Formale Modellierung
Vorlesung 8 vom 27.05.13: Die Gödel-Theoreme

Serge Autexier & Christoph Lüth

Universität Bremen

Sommersemester 2013

Fahrplan

- Teil I: Formale Logik
  - Einführung
  - Aussagenlogik: Syntax und Semantik, Natürliches Schließen
  - Konsistenz & Vollständigkeit der Aussagenlogik
  - Prädikatenlogik (FOL): Syntax und Semantik
  - Konsistenz & Vollständigkeit von FOL
  - FOL mit induktiven Datentypen
  - FOL mit Induktion und Rekursion
  - Die Gödel-Theoreme
  - Weitere Datentypen: Mengen, Multimengen, Punkte
- Teil II: Spezifikation und Verifikation
- Teil III: Schluß

Das Tagesmenü

- Terminierende Funktionen und abgeleitete Induktionsschemata

- Gödels erster Unvollständigkeitssatz

  Jede konsistente Theorie, die hinreichend expressiv ist, um die natürlichen Zahlen zu Formalisieren erlaubt die Formulierung von wahren Aussagen, die weder beweisbar noch widerlegbar sind.

Sicheres Spezifikationsprinzip

- Beginne mit Basistheorie mit $\mathbb{N}$ und wohlfundiertem Induktionsschemata für $\mathbb{N}$ (getypte Prädikatenlogik mit Typ $\mathbb{N}$ und Induktionsschemata!)
  - $\mathbb{N}$ hat beweisbar nicht-leere Trägermenge
- Erweitere nur konservativ um
  - totale, terminierende Funktionen und Prädikate
  - Typdefinitionen (ausgehend von $\mathbb{N}$)
    - Erbt Induktionsprinzip über Umweg über $\mathbb{N}$
- Erlaubt Definition von Konstruktoren für neue Typen
  - Terminierung: Abbildung der Termgröße auf $\mathbb{N}$ mittels geschachtelter Anwendung von Rep_t
  - Wenn freie Erzeugtheit des neuen Typs beweisbar, dann folgt Induktionsschema direkt auf dem neuen Typ
- Damit hat man garantiert immer konsistente Spezifikationen (= Modellierung).

Abgeleitetete Induktionsschemata

- $\mathsf{fib}(x)$

$$\frac{P(0) \quad P(s(0)) \quad \forall x. P(x) \wedge P(\mathsf{s}(x)) \longrightarrow P(\mathsf{s}(\mathsf{s}(x)))}{\forall x. P(x)}$$

- $\mathsf{half}(x)$

$$\frac{P(0) \quad P(s(0)) \quad \forall x. P(x) \longrightarrow P(\mathsf{s}(\mathsf{s}(x)))}{\forall x. P(x)}$$

- $\mathsf{gcd}(x)$

$$\frac{\begin{array}{l} P(0, y) \\ x > 0 \longrightarrow P(x, 0) \\ \forall x, y. x > y \wedge P(x - y, y) \longrightarrow P(x, y) \\ \forall x, y. \neg(x > y) \wedge P(x, y - x) \longrightarrow P(x, y) \end{array}}{\forall x. \forall y. P(x, y)}$$

Abgeleitetete Induktionsschemata besser zum Beweisen

- Abgeleitete Induktionsschemata erzeugen Fälle, in denen die Rekursionsgleichungen der Funktion/Prädikate direkt anwendbar sind
- Abgeleitete Induktionsschemata hilfreich wenn Induktion über Variablen gemacht wird, die als Argument der entsprechenden Funktion vorkommen.

$$\forall x. \varphi(\mathsf{half}(x))$$

- Fälle:
  1. $\varphi(\mathsf{half}(0)) \rightsquigarrow \varphi(0)$
  2. $\varphi(\mathsf{half}(\mathsf{s}(0))) \rightsquigarrow \varphi(0)$
  3. $\varphi(\mathsf{half}(x) \longrightarrow \varphi(\mathsf{half}(\mathsf{s}(\mathsf{s}(x)))) \rightsquigarrow \varphi(\mathsf{half}(x) \longrightarrow \varphi(\mathsf{s}(\mathsf{half}(x)))$

Gödels erster Unvollständigkeitssatz

Gödels erster Unvollständigkeitssatz

Jede konsistente Theorie, die hinreichend expressiv ist, um die natürlichen Zahlen zu Formalisieren erlaubt die Formulierung von wahren Aussagen, die weder beweisbar noch widerlegbar sind.

