Folgerung 4.30 (Satz von Löwenheim-Skolem):

Jede erfüllbare Formel der Prädikatenlogik erster Stufe besitzt ein Modell $M = (D, I)$, dessen Datenbereich D abzählbar ist.

Beweis (Skizze):

- Jede Formel $A \in FO(S)$ kann in eine geschlossene erfüllbarkeitsäquivalente Formel
  $$B \in FO^{\neq}(S \cup Sko)$$ in Skolemform
  überführt werden.
  Ist also A erfüllbar, dann ist auch B erfüllbar.
- Mit dem Satz von Herbrand hat B ein Herbrand-Modell.
- Die Umformungen von A nach B erlauben es aber, das Modell für B auch für A zu nutzen
  (Eliminierung von Gleichheit (=) erfordert Faktorisierung nach $I_H(g)$).
- Dieses (faktorisierte) Herbrand-Modell hat einen abzählbaren Datenbereich. $\square$

Beispiel (Herbrand-Expansion):

$A \equiv \forall x \forall y \forall z : p(a, f(y), g(z, x))$

Dann enthält $E(A)$ unter anderem folgende Formeln:

$p(a, f(a), g(a, a))$ mit $\{x/a\}\{y/a\}\{z/a\}$

$p(a, f(a), g(a, f(a)))$ mit $\{x/f(a)\}\{y/a\}\{z/a\}$

$p(a, f(f(a)), g(a, a))$ mit $\{x/a\}\{y/f(a)\}\{z/a\}$

...

Beobachtung:

- Die Formeln in $E(A)$ lassen sich wie aussagenlogische Formeln behandeln.
- Genauer: Es genügt, ein Herbrand-Modell H zu finden.
  - ↳ Die Formeln in $E(A)$ enthalten keine Variablen.
    - ⇒ Damit legt H nur den Wahrheitswert der atomaren Formeln $p(t_1, \ldots, t_n)$ fest.
  - ↳ Außerdem interpretiert H die Funktionssymbole nicht, insbesondere $I_H(t) \neq I_H(t')$, falls $t \not\equiv t'$.
    - ⇒ Damit entspricht das Festlegen des Wahrheitswerts für atomare Formeln $p(t_1, \ldots, t_n)$ dem Festlegen des Wahrheitswerts für aussagenlogische Variablen (die auch $p(t_1, \ldots, t_n)$ heißen).

Beweis (Satz von Gödel-Herbrand-Skolem):

Zeige:

A hat ein Herbrand-Modell gdw.

$E(B)$ ist in aussagenlogischem Sinn erfüllbar.

Sei $A \equiv \forall y_1 \ldots \forall y_n . B$.

Es gilt:

H ist Herbrand-Modell für A

gdw. für alle $t_1, \ldots, t_n \in D_H$ gilt:

$$H[\![B]\!](\{y_1/t_1\} \ldots \{y_n/t_n\}) = 1$$

(Herbrand) gdw. für alle $t_1, \ldots, t_n \in D_H$ gilt:

$$H[\![B]\!](\{y_1/H[\![t_1]\!]\} \ldots \{y_n/H[\![t_n]\!]\}) = 1$$

(Substitutions-lemma) gdw. für alle $t_1, \dots, t_n \in D_H$ gilt:

$$H[\![B[y_1/t_1]\dots[y_n/t_n]]\!] = 1$$

(Def. $E(A)$) gdw. für alle $G \in E(A)$ gilt:

$$H[\![G]\!] = 1.$$

(Argumentation oben) gdw. H erfüllt $E(A)$ als Menge aussagenlogischer Formeln. $\square$

Beispiel (PCP):

Betrachte die PCP-Instanz

$$I = (\underbrace{(1}_{x_1}, \underbrace{101}_{y_1}), (\underbrace{10}_{x_2}, \underbrace{00}_{y_2}), (\underbrace{011}_{x_3}, \underbrace{11}_{y_3}))$$

Dann ist 1.3.2.3 eine Lösung, denn

$$x_1 x_3 x_2 x_3 = 101110011 = y_1 y_3 y_2 y_3.$$

Beweis (Satz von Church):

Definiere die Funktion

$$f : PCP \longrightarrow \text{Allgemeingültigkeit},$$

so dass (A)

PCP-Instanz I hat Lösung gdw. FO-Formel $f(I)$ ist allgemeingültig.

Mit Terminologie der Folien ist f also eine many-one Reduktion.

