Prof. Dr. H. Brenner **Osnabrück SS 2018**

Einführung in die mathematische Logik

Vorlesung 21

> Für uns gibt es kein Ignorabimus, und meiner Meinung nach auch für die Naturwissenschaft überhaupt nicht. Statt des törichten Ignorabimus heiße im Gegenteil unsere Losung: Wir müssen wissen, wir werden wissen.
>
> David Hilbert

Zuletzt haben wir gezeigt, wir man die Programmabbildung zu einem Registerprogamm arithmetisch repräsentieren kann. Die Programmabbildung enthält zwar die volle Information über das Programm, doch die Frage, wie man die Eigenschaft, ob ein Programm anhält oder nicht, arithmetisch repräsentiert, ist damit noch nicht beantwortet, sondern bedarf weiterer Überlegungen.

Repräsentierbarkeit der Halteeigenschaft

Ein Durchlauf eines Registerprogramms P (das auf m Register Bezug nimmt) bis zum Rechenschritt t wird am einfachsten durch die Folge der Programmkonfigurationen K_s, $1 \leq s \leq t$, dokumentiert, 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 des Programms bis zum Schritt t korrekt dokumentiert. Man muss sicherstellen, 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 (der Abschnitt muss also durch die Programmabbildung aus dem Vorgängerabschnitt hervorgehen).

Lemma 21.1. *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. Es sei A_P der das Programm repräsentierende Ausdruck im Sinne von Lemma 20.4 in den Variablen $r_0, \ldots, r_m, r'_0, \ldots, r'_m$ (zur Notationsvereinfachung schreiben wir also r_0 statt z und r'_0 statt z'.). Es sei ϑ der Ausdruck (in den vier freien Variablen p, n, i, r), der die β-Funktion arithmetisch repräsentiert. Der Ausdruck

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

ist also genau dann wahr in $\mathbb{N}$, wenn[1] $\beta(p, n, i) = r$ 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 ist der Ausdruck (in den freien Variablen p, n, s, r_j, r'_j)

$$\begin{aligned} T(p, n, s) := &\vartheta(p, n, s(m+1), r_0) \wedge \ldots \wedge \vartheta(p, n, s(m+1) + m, r_m) \wedge \\ &\vartheta(p, n, (s+1)(m+1), r'_0) \wedge \ldots \wedge \vartheta(p, n, (s+1)(m+1) + m, r'_m) \end{aligned}$$

bei Interpretation in $\mathbb{N}$ genau dann wahr, wenn 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. An der mit $s(m+1)+j$ bezeichneten Stelle in $T(p, n, s)$ 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, dass der durch p, n, s über die β-Funktion kodierte Konfigurationsübergang durch das Programm bewirkt wird.

In analoger Weise ist der Ausdruck (in den $m+2$ freien Variablen $p, n, x_1, \ldots, x_m$)

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

[1] Wir verwenden hier für die Termvariablen und mögliche Einsetzungen die gleichen Buchstaben.

(bei inhaltlicher Interpretation) genau dann wahr, wenn $\beta(p,n,0) = 1$ und $\beta(p,n,j) = x_j$ für $j = 1,\ldots,m$ ist, und der Ausdruck (in den $m+3$ freien Variablen $p, n, t, y_1, \ldots, y_m$)

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

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

Somit besagt der Ausdruck

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

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 21.2. *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 vorgegebenen Ausdruck $\alpha \in L_0^{\mathrm{Ar}}$ der arithmetischen Sprache bestimmen kann, ob er (in der Standardinterpretation $\mathbb{N}$) wahr oder falsch ist.*

Beweis. Nach Lemma 21.1 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 der Belegung mit $e_1,\ldots,e_m,a_1,\ldots,a_m \in \mathbb{N}$ 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, so könnte man insbesondere auch die Richtigkeit von $\mathbb{N} \vDash \theta_P$ entscheiden. Doch dann würde es ein Entscheidungsverfahren für das Halteproblem im Widerspruch zu Satz 19.6 geben. □

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 21.3. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Teilmenge $T \subseteq L_0^S$ heißt *Theorie*, wenn T abgeschlossen unter der Ableitungsbeziehung ist, d.h. wenn aus $T \vdash \alpha$ für $\alpha \in L_0^S$ bereits $\alpha \in T$ 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 gehört.

Wenn I eine Interpretation einer Sprache erster Stufe ist, so ist $I_0^\vDash$, also die Menge der in dem Modell gültigen Sätze, ebenfalls eine Theorie. Dies folgt direkt aus der Korrektheit des Ableitungskalküls. So ist $\mathbb{N}_0^\vDash$ eine Theorie zur Sprache L_0^{Ar}, die alle bei der Standardinterpretation gültigen Sätze beinhaltet.

Die Menge aller aus den erststufigen Peano-Axiomen ableitbaren Sätze bildet die *Peano-Arithmetik*, die wir hier PA nennen. Es ist $\mathrm{PA} \subseteq \mathbb{N}_0^\vDash$.

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

Definition 21.4. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^S$ heißt *widersprüchlich*, wenn es einen Satz $\alpha \in L_0^S$ mit $\alpha \in T$ und $\neg\alpha \in T$ gibt.

Lemma 21.5. *Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe, wobei die Sprache zumindest eine Variable besitzen möge. Es sei $T \subseteq L_0^S$ eine Theorie. Dann ist T genau dann widersprüchlich, wenn $T = L_0^S$ ist.*

Beweis. Siehe Aufgabe 21.4. □

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

DEFINITION 21.6. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Theorie T heißt *vollständig*, wenn für jeden Satz $\alpha \in L_0^S$ gilt $\alpha \in T$ oder $\neg\alpha \in T$.

