Unentscheidbarkeit des Gültigkeitsproblems

Wir gehen in zwei Schritten vor:

- Das Terminierungsproblem ist unentscheidbar.
  Es gibt kein Programm, welches als Eingabe ein Programm P und eine Belegung β der Variablen von P akzeptiert und entscheidet, ob P mit β als Anfangsbelegung terminiert.
- Wenn das Gültigkeitsproblem entscheidbar wäre, dann wäre auch das Terminierungsproblem entscheidbar.

Kodierungen

Fakt: Sowohl Programme als auch Anfangsbelegungen können als Integer kodiert werden.

Wir beschränken uns auf Programme, deren Eingabe aus einem Tupel von Integern besteht. Wir nehmen an, dass Variablen $x_1, \ldots, x_n$ mit dieser Eingabe initialisiert werden.
Einige Notationen:

- $P(a_1, \ldots, a_i)$ bezeichnet das Programm P mit der Anfangsbelegung $(a_1, \ldots, a_i, 0, \ldots, 0)$.
  D.h., die Variablen $x_1, \ldots, x_i$ bekommen Anfangswerte $a_1, \ldots, a_i$ und die Variablen $x_{i+1}, \ldots, x_n$ den Anfangswert 0.
- Π_n bezeichet das Programm mit dem Code n (wenn es ein solches Programm gibt).

Berechenbare Kodierungen

Fakt: Es gibt berechenbare Kodierungen, d.h., Kodierungen, für die die folgenden zwei Programme existieren:

- Der Kodierer.
  Eingabe: ein Programm P.
  Ausgabe: der Code von P, d.h., die Zahl n mit $P = \Pi_n$.
- Der Dekodierer.
  Eingabe: eine Zahl n.
  Ausgabe: das Programm Π_n falls n ein Programm kodiert, sonst 'KP' (Kein Programm).

Annahme: Es gibt ein Programm T, so dass für jedes Paar $n, m \in \mathbb{N}$ das initialisierte Programm $T(n, m)$ terminiert und zwar mit

KP	falls n kein Programm kodiert
JA	falls n ein Programm kodiert und $\Pi_n(m)$ terminiert
NEIN	falls n ein Programm kodiert und $\Pi_n(m)$ nicht terminiert

Wir zeigen, dass diese Annahme zu einem Widerspruch führt.

Der Widerspruch

Fakt: Aus der Annahme folgt, dass es ein Programm T' gibt, so dass für jedes $n \in \mathbb{N}$ das initialisierte Programm $T'(n)$

terminiert	falls n ein Programm kodiert und $\Pi_n(n)$ nicht terminiert
nicht terminiert	falls n kein Programm kodiert oder $\Pi_n(n)$ terminiert

Sei k der Code des Programms T', d.h. $\Pi_k = T'$. Das initialisierte Programm $T'(k)$ terminiert oder terminiert nicht. Wir haben jedoch:

$$
\begin{array}{lll}
 & T'(k) \text{ terminiert} & \\
\Longrightarrow & k \text{ kodiert ein Programm und} & \\
 & \Pi_k(k) \text{ terminiert nicht} & (\text{Def. von } T') \\
\Longrightarrow & T'(k) \text{ terminiert nicht} & (\Pi_k = T')
\end{array}
$$

$$
\begin{array}{lll}
 & T'(k) \text{ terminiert nicht} & \\
\Longrightarrow & \Pi_k(k) \text{ terminiert} & (\text{Def. von } T', \text{ denn } k \text{ ist Code}) \\
\Longrightarrow & T'(k) \text{ terminiert} & (\Pi_k = T')
\end{array}
$$

Damit ist die Annahme falsch.

Unentscheidbarkeit des Gültigkeitsproblems

Wir ordnen jedem Programm P und Variablenbelegung β
eine Formel $\phi_{P\beta}$ der Prädikatenlogik zu mit

$\phi_{P\beta}$ ist gültig

genau dann, wenn

das Programm P mit der Anfangsbelegung β terminiert

Die Formel $\phi_{P\beta}$ kann von einem Programm konstruiert werden.