- Zu jeder Formel φ gibt es eine natürliche Zahl, die diese Formel eindeutig kodiert $\lceil \varphi \rceil$
- Zu jedem ND-Beweis D für φ gibt es eine natürliche Zahl, die diesen Beweis eindeutig kodiert $\lceil D \rceil$
- Beweisbarkeit von φ in $\mathbb{N}$ ist als Prädikat Provable($\lceil \varphi \rceil$) formalisierbar in $\mathbb{N}$
- Konstruktion einer Formel mit Aussage "Ich bin nicht beweisbar" $\varphi \longleftrightarrow \neg \mathrm{Prov}(\lceil \varphi \rceil)$

Gödel Kodierung

Folgende Funktion ist definierbar in PA:

$$(n, m) = 2^n \times 3^m$$

Eigenschaften: Es gibt eindeutige Projektionen

$$\mathrm{Left}((n, m)) = n \qquad \mathrm{Right}((n, m)) = m$$

Gödel Kodierung für Terme

Signatur $\Sigma = (\mathcal{F}, \mathcal{P})$, Variables X

- Variablen $x_1, x_2, \dots \in X$

$$\lceil x_i \rceil := (0, i)$$

- Funktionen $f_1, \dots \in \mathcal{F}$

$$\lceil f_i \rceil := (1, i)$$

- Terme

$$\lceil f_i(t_1, \dots t_n) \rceil := \langle \lceil f_i \rceil, \lceil t_1 \rceil, \dots \lceil t_n \rceil \rangle$$

wobei

$$\langle n_1, \dots, n_k \rangle := \begin{cases} n_1 & \text{if } k = 1 \\ (n_1, \langle n_2, \dots, n_k \rangle) & \text{if k} > 1 \end{cases}$$

Gödel Kodierung für Formeln

Signatur $\Sigma = (\mathcal{F}, \mathcal{P})$, Variables X

- Prädikate $p_1, \dots \in \mathcal{P}$, $\perp := p_1$, $\doteq := p_2$

$$\lceil p_i \rceil := (2, i)$$

- Atome

$$\lceil p_i(t_1, \dots t_n) \rceil := \langle \lceil p_i \rceil, \lceil t_1 \rceil, \dots \lceil t_n \rceil \rangle$$

- Konnektive und Quantoren

$$\begin{aligned} \lceil \neg \rceil = (3,1), \lceil \wedge \rceil = (3,2), \lceil \vee \rceil = (3,3) \\ \lceil \longrightarrow \rceil = (3,4), \lceil \longleftrightarrow \rceil = (3,5), \lceil \forall \rceil = (3,6), \lceil \exists \rceil = (3,7) \end{aligned}$$

Gödel Kodierung für Formeln II

Signatur $\Sigma = (\mathcal{F}, \mathcal{P})$, Variables X

- $\lceil \neg\varphi \rceil = (\lceil \neg \rceil, \lceil \varphi \rceil)$
- $\lceil \psi \circ \varphi \rceil = \langle \lceil \circ \rceil, \lceil \psi \rceil, \lceil \varphi \rceil \rangle$
- $\lceil Qx_i.\varphi \rceil = \langle \lceil Q \rceil, \lceil x_i \rceil, \lceil \varphi \rceil \rangle$

Lemma 1 (Facts)

- *Sei* $G := \{ \lceil \varphi \rceil \mid \varphi$ *Variable, Term, oder Formel* $\}$
- G *ist entscheidbar*
- $\lfloor n \rfloor = \varphi :\Leftrightarrow \lceil \varphi \rceil = n$ *ist eindeutig definiert auf* G
- *Substitutionsfunktion* $\mathrm{subst}(n, x, t) = m$ *definierbar auf* G

$$\lceil \varphi[t/x] \rceil = \mathrm{subst}(\lceil \varphi \rceil, \lceil x \rceil, \lceil t \rceil)$$

