Prof. Dr. H. Brenner **Osnabrück WS 2011/2012**

Einführung in die mathematische Logik

Vorlesung 11

Repräsentierbarkeit der Halteeigenschaft

Ein Durchlauf eines Registerprogramms P bis zum Rechenschritt t wird am einfachsten dokumentiert durch die Folge der Programmkonfigurationen K_s, $1 \leq s \leq t$, wobei jede Programmkonfiguration K_s aus der Nummer der im Rechenschritt s abzuarbeitenden Programmzeile und der Folge der Registerinhalte (zu diesem Zeitpunkt) besteht. Wenn man diese Konfigurationen einfach hintereinander schreibt, so erhält man eine Folge von $t(m+1)$ Zahlen. Wenn umgekehrt eine solche Zahlenfolge gegeben ist, so kann man einfach überprüfen, ob sie den Durchlauf eines Programms bis zum Schritt t korrekt dokumentiert. Man muss sicher stellen, dass sich jeder Abschnitt $(s+1)(m+1)+1, \ldots, (s+1)(m+1)+m+1$ aus dem Vorgängerabschnitt $s(m+1)+1, \ldots, s(m+1)+m+1$ ergibt, wenn die Programmzeile $s(m+1)+1$ angewendet wird.

Lemma 11.1. *Für ein Programm P für eine Registermaschine gibt es einen arithmetischen Ausdruck ψ_P, der genau dann (bei der Standardinterpretation in den natürlichen Zahlen) gilt, wenn das Programm anhält. Genauer gesagt: Wenn das Programm h Programmzeilen besitzt und m Register verwendet, so gibt es einen arithmetischen Ausdruck ψ_P in $2m$ freien Variablen derart, dass*

$$\mathbb{N} \vDash \psi_P(e_1, \ldots, e_m, a_1, \ldots, a_m)$$

genau dann gilt, wenn das Programm bei Eingabe von $(1, e_1, \ldots, e_m)$ nach endlich vielen Schritten bei der Konfiguration $(h, a_1, \ldots, a_m)$ anlangt (und insbesondere anhält).

Beweis. Zur Notationsvereinfachung schreiben wir r_0 statt z und r_0' statt z'. Es sei ϑ der Ausdruck (in vier freien Variablen), der die β-Funktion arithmetisch repräsentiert. Der Ausdruck

$$\vartheta(p, n, i, r)$$

ist also genau dann wahr in $\mathbb{N}$, wenn $\beta(p, n, i) = r$ ist. Diese Beziehung verwenden wir für $i = s(m+1)+j$ (bzw. $i = (s+1)(m+1)+j$) und $r = r_j$ (bzw. $r = r_j'$) und $j = 0, \ldots, m$. Daher besagt der Ausdruck (bei Interpretation in $\mathbb{N}$)

$$\begin{aligned} T(p, n, s) := {} & \vartheta(p, n, s(m+1), r_0) \wedge \ldots \wedge \vartheta(p, n, s(m+1)+m, r_m) \\ & \wedge \vartheta(p, n, (s+1)(m+1), r_0') \wedge \ldots \wedge \vartheta(p, n, (s+1)(m+1)+m, r_m'), \end{aligned}$$

dass die β-Funktion $\beta(p, n, -)$ für die $m + 1$ aufeinander folgenden Zahlen (eingesetzt in die dritte Komponente der β-Funktion) $s(m + 1), s(m + 1) + 1, \ldots, s(m+1)+m$ gleich $r_0, r_1, \ldots, r_m$ und für die $m+1$ aufeinander folgenden Zahlen $(s + 1)(m + 1), (s + 1)(m + 1) + 1, \ldots, (s + 1)(m + 1) + m$ gleich $r'_0, r'_1, \ldots, r'_m$ ist. Hierbei sind p, n, s und die r_j, r'_j Variablen und m ist eine (vom Programm abhängige) Zahl. An der mit $s(m + 1) + j$ bezeichneten Stelle steht die $(m + 1)$-fache Addition der Variablen s mit sich selbst plus die j-fache Addition der 1.