Daraus folgt, dass kein Programm das Gültigkeitsproblem der Prädikatenlogik lösen kann.

if-goto-Programme

$$
\begin{array}{rcll}
\mathit{Prog} & ::= & \ell : \mathit{Zuw} & \text{(Zuweisung)} \\
 & & \ell : \ \mathbf{goto}\ \ell' & \text{(unbedingter Sprung)} \\
 & & \ell : \mathbf{if}\ x_i \neq 0\ \mathbf{then\ goto}\ \ell' & \text{(bedingter Sprung)} \\
 & & \ell : \mathbf{halt} & \text{(Terminierung)} \\
 & & \mathit{Prog}\ ;\ \mathit{Prog} & \text{(Hintereinanderausführung)}
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{Zuw} & ::= & x_i := 0 \ \mid \ x_i := x_j \\
 & & x_i := x_j + 1 \ \mid \ x_i := x_j - 1 \\
\ell & ::= & 1 \mid 2 \mid 3 \mid \ldots
\end{array}
$$

Beispiel

1: **if** $x_1 = 0$ **then goto** 4;

2: $x_1 := x_1 - 1$;

3: **goto** 1;

4: **halt**

Wir haben gezeigt: kein **if-goto**-Programm löst das Terminierungsproblem für **if-goto**-Programme.

Behauptung: **if-goto**-Programme können alle anderen Programme simulieren.

Konsequenz: Es gibt kein Programm, egal in welcher Sprache, für die Terminierung von **if-goto**-Programmen

Notationen und Definitionen

Mit k bezeichnen wir die Anzahl der Anweisungen von P
(Die letzte Anweisung ist immer $\mathbf{halt}$)

Mit n bezeichnen wir die Anzahl der Variablen von P
(D.h. die Variablen von P sind $x_1, \ldots, x_n$)

Eine Konfiguration von P ist eine Tupel $(Z, m_1, \ldots, m_n) \in \mathbb{N}^{n+1}$.
Z bezeichnet die aktuelle Anweisung und $m_1, \ldots m_n$ die aktuelle Belegung der Variablen

Konvention: die Nachfolgekonfiguration einer Konfiguration der Gestalt $(\ell_k, m_1, \ldots, m_n)$ ist wieder $(\ell_k, m_1, \ldots, m_n)$

Symbole der Formel $\phi_{P\beta}$

- R, Prädikatensymbol, $(n+2)$-stellig.
- $<$, Prädikatensymbol, 2-stellig.
- f, Funktionssymbol, 1-stellig.
- $\mathbf{0}$, Konstante.

Die kanonische Interpretation $\mathcal{A}$

- Universum: $\mathbb{N}$.
- $<^{\mathcal{A}}$ ist die gewöhnliche Ordnung auf $\mathbb{N}$.
- $\mathbf{0}^{\mathcal{A}} = 0$.
- $f^{\mathcal{A}}$ ist die Nachfolgerfunktion, i.e., $f^{\mathcal{A}}(n) = n + 1$.
- $R^{\mathcal{A}}(s, Z, m_1, \ldots, m_n) = 1$ wenn $(Z, m_1, \ldots, m_n)$ die Konfiguration von P nach s Schritten ist (für die Anfangsbelegung β).

Die Hilfsformel $\psi_{P\beta}$

$$\psi_{P\beta} = \quad \psi_0 \quad \wedge \quad R(\mathbf{0}, \beta) \quad \wedge \quad \psi_1 \quad \wedge \quad \ldots \quad \wedge \quad \psi_{k-1}$$

Unter der Interpretation $\mathcal{A}$ besagt $R(\mathbf{0}, \beta)$, dass β die Anfangsbelegung des Programms P ist

Unter der Interpretation $\mathcal{A}$ beschreibt ψ_i die Wirkungsweise der i-te Zeile von P. Zum Beispiel:

