x eine Variable, die nicht in γ vorkommt.

- Dann gilt $\gamma(t) = \gamma(x)\{ x / t \}$.

Es sei x eine Variable, die nicht in γ vorkommt.

- Z.B.: $\gamma = (\forall v)\ \Phi$ und in Φ kommt x nicht vor.
- Dann $\gamma(x) = \Phi\{v / x\}$
- Dann $\gamma(t) = \Phi\{v / t\} = \Phi\{v / x\}\{ x / t \}$

wg. Komposition von Substitutionen

γ	$\gamma(t)$	δ	$\delta(p)$
$(\forall v)\ \Phi$	$\Phi\{v / t\}$	$(\exists v)\ \Phi$	$\Phi\{v / p\}$
$\neg(\exists v)\ \Phi$	$\neg\Phi\{v / t\}$	$\neg(\forall v)\ \Phi$	$\neg\Phi\{v / p\}$

- Der zweite Teil des Satzes stellt den semantischen Sachverhalt dar, der die Skolemisierung rechtfertigt.

(Un-)Endlichkeit von Modellen

Corollar 5.9.2

Jede Menge ***S*** von geschlossenen Formeln der Sprache $\mathcal{L}_{PL}$, die in beliebig großen endlichen Modellen erfüllbar ist, ist erfüllbar in einem nicht-endlichen Modell.

Bemerkung

Aus Corollar 5.9.2 ergibt sich, dass es keine Formelmenge der Prädikatenlogik gibt, die in allen endlichen Domänen erfüllbar ist, aber in keiner unendlichen.

D.h.: Die Annahme, dass eine Domäne endlich ist, ist in der Prädikatenlogik nicht formulierbar, solange wir keine explizite „obere Schranke“ für die Mächtigkeit angeben können.

- Beweis in Fitting (1996) greift auf das Kompaktheitstheorem zurück.

Theorem von Löwenheim & Skolem

Theorem 5.9.3 (Ben-Ari, 2001, Th. 5.39)

Sei ***S*** $\subseteq \mathcal{gFor}(\mathcal{L}_{\mathrm{PL}})$. Wenn ***S*** erfüllbar ist, dann ist ***S*** in einem abzählbaren Modell erfüllbar.

Beweisidee

Das Herbrand-Modell aus dem ersten Teil von 5.9.4 ist abzählbar.

Anmerkung

Das Theorem zeigt, dass es keine prädikatenlogische (first-order) Charakterisierung der reellen Zahlen geben kann.

In der monadischen Prädikatenlogik, d.h. in prädikatenlogischen Sprachen, die nur ein-stellige Relationssymbole zulassen, kann aus der Existenz eine Modells auf die Existenz eines endlichen Modells geschlossen werden.
Genauer: Falls S eine erfüllbare geschlossene Formel einer monadischen Sprache ist, und diese Formel k verschiedene Relationssymbole und r Variablen enthält, dann existiert ein Modell mit $2^k r$ Elemente in $\mathcal{D}$.

Zur Anmerkung.

Annahme: Wir versuchen die Reellen Zahlen durch eine Formel der Prädikatenlogik zu charakterisieren, d.h. dass diese Formel S über der Domäne $\mathcal{D} = \mathbb{R}$, der reellen Zahlen, erfüllt wird, aber nicht über Domänen, die nicht isomorph zu $\mathbb{R}$ sind.
Das Löwenheim-Skolem Theorem besagt, dass bei Erfüllbarkeit über $\mathbb{R}$ auch Erfüllbarkeit in abzählbaren – also nicht-isomorphen Domänen – vorliegt.

Es gibt keine prädikatenlogische (first-order) Charakterisierung der reellen Zahlen

Annahme

S sei eine Menge geschlossener Formeln, die das System der reellen Zahlen, und somit die Menge $\mathbb{R}$ charakterisiert, d.h.

- ***S*** wird über der Domäne $\mathcal{D} = \mathbb{R}$ erfüllt
- ***S*** wird nur über Domänen erfüllt, die isomorph zu $\mathbb{R}$ sind.

Konsequenz aus der Annahme:

- Dann ist ***S*** auch in einem abzählbaren Modell erfüllbar.
- Derartige abzählbare Modelle sind nicht isomorph zu $\mathbb{R}$.

Charakterisierung der Reellen Zahlen erfordert Prädikatenlogik zweiter Stufe.

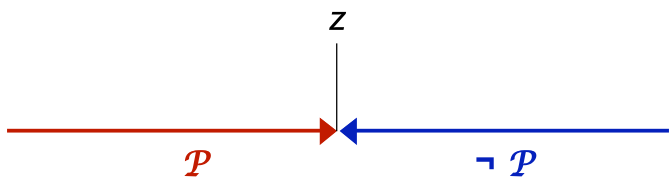
Prädikatenlogik zweiter Stufe ist nicht endlich axiomatisierbar. Das heißt: es gibt keine endliche Menge von Formeln und Ableitungsregeln, so dass alle Tautologien der Prädikatenlogik zweiter Stufe mit den Axiomen und Regeln beweisbar sind.

Entsprechend ist die Verwendung dieser Logik im Rahmen des automatischen Beweisens nur von sehr eingeschränktem Nutzen, da noch nicht einmal ein Semi-Entscheidungsverfahren in Aussicht steht.

Dedekindscher Schnitt

Das Schnittaxiom

$$\forall \mathcal{P}\, [\forall x\, y\, [\mathcal{P}(x) \wedge \neg \mathcal{P}(y) \rightarrow x \prec y] \wedge \exists x\, [\mathcal{P}(x)] \wedge \exists y\, [\neg \mathcal{P}(y)]$$
$$\rightarrow$$
$$\exists z\, [\forall x\, [x \prec z \rightarrow \mathcal{P}(x)] \wedge \forall y\, [z \prec y \rightarrow \neg \mathcal{P}(y)]]]$$



- Jede vollständige Aufteilung der reellen Zahlen in eine *Kleiner*-Menge und eine *Grösser*-Menge definiert einen eindeutigen trennenden Punkt z. (Es wird keine Aussage über z bzgl. der Eigenschaft $\mathcal{P}$ gemacht.)

Mit $\mathcal{P}(x)$ gdw. $x < 0 \vee x^2 < 2$

ergibt sich gemäss Dedekindschem Schnitt

für z die Bedingung

$$\forall u\, (u < z \rightarrow u < 0 \vee u^2 < 2) \wedge \forall u\, (z < u \rightarrow u^2 \geq 2 \wedge u \geq 0)$$

Dieses z nennen wir auch ‚positive Wurzel aus 2 ’