Mit diesem Ausdruck soll der Konfigurationsübergang beim s-ten Rechenschritt beschrieben werden. Da man die Registerbelegung beim s-ten Rechenschritt nicht von vornherein kennt, muss man den Übergang mit Allquantoren ansetzen. Der Ausdruck

$$E(p, n, s) = \forall r_0 \forall r_1 \ldots \forall r_m \forall r'_0 \forall r'_1 \ldots \forall r'_m (T(p, n, s) \to A_P)$$

besagt (A_P repräsentiere das Programm), dass wenn $(r_0, r_1, \ldots, r_m)$ die Konfiguration beim s-ten Rechenschritt und $(r'_0, r'_1, \ldots, r'_m)$ die Konfiguration beim $(s + 1)$-ten Rechenschritt beschreibt, dass dann dieser Konfigurationsübergang durch das Programm bewirkt wird.

In analoger Weise besagt der Ausdruck

$$D(p, n)(x_1, \ldots, x_m) := \vartheta(p, n, 0, 1) \wedge \vartheta(p, n, 1, x_1) \wedge \ldots \wedge \vartheta(p, n, m, x_m)\,,$$

dass $\beta(p, n, 0) = 1$ und $\beta(p, n, j) = x_j$ für $j = 1, \ldots, m$ ist, und der Ausdruck

$$F(p, n, t)(y_1, \ldots, y_m) := \vartheta(p, n, t(m + 1), h) \wedge \vartheta(p, n, t(m + 1) + 1, y_1) \\ \wedge \ldots \wedge \vartheta(p, n, t(m + 1) + m, y_m),$$

besagt, dass $\beta(p, n, t(m + 1)) = h$ und $\beta(p, n, t(m + 1) + j) = y_j$ für $j = 1, \ldots, m$ ist.

Somit besagt der Ausdruck

$$\exists p \exists n \exists t\,(\; D(p, n)(x_1, \ldots, x_m) \wedge \forall s(1 \leq s < t \to E(p, n, s)) \\ \wedge F(p, n, t)(y_1, \ldots, y_m)\;)\,,$$

dass das Programm mit der Startkonfiguration $(1, x_1, \ldots, x_m)$ anhält und dabei die Konfiguration $(h, y_1, \ldots, y_m)$ erreicht. □

Die Unentscheidbarkeit der Arithmetik

Die Idee des folgenden Beweises beruht darauf, dass man, wie wir in der letzten Vorlesung gezeigt haben, die Arbeitsweise von Registerprogrammen mit arithmetischen Ausdrücken repräsentieren und damit die Unentscheidbarkeit des Halteproblems arithmetisch modellieren kann.

SATZ 11.2. *Die Menge der wahren arithmetischen Ausdrücke (ohne freie Variablen) ist nicht R-entscheidbar. D.h. es gibt kein R-Entscheidungsverfahren, mit dem man von einem beliebigen vorgegeben Ausdruck $p \in L_0^{\mathrm{Ar}}$ der arithmetischen Sprache bestimmen kann, ob er wahr oder falsch ist.*

Beweis. Nach Lemma 11.1 gibt es zu jedem Programm P (mit h Befehlen und m Registern) einen arithmetischen Ausdruck ψ_P in $2m$ freien Variablen $x_1, \ldots, x_m, y_1, \ldots, y_m$, der bei Belegung mit $e_1, \ldots, e_m, a_1, \ldots, a_m$ genau dann wahr ist, wenn das Programm, angesetzt auf $(1, e_1, \ldots, e_m)$, schließlich mit der Konfiguration $(h, a_1, \ldots, a_m)$ anhält. Der Ausdruck

$$\varphi_P = \psi_P(0, 0, \ldots, 0, y_1, \ldots, y_m)$$

besagt daher, dass das Programm bei Nulleingabe mit der Registerbelegung $(y_1, \ldots, y_m)$ anhält und der Ausdruck (ohne freie Variablen)

$$\theta_P = \exists y_1 \exists y_2 \ldots \exists y_m \varphi_P$$

besagt, dass das Programm überhaupt anhält. Es gilt also

$$\mathbb{N} \vDash \theta_P$$

genau dann, wenn P bei Nulleingabe anhält. Man beachte, dass die Abbildung, die einem jeden Programm P dieses θ_P zuordnet, effektiv durch eine Registermaschine durchführbar ist.