- Wenn die i-te Zeile die Gestalt i: $x_j := x_j + 1$ hat, dann

$$\begin{aligned} \psi_i \quad = \quad & \forall x \forall y_1 \ldots \forall y_n \ (\\ & R(x, f^i(\mathbf{0}), y_1, \ldots y_n) \quad \rightarrow \\ & R(f(x), f^{(i+1)}(\mathbf{0}), y_1, \ldots y_{j-1}, f(y_j), y_{j+1}, \ldots, y_n) \\ &) \end{aligned}$$

- Wenn die **i**-te Zeile die Gestalt i: $\mathbf{if}\ x_j = 0\ \mathbf{then\ goto}\ j$ hat, dann

$$
\begin{aligned}
\psi_i \quad = \quad & \forall x \forall y_1 \ldots \forall y_n \ (\\
& R(x, f^i(\mathbf{0}), y_1, \ldots y_n) \rightarrow \\
& \quad (\quad y_j = \mathbf{0} \quad \wedge \quad R(f(x), f^j(\mathbf{0}), y_1, \ldots, y_n) \\
& \qquad \vee \\
& \quad \neg(y_j = \mathbf{0}) \quad \wedge \quad R(f(x), f^{(i+1)}(\mathbf{0}), y_1, \ldots, y_n) \\
& \quad) \\
&)
\end{aligned}
$$

ψ_0 garantiert, dass in allen Modellen $<$ eine Ordnung mit $\mathbf{0}$ als kleinstem Element ist, daß stets $x < f(x)$ gilt, und dass $f(x)$ der unmittelbare $<$-Nachfolger von x ist:

$$
\begin{aligned}
\psi_0 \quad = \quad & \forall x \forall y (x < y \rightarrow \neg (y < x)) \quad \wedge \\
& \forall x \forall y \forall z ((x < y \wedge y < z) \rightarrow x < z) \quad \wedge \\
& \forall x (\mathbf{0} < x \vee \mathbf{0} = x) \quad \wedge \\
& \forall x (x < f(x)) \quad \wedge \\
& \forall x \forall z (x < z \rightarrow (f(x) < z \vee f(x) = z)
\end{aligned}
$$

Die Formel $\phi_{P\beta}$

Wir setzen

$$\phi_{P\beta} \quad = \quad \psi_{P\beta} \quad \longrightarrow \quad \exists x \exists y_1 \ldots \exists y_n \;\; R(x, f^k(\mathbf{0}), y_1, \ldots, y_n)$$

Satz: $\phi_{P\beta}$ ist gültig genau dann, wenn das Programm P mit der Anfangsbelegung β terminiert

Beweis: ($\Rightarrow$): Wenn $\phi_{P\beta}$ gültig ist, dann ist insbesondere die kanonische Interpretation $\mathcal{A}$ Modell von $\phi_{P\beta}$. Da $\mathcal{A} \models \psi_{P\beta}$ offenscichtlich gilt haben wir
$\mathcal{A} \models \exists x \exists y_1 \ldots \exists y_n \;\; R(x, f^k(\mathbf{0}), y_1, \ldots, y_n)$. Es folgt, dass P mit Anfangsbelegung β terminiert.

($\Leftarrow$): (Skizze.) Wenn $\phi_{P\beta}$ nicht gültig ist, dann gibt es eine Struktur $\mathcal{B} = (U_\mathcal{B}, I_\mathcal{B})$ mit

$$\mathcal{B} \models \psi_{P\beta} \text{ und } \mathcal{B} \not\models \exists x \exists y_1 \ldots \exists y_n \; R(x, f^k(\mathbf{0}), y_1, \ldots, y_n) \, .$$

Für jedes $i \geq 0$ sei d_i das Element von $U_\mathcal{B}$ mit $(f^i(\mathbf{0}))^\mathcal{B} = d_i$. Aus $\mathcal{B} \models \psi_{P\beta}$ folgt $\mathcal{B} \models \psi_0$, und damit gilt (warum?):

- $d_0 <^\mathcal{B} d_1 <^\mathcal{B} d_2 \ldots$,
- $d_i = d_j$ gdw. $i = j$, und
- für alle $d \in U_\mathcal{B}$: wenn $f^\mathcal{B}(d) = d_i$ dann $d = d_{i-1}$.