Dabei ist grundsätzlich auch erlaubt, dass sowohl α als auch $\neg\alpha$ zu T gehört, doch liegt dann bereits eine widersprüchliche Theorie vor. Zu einer Interpretation I einer Sprache erster Stufe ist die Gültigkeitsmenge $I_0^{\models}$ 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 21.7. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^S$ heißt *endlich axiomatisierbar*, wenn es endlich viele Sätze $\alpha_1, \ldots, \alpha_n \in L_0^S$ mit[2] $T = \{\alpha_1, \ldots, \alpha_n\}^{\vdash}$ gibt.

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

DEFINITION 21.8. Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine Theorie $T \subseteq L_0^S$ heißt *aufzählbar axiomatisierbar*, wenn es eine R-aufzählbare Satzmenge $\Gamma \subseteq L_0^S$ mit $T = \Gamma^{\vdash}$ gibt.

LEMMA 21.9. *Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Eine aufzählbar axiomatisierbare Theorie $T \subseteq L_0^S$ ist R-aufzählbar.*

Beweis. Es sei Γ eine R-aufzählbare Satzmenge, die T axiomatisiert, und es sei α_n, $n \in \mathbb{N}_+$, eine R-Aufzählung von Γ. Es sei β_n, $n \in \mathbb{N}_+$, eine R-Aufzählung der prädikatenlogischen Tautologien aus L^S. Wenn ein Satz γ aus Γ ableitbar ist, so gibt es eine endliche Auswahl $\alpha_1, \ldots, \alpha_n$ aus Γ (bzw. aus der gewählten Aufzählung) derart, dass

$$\vdash \alpha_1 \wedge \ldots \wedge \alpha_n \to \gamma$$

eine prädikatenlogische Tautologie ist. Daher leistet das folgende Verfahren, bei dem n wächst, das Gewünschte: Für jedes n notiert man die Tautologien $\beta_1, \ldots, \beta_n$ in der Form

$$\beta_i = \delta_1 \wedge \ldots \wedge \delta_s \to \epsilon.$$

Wenn β_i überhaupt diese Form besitzt, so ist diese eindeutig betimmt. Danach überprüft man für jedes $i \leq n$, ob alle $\delta_1, \ldots, \delta_s$ zu $\{\alpha_1, \ldots, \alpha_n\}$ gehören. Falls ja, und wenn ϵ ein Satz ist, so wird ϵ 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. □

[2]Das Ableitungssymbol schränken wir hier auf die Sätze ein, eigentlich müssten wir $T = \{\alpha_1, \ldots, \alpha_n\}^{\vdash} \cap L_0^S$ schreiben.

Satz 21.10. *Es sei S ein Symbolalphabet und L^S die zugehörige Sprache erster Stufe. Jede aufzählbare (oder aufzählbar axiomatisierbare), widerspruchsfreie und vollständige Theorie $T \subseteq L_0^S$ ist entscheidbar.*

Beweis. Nach Lemma 21.9 bedeutet die aufzählbare Axiomatisierbarkeit, dass schon die Theorie selbst aufzählbar ist. Sei also T aufzählbar, vollständig und widerspruchsfrei, und sei α_n, $n \in \mathbb{N}_+$, eine Aufzählung von T. Es sei $\beta \in L_0^S$ ein Satz. Wegen der Widerspruchsfreiheit und der Vollständigkeit gilt entweder $\beta \in T$ oder $\neg\beta \in T$. Daher kommt entweder β oder $\neg\beta$ in der Aufzählung von T vor. Bei $\alpha_n = \beta$ ist $\beta \in T$ und bei $\alpha_n = \neg\beta$ ist $\beta \notin T$. □

Bemerkung 21.11. Eine widersprüchliche Theorie ist natürlich aufzählbar, vollständig und entscheidbar, da sie jeden Satz enthält. Ohne die Voraussetzung der Widerspruchsfreiheit ist aber das Argument im Beweis zu Satz 21.10 nicht durchführbar. Wenn in einer Aufzählung einer Theorie eine widersprüchliche Aussage auftritt, so ist die Theorie natürlich widersprüchlich. Wenn aber bis zu einem bestimmten Zeitpunkt keine widersprüchliche Aussage auftritt, so lässt sich nicht entscheiden, ob dies an der Widerspruchsfreiheit der Theorie oder der Art der Aufzählung liegt. Wenn also in der Aufzählung $\neg\beta$ vorkommt, so kann man daraus nicht ohne die Bedingung der Widerspruchsfreiheit auf $\beta \notin T$ schließen.

Satz 21.12. *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 21.10 und aus Satz 21.2. □

Korollar 21.13. *Die (erststufige) Peano-Arithmetik ist unvollständig.*

Beweis. Wegen $PA \subseteq \mathbb{N}^{\vdash}$ würde die Vollständigkeit hier die Gleichheit bedeuten. Da die Peano-Arithmetik R-aufzählbar ist, würde aus Satz 21.10 die Entscheidbarkeit folgen im Widerspruch zu Satz 21.2. □

Die Lücke zwischen PA und $\mathbb{N}_0^{\vdash}$ kann man nicht systematisch auffüllen, da man das vorstehende Argument auf jede aufzählbar-axiomatisierbare Theorie T mit $PA \subseteq T \subseteq \mathbb{N}_0^{\vdash}$ anwenden kann.