Wenn es ein Entscheidungsverfahren für arithmetische Sätze geben würde, das die Richtigkeit von $\mathbb{N} \vDash \theta_P$ entscheiden könnte, so würde es auch ein Entscheidungsverfahren für das Halteproblem geben im Widerspruch zu Lemma 9.5. □

Folgerungen aus der Unentscheidbarkeit

Wir werden aus der Unentscheidbarkeit weitere Folgerungen über die Aufzählbarkeit und die Axiomatisierbarkeit der Arithmetik in der ersten Stufe ziehen. Dazu werden wir diese Begriffe allgemein für sogenannte Theorien einführen.

DEFINITION 11.3. Es sei A ein Symbolalphabet und L^A die zugehörige Sprache erster Stufe. Eine Teilmenge $T \subseteq L_0^A$ heißt *Theorie*, wenn T abgeschlossenen unter der Ableitungsbeziehung ist, d.h. wenn aus $T \vdash p$ bereits $p \in T$ folgt.

Zu jeder Ausdrucksmenge Γ ist die Menge $\Gamma^{\vdash}$ der aus Γ ableitbaren Sätze eine Theorie. Häufig wählt man „kleine“ und „handhabbare“ Mengen, um übersichtliche Theorien zu erhalten. Mengen, die eine Theorie erzeugen, heißen auch *Axiomensysteme* für diese Theorie. Es ist im Allgemeinen schwierig zu entscheiden, ob ein bestimmter Satz aus einem Axiomensystem ableitbar ist, also zu der entsprechenden Theorie dazugehört.

Wenn I eine Interpretation einer Sprache erster Stufe ist, so ist $I^{\vDash}$, also die Menge der in dem Modell gültigen Sätze, ebenfalls eine Theorie. Dies folgt direkt aus der Korrektheit des Ableitungskalküls. So ist $\mathbb{N}^{\vDash}$ eine Theorie zur Sprache L_0^{Ar}, die alle bei der Standardinterpretation gültigen Sätze beinhaltet.

Die Menge aller aus den Peano-Axiomen ableitbaren Sätze bildet die *Peano-Arithmetik*, die wir hier PA nennen. Es ist $\mathrm{PA} \subseteq \mathbb{N}^{\vDash}$.

Die Gesamtmenge L_0^A ist natürlich ebenfalls abgeschlossen unter der Ableitungsbeziehung. Sie ist widersprüchlich im Sinne der folgenden Definition.

Definition 11.4. Es sei A ein Symbolalphabet und L^A die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^A$ heißt *widersprüchlich*, wenn es einen Satz $p \in L_0^A$ gibt mit $p \in T$ und $\neg p \in T$.

Lemma 11.5. *Es sei A ein Symbolalphabet und L^A die zugehörige Sprache erster Stufe, wobei die Sprache zumindest eine Variable besitzen möge. Es sei $T \subseteq L_0^A$ eine Theorie. Dann ist T genau dann widersprüchlich, wenn $T = L_0^A$ ist.*

Beweis. Siehe Aufgabe 11.5. □

Man interessiert sich natürlich hauptsächlich für widerspruchsfreie (also nicht widersprüchliche) Theorien.

Definition 11.6. Es sei A ein Symbolalphabet und L^A die zugehörige Sprache erster Stufe. Eine Theorie T heißt *vollständig*, wenn für jeden Satz $p \in L_0^A$ gilt $p \in T$ oder $\neg p \in T$.

Dabei ist grundsätzlich auch erlaubt, dass sowohl p als auch $\neg p$ zu T gehört, doch liegt dann bereits eine widersprüchliche Theorie vor.

Zu einer Interpretation I einer Sprache erster Stufe ist die Gültigkeitsmenge $I^{\vDash}$ eine widerspruchsfreie vollständige Theorie. Dies ergibt sich aus dem rekursiven Aufbau der Gültigkeitsbeziehung (die beinhaltet, dass wir das Tertium non datur anerkennen - sonst wäre eine mathematische Argumentation nicht möglich).

Definition 11.7. Es sei A ein Symbolalphabet und L^A die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^A$ heißt *endlich axiomatisierbar*, wenn es endlich viele Sätze $p_1, \ldots, p_s \in L_0^A$ gibt mit $T = \{p_1, \ldots, p_s\}^{\vdash}$.