Sei $(Z, m_1, \ldots, m_n)$ die Konfiguration von P nach s Schritten (für die Anfangsbelegung β). Aus $\mathcal{B} \models \psi_{P\beta}$ folgt $R^\mathcal{B}(d^{s_i}, d^{Z_i}, d^{m_{1i}}, \ldots, d^{m_{1n}})$ für alle $i \geq 0$. Mit $\mathcal{B} \not\models \exists x \exists y_1 \ldots \exists y_n \; R(x, f^k(\mathbf{0}), y_1, \ldots, y_n)$ gilt, daß P mit β als Anfangsbelegung nicht terminiert.

Ein alternativer Beweis

Das Parkettierungsproblem:
Gegeben: endliche Menge quadratischer Dominosteine mit fester Orientierung und beschrifteten Rändern: oben, links, unten, rechts. Ein Stein wird durch zwei Diagonalen in vier Dreiecke geteilt, die gefärbt sind.
Frage: Kann man die Ebene so parkettieren, dass horizontal oder vertikal nebeneinanderliegende Dominosteine auf den anstoßenden Rändern dieselbe Farbe tragen?

Satz: Das Parkettierungsproblem ist unentscheidbar.

Die Reduktion

Wir definieren für jede Menge S von Dominosteine eine Formel ϕ_S mit: ϕ_S ist erfüllbar genau dann, wenn mit S die Ebene parkettiert werden kann.

Symbole: ein zweistelliges Prädikatensymbol P_s für jeden Stein $s \in S$, ein einstelliges Funktionsymbol f.

Kanonische Struktur $\mathcal{A}$:

- Universum: $\mathbb{Z} \times \mathbb{Z}$.
- $f^{\mathcal{A}}$ ist die Nachfolgerfunktion, i.e., $f^{\mathcal{A}}(n) = n + 1$.
- $(i, j) \in P_s$ wenn auf dem Punkt mit Koordinaten (i, j) den Stein s liegt.

Die Formel ϕ_S

Sei H die Menge der Paare (s, s') von Steinen, so dass s' rechts von s platziert werden kann.
Sei V die Menge der Paare (s, s') von Steinen, so dass s' über s platziert werden kann.
Wir nehmen $\phi_S = \forall x \forall y (F_1 \wedge F_2)$ mit

$$
\begin{aligned}
F_1 &= \bigwedge_{s \neq s'} \neg (P_s(x, y) \wedge P_{s'}(x, y)) \\
F_2 &= \bigvee_{(s,s') \in H} (P_s(x, y) \wedge P_{s'}(f(x), y)) \ \wedge \\
&\quad \bigvee_{(s,s') \in V} (P_s(x, y) \wedge P_{s'}(x, f(y)))
\end{aligned}
$$

Korollar: Das Erfüllbarkeitsproblem ist unentscheidbar für Formeln der Gestalt $F = \forall x \forall y F^*$.

Korollar: Das Erfüllbarkeitsproblem ist unentscheidbar für Formeln der Gestalt $F = \forall x \exists z \forall y F^*$, wobei F^* keine Funktionssymbole enthält.

Präfixklassen

Wir betrachten Klassen von Formeln in Pränex-Normalform ohne Funktionssymbole.

Unentscheidbare Klassen:

- $\forall^*\exists^*$ (Skolem, 1920)
- $\forall\forall\forall\exists$ (Suranyi, 1959)
- $\forall\exists\forall$ (Kahr, Moore, Wang, 1962)

Entscheidbare Klassen:

- $\exists^*\forall^*$ (Bernays, Schönfinkel, 1928)
- $\exists^*\forall\exists^*$ (Ackerman, 1928)
- $\exists^*\forall^2\exists^*$ (Gödel 1932, Kalmar 1933, Schütte 1934)