„$\Leftarrow$": analog: Eine Lösung von $f(\langle M \rangle w)$ liefert eine Folge von Konfigurationen, die einer akzeptierenden Berechnung von TM M auf Eingabe w entspricht.

(c) $\rightarrow$ Blatt 7.

□

Satz (Alonzo Church, 1936)

Das Erfüllbarkeitsproblem der Prädikatenlogik (gg.: prädikatenlogische Formel F, gefragt: Ist F erfüllbar?) ist nicht rekursiv:

$$PKP \leq \text{Gültigkeitsproblem} \leq \text{Erfüllbarkeitsproblem}$$

(gg.: F, gefragt: $\models F$?)

Bew.: „Gültigkeit $\leq$ Erfüllbarkeit"

Klar: F gültig gdw. $\neg F$ unerfüllbar.

„PKP ≤ Gültigkeit"

Können oBdA PKP mit Alphabet $\Sigma = \{0,1\}$ betrachten ($\rightarrow$ Blatt 6, Aufgabe 4).

Sei $K = ((x_1, y_1), \ldots, (x_k, y_k))$

eine Eingabe für PKP.

Definiere prädikatenlogische Formel $f(K) = F_K$:

$$F_K = ((F_1 \wedge F_2) \Rightarrow F_3),$$

mit

$$F_1 = \bigwedge_{i=1}^{k} P(f_{x_i}(a), f_{y_i}(a))$$

$$F_2 = \forall u \forall v \left(P(u,v) \Rightarrow \bigwedge_{i=1}^{k} P(f_{x_i}(u), f_{y_i}(v))\right)$$

$$F_3 = \exists z\, P(z,z),$$

wobei f_0, f_1 zwei einstellige Fkt.symbole sind, a eine Konstante, und $f_{j_k \ldots j_2 j_1}(x) = f_{j_1}(f_{j_2}(\ldots f_{j_k}(x)\ldots))$ mit $j_i \in \{0,1\}$, ist.

Klar: F_K ist aus K mit Hilfe einer TM berechenbar.

F_K gültig $\Rightarrow$ K hat Lösung

Für jede zu F_K passende Struktur $\mathcal{A} = (U_{\mathcal{A}}, I_{\mathcal{A}})$ ist $\mathcal{A} \models F$. Insbesondere ist folgender $\mathcal{A}$ ein Modell von F_K:

$$U_{\mathcal{A}} = \{0,1\}^*$$

$$I_{\mathcal{A}}(a) = \varepsilon \quad \text{(das leere Wort)}$$

$$I_{\mathcal{A}}(f_0)(\alpha) = \alpha 0$$

$$I_{\mathcal{A}}(f_1)(\alpha) = \alpha 1$$

$$I_{\mathcal{A}}(P) = \{(\alpha,\beta) : \alpha,\beta \in \{0,1\}^*,\ \alpha,\beta \neq \varepsilon,$$
es gibt Indizes $i_1,\dots,i_n$ mit
$\alpha = x_{i_1} x_{i_2} \dots x_{i_n}$ und
$\beta = y_{i_1} y_{i_2} \dots y_{i_n}\}$.

Es ist dann

$$f_{x_i}(a) = x_i, \quad f_{y_i}(a) = y_i.$$

Somit $\mathcal{A} \models F_1$ und auch $\mathcal{A} \models F_2$.

Also, weil $\mathcal{A} \models F$, muss auch $\mathcal{A} \models F_3$.

Dies bedeutet, dass es ein Wort $z \in \{a,b\}^*$ gibt, dass man schreiben kann als

$$z = \alpha = \beta$$

und $\alpha = x_{i_1} \dots x_{i_n}$, $\beta = y_{i_1} \dots y_{i_n}$, also hat das PKP K eine Lösung.

<u>K hat Lösung $\Rightarrow$ F_K gültig</u>

Sei $i_1, \dots, i_n$ eine Lösung von K.

Sei $\mathcal{A}$ eine zu F_K passende Struktur.

Falls $\mathcal{A} \not\models F_1$ oder $\mathcal{A} \not\models F_2$, dann $\mathcal{A} \models F$.

Wir können also annehmen, dass $\mathcal{A} \models F_1 \wedge F_2$.

Definiere Abbildung

$$\mu : \{0,1\}^* \to U_{\mathcal{A}}$$

induktiv durch

$$\mu(\varepsilon) = I_{\mathcal{A}}(a)$$

$$\mu(x0) = I_{\mathcal{A}}(f_0)(\mu(x))$$

$$\mu(x1) = I_{\mathcal{A}}(f_1)(\mu(x))$$

Also $\mu(x) = I_{\mathcal{A}}(f_x)(I_{\mathcal{A}}(a))$, z.B.

$$\mu(011) = I_{\mathcal{A}}(f_{011})(I_{\mathcal{A}}(a))$$

Weil $\mathcal{A} \models F_1$ gilt $(\mu(x_i), \mu(y_i)) \in I_{\mathcal{A}}(P)$ für $i = 1, \dots, k$

Weil $\mathcal{A} \models F_2$ gilt: aus $(\mu(u), \mu(v)) \in I_{\mathcal{A}}(P)$ folgt

$$\mu(ux_i, vy_i) \in I_{\mathcal{A}}(P)$$

Somit per Induktion:

$$(\underbrace{\mu(x_{i_1} x_{i_2} \dots x_{i_n})}_{z}, \underbrace{\mu(y_{i_1} y_{i_2} \dots y_{i_n})}_{z}) \in I_{\mathcal{A}}(P)$$

, weil $i_1, \dots, i_n$ Lösung von K.

Also gilt $\mathcal{A} \models \exists z\, P(z,z)$, und so $\mathcal{A} \models F$. ⊠

Weitere, wichtige unentscheidbare Probleme:

- Hilberts 10. Problem

  Hat $f \in \mathbb{Z}[x_1, \dots x_n]$ eine ganzzahlige Lösung?

  (Matiyasevich, 1970)

- Das Wortproblem in Gruppen

  Gegeben eine Gruppe durch eine endliche Präsentation,

  $G = \langle g_1, \dots, g_k \mid \text{Relationen (z.B. } g_1 g_2 = g_2 g_1) \rangle$,

  und ein $w = g_{i_1} g_{i_2} \dots g_{i_n}$. Ist w das neutrale Element?

  (Novikov, 1955)

- Wang-Parkettierungen

  Gegeben eine Menge von Wang-Dominos 

.

  Kann man damit die Ebene parkettieren? (Berger, 1966).