Das ist häufig zu viel verlangt, wie die einstufige Peano-Arithmetik zeigt (zumindest haben wir sie nicht durch ein endliches Axiomensystem eingeführt). Eine schwächere Variante wird in der folgenden Definition beschrieben.

Definition 11.8. Es sei A ein Symbolalphabet und L^A die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^A$ heißt *aufzählbar axiomatisierbar*, wenn es eine R-aufzählbare Satzmenge $\Gamma \subseteq L_0^A$ gibt mit $T = \Gamma^{\vdash}$.

LEMMA 11.9. *Es sei A ein Symbolalphabet und L^A die zugehörige Sprache erster Stufe. Eine aufzählbar axiomatisierbare Theorie $T \subseteq L_0^A$ ist R-aufzählbar.*

Beweis. Es sei Γ eine aufzählbare Satzmenge, die T axiomatisiert, und es sei p_n, $n \in \mathbb{N}_+$, eine Aufzählung von Γ. Es sei q_n, $n \in \mathbb{N}_+$, eine Aufzählung der prädikatenlogischen Tautologien aus L^A. Wenn ein Satz r aus Γ ableitbar ist, so gibt es eine endliche Auswahl $p_1, \ldots, p_n$ aus Γ (bzw. aus der gewählten Aufzählung) derart, dass

$$\vdash p_1 \wedge \ldots \wedge p_n \to r$$

eine prädikatenlogische Tautologie ist. Daher leistet das folgende Verfahren, bei dem n wächst, das Gewünschte: Für jedes n notiert man die Tautologien $q_1, \ldots, q_n$ in der Form

$$q_i = a_1 \wedge \ldots \wedge a_s \to b\,.$$

Wenn q_i überhaupt diese Form besitzt, so ist diese eindeutig betimmt. Danach überprüft man für jedes $i \leq n$, ob alle $a_1, \ldots, a_s$ zu $\{p_1, \ldots, p_n\}$ gehören. Falls ja, und wenn b ein Satz ist, so wird b notiert. Danach geht man zum nächsten i. Wenn man $i = n$ erreicht hat, so geht man zu $n+1$, wobei man aber wieder bei $i = 1$ anfängt. □

SATZ 11.10. *Es sei A ein Symbolalphabet und L^A die zugehörige Sprache erster Stufe. Jede aufzählbare (oder aufzählbar axiomatisierbare), widerspruchsfreie und vollständige Theorie $T \subseteq L_0^A$ ist entscheidbar.*

Beweis. Nach Lemma 11.9 bedeutet die aufzählbare Axiomatisierbarkeit, dass schon die Theorie selbst aufzählbar ist. Sei also T aufzählbar, vollständig und widerspruchsfrei, und sei p_n, $n \in \mathbb{N}_+$, eine Aufzählung von T. Es sei $q \in L_0^A$ ein Satz. Wegen der Widerspruchsfreiheit und der Vollständigkeit gilt entweder $q \in T$ oder $\neg q \in T$. Daher kommt entweder q oder $\neg q$ in der Aufzählung von T vor. Bei $p_n = q$ ist $q \in T$ und bei $p_n = \neg q$ ist $q \notin T$. □

BEMERKUNG 11.11. Ohne die Voraussetzung der Widerspruchsfreiheit ist obiges Argument nicht durchführbar. Eine widersprüchliche Theorie ist natürlich aufzählbar und vollständig. Es lässt sich aber an einer Aufzählung zu keinem Zeitpunkt mit Sicherheit ablesen, ob die Theorie widersprüchlich ist. Wenn bis zu einem bestimmten Zeitpunkt weder eine widersprüchliche Aussage noch eine Aussage und ihre Negation ausgegeben wurden, so lässt sich nicht entscheiden, ob dies an der Widerspruchsfreiheit der Theorie oder der Art der Aufzählung liegt.

SATZ 11.12. *Die Menge der wahren arithmetischen Ausdrücke ist nicht R-aufzählbar. D.h. es gibt kein R-Verfahren, das alle in $\mathbb{N}$ wahren Sätze der arithmetischen Sprache auflistet.*

Beweis. Dies folgt direkt aus Satz 11.10 und aus Satz 11.2. □