Gödel Kodierung für Ableitungen

- Gödel Kodierung für Hypothesen Liste:

$$\ulcorner [\varphi_1, \ldots, \varphi_n] \urcorner = \begin{cases} 1 & \text{if } n = 0 \\ \langle (4, \ulcorner \varphi_1 \urcorner), \ldots, (4, \ulcorner \varphi_n \urcorner) \rangle & \text{if } n > 0 \end{cases}$$

$$n \in h \Leftrightarrow \begin{cases} \bot & \text{if } h = 1 \\ \top & \text{if } h = (4, n) \vee \exists m. h = ((4, n), m) \\ n \in m & \text{if } \exists q, m. \neg (q = n) \wedge h = ((4, q), m) \end{cases}$$

- Definition von Konkatenation $*$ und Streichen von Hypothesen

Gödel Kodierung für Ableitungen

$$\left\ulcorner \dfrac{\begin{matrix} D_1 & D_2 \\ \phi & \psi \end{matrix}}{\phi \wedge \psi}\ \wedge I \right\urcorner = \langle (5, \ulcorner \wedge \urcorner), \left\ulcorner \begin{matrix} D_1 \\ \phi \end{matrix} \right\urcorner, \left\ulcorner \begin{matrix} D_2 \\ \psi \end{matrix} \right\urcorner, \ulcorner \phi \wedge \psi \urcorner \rangle$$

$$\left\ulcorner \dfrac{\begin{matrix} D \\ \phi \wedge \psi \end{matrix}}{\phi}\ \wedge E_L \right\urcorner = \langle (6, \ulcorner \wedge \urcorner), \left\ulcorner \begin{matrix} D \\ \phi \wedge \psi \end{matrix} \right\urcorner, \ulcorner \phi \urcorner \rangle$$

Gödel Kodierung für Ableitungen

$$\left\lceil \dfrac{\begin{matrix} D \\ \psi \end{matrix}}{\phi \longrightarrow \psi} \longrightarrow I \right\rceil \quad = \quad \left\langle (5, \lceil \longrightarrow \rceil), \left\lceil \begin{matrix} D \\ \psi \end{matrix} \right\rceil, \lceil \phi \longrightarrow \psi \rceil \right\rangle$$

$$\left\lceil \dfrac{\overset{D_1}{\phi} \qquad \overset{D_2}{\phi \longrightarrow \psi}}{\psi} \longrightarrow E \right\rceil \quad = \quad \left\langle (6, \lceil \longrightarrow \rceil), \left\lceil \overset{D_1}{\phi} \right\rceil, \left\lceil \overset{D_2}{\phi \longrightarrow \psi} \right\rceil, \lceil \psi \rceil \right\rangle$$

Gödel Kodierung für Ableitungen

- Basisfall: $\lceil [\phi] \rceil := \langle (4, \lceil \phi \rceil) \rangle$
- Entsprechend für RAA, $\forall I$, $\forall E$
- Definiere $\mathrm{Der}(p, h, z)$: $\lfloor p \rfloor$ ist Beweis für $\lfloor z \rfloor$ aus Hypothesen $\lfloor h \rfloor$

$$
\begin{aligned}
\mathrm{Der}(p, h, z) := {} & (4, z) \in h && \text{Hypothese} \\
& \vee \quad \exists p_1, h_1, z_1, p_2, h_2, z_2. && \wedge I \\
& \qquad \mathrm{Der}(p_1, h_1, z_1) \wedge \mathrm{Der}(p_2, h_2, z_2) \wedge \\
& \qquad h = h_1 * h_2 \wedge \\
& \qquad p = \langle (5, \lceil \wedge \rceil), p_1, p_2, \lceil \lfloor z_1 \rfloor \wedge \lfloor z_2 \rfloor \rceil \rangle \\
& \vee \quad \exists p_1, h_1, z_1, u. && \longrightarrow I \\
& \qquad \mathrm{Der}(p_1, h_1, z_1) \wedge \\
& \qquad h = \mathrm{Streiche}(u, h_1) \wedge \\
& \qquad p = \langle (5, \lceil \longrightarrow \rceil), p_1, \lceil \lfloor u \rfloor \longrightarrow \lfloor z_2 \rfloor \rceil \rangle \\
& \ldots
\end{aligned}
$$

Beweisbarkeit

- Peano-Axiome + Erweiterung: PA Sei $Ax : \mathbb{N}$ Prädikat

$$\mathcal{A}x(n) \longleftrightarrow \bigvee_{\varphi \in PA} n = \lceil \varphi \rceil$$

- $\mathrm{Prov}(p, f)$: p is Gödelnummer eines ND-Beweis für $\lfloor f \rfloor$

$$\mathrm{Prov}(p, f) \Leftrightarrow \exists h.(\mathrm{Der}(p, h, z) \wedge \forall g.g \in h \wedge Ax(g))$$

- $\mathrm{Thm}(f)$: $\lfloor f \rfloor$ ist ein PA Theorem

$$\mathrm{Thm}(f) \longleftrightarrow \exists p.\, \mathrm{Prov}(p, f)$$

Fixpoint Theorem

Theorem 2 (Fixpoint Theorem)

For each formula $\varphi(x)$ *with only one free variable* x *there exists a formula* ψ *such that* $\vdash \varphi(\ulcorner \psi \urcorner) \longleftrightarrow \psi$

Gödels erster Unvollständigkeitssatz

Jede konsistente Theorie, die hinreichend expressiv ist, um die natürlichen Zahlen zu Formalisieren erlaubt die Formulierung von wahren Aussagen, die weder beweisbar noch widerlegbar sind.

$\mathsf{Thm}(f) \longleftrightarrow \exists p.\, \mathsf{Prov}(p, f)$

existiert φ so dass $\vdash \varphi \longleftrightarrow \neg\, \mathsf{Thm}(\lceil \varphi \rceil)$ Fixpoint auf $\neg\, \mathsf{Thm}(f)$

φ bedeutet: "Ich bin nicht beweisbar"

- Es gilt $\mathbb{N} \models \varphi \longleftrightarrow \neg\, \mathsf{Thm}(\lceil \varphi \rceil)$
- Annahme $\mathbb{N} \models \mathsf{Thm}(\lceil \varphi \rceil)$

$$
\begin{array}{ll}
\Leftrightarrow \mathbb{N} \models \exists x.\, \mathsf{Prov}(x, \lceil \varphi \rceil) & \Leftrightarrow \mathbb{N} \models \mathsf{Prov}(n, \lceil \varphi \rceil) \text{ for some } n \\
\Leftrightarrow\, \vdash \mathsf{Prov}(n, \lceil \varphi \rceil) \text{ for some } n & \Leftrightarrow\, \vdash \varphi \\
\Rightarrow\, \vdash \neg\, \mathsf{Thm}(\lceil \varphi \rceil) & \Rightarrow \mathbb{N} \models \neg\, \mathsf{Thm}(\lceil \varphi \rceil)
\end{array}
$$

- Contradiction, hence φ is true in $\mathbb{N}$, but not provable

Zusammenfassung

- Terminierende Funktionen und abgeleitete Induktionsschemata
  - Hilfreich bei Induktion über Variablen in Argumenten von terminierenden Funktionen um Rekursionsgleichungen anwendbar zu machen
- Gödels erster Unvollständigkeitssatz

  Jede konsistente Theorie, die hinreichend expressiv ist, um die natürlichen Zahlen zu Formalisieren erlaubt die Formulierung von wahren Aussagen, die weder beweisbar noch widerlegbar sind.

  - Beweis durch Kodierung von Formeln und Ableitbarkeit in Peano-Arithmetik
  - Reflektion der Beweisbarkeit in einer Formel
  - Konstruktion einer Formel mit der Aussage "Ich bin nicht beweisbar"