Als Signatur wähle

$$S = (\{f_0/1, f_1/1, a/0\}, \{p/2\}).$$

Verwende die Abkürzung

$$f_{j_1 \dots j_l}(x) := f_{j_l}(\dots(f_{j_1}(x))\dots).$$

Sei die PCP-Instanz

$$I = ((x_1, y_1), \dots, (x_n, y_n)).$$

Definiere

$$f(I) \equiv A_1 \wedge A_2 \rightarrow A_3,$$

wobei

$$A_1 \equiv \bigwedge_{i=1}^{n} p(f_{x_i}(a), f_{y_i}(a))$$

$$A_2 \equiv \forall x \forall y : p(x, y) \longrightarrow \bigwedge_{i=1}^{n} p(f_{x_i}(x), f_{y_i}(y))$$

$$A_3 \equiv \exists z : p(z, z).$$

Intuition:

- Gelte $p(\alpha, \beta)$ mit $\alpha, \beta \in \{0,1\}^*$.
  Das heißt, es gibt Indizes $i_1, \dots, i_k$,
  so dass
  $$\alpha = x_{i_1} \dots x_{i_k} \quad \text{und} \quad \beta = y_{i_1} \dots y_{i_k}.$$
- A_3 besagt nun, dass
  $$x_{i_1} \dots x_{i_k} = y_{i_1} \dots y_{i_k},$$
  die PCP-Instanz hat also eine Lösung.

Zeige (Δ):

I hat Lösung gdw. $f(I)$ ist allgemeingültig.

Beweis:

„$\Leftarrow$" Angenommen $f(I)$ ist allgemeingültig.

Dann gilt für jede S-Struktur $\mathcal{M}$,
dass

$$\mathcal{M} \models \varphi(I).$$

- Betrachte $\mathcal{M} = (D, I)$ mit

$D := \{0,1\}^*$ // Endliche Worte über 0,1.

$I(a) := \varepsilon$ // Leeres Wort

$I(f_0)(\alpha) := \alpha.0$ // Konkatenation von 0

$I(f_1)(\alpha) := \alpha.1$ // Konkatenation von 1.

$I(p)(\alpha,\beta) := 1$ gdw.
es gibt Indizes $i_1, \dots, i_k$ mit
$\alpha = x_{i_1} \dots x_{i_k}$ und $\beta = y_{i_1} \dots y_{i_k}$.

- Natürlich ist $\mathcal{M}$ eine S-Struktur.
Also gilt $\mathcal{M} \models \varphi(I)$.
Ferner gilt $\mathcal{M} \models A_1$ und $\mathcal{M} \models A_2$.
Also folgt $\mathcal{M} \models A_3$.
- Das heißt, es gibt $\beta \in \{0,1\}^*$ mit
$$I(p)(\beta,\beta) = 1.$$
Also gibt es Indizes $i_1, \dots, i_k$ mit
$$\beta = x_{i_1} \dots x_{i_k} \text{ und } \beta = y_{i_1} \dots y_{i_k}.$$
Also hat I eine Lösung.

„$\Rightarrow$" Sei $i_1 \dots i_k$ eine Lösung von I,
also
$$x_{i_1} \dots x_{i_k} = y_{i_1} \dots y_{i_k}.$$
Sei $\mathcal{M} = (D, I)$ eine S-Struktur.
<u>Zeige</u>: $\mathcal{M} \models \varphi(I)$.

- Falls $\mathcal{M} \not\models A_1$ oder $\mathcal{M} \not\models A_2$,

  dann

  $$\mathcal{M} \models f(I), \text{ denn } f(I) \equiv A_1 \wedge A_2 \to A_3.$$

- Nimm also an, dass

  $$\mathcal{M} \models A_1 \text{ und } \mathcal{M} \models A_2.$$

- Um $\mathcal{M} \models A_3$ zu zeigen,

  definiere die Einbettung

  $$\mu : \{0,1\}^* \longrightarrow D$$

  mittels

  $$\mu(\varepsilon) := I(a)$$
  $$\mu(x.0) := I(f_0)(\mu(x))$$
  $$\mu(x.1) := I(f_1)(\mu(x)).$$

  Zum Beispiel

  $$\mu(0.1) = I(f_1)(\ I(f_0)(I(a))\ )$$

  Allgemein

  $$\mu(j_1 \dots j_\ell) = I(f_{j_1 \dots j_\ell})(I(a)).$$

- Da $\mathcal{M} \models A_1$, gilt für $i = 1, \dots, n$:

  $$I(p)(\mu(x_i), \mu(y_i))$$
  $$= I(p)(\ I(f_{x_i})(I(a)), I(f_{y_i})(I(a))\ )$$
  $$= 1$$

  Da $\mathcal{M} \models A_2$, folgt aus

  $$I(p)(\mu(\alpha), \mu(\beta)) = 1,$$

  dass

  $$I(p)(\mu(\alpha.x_i), \mu(\beta.y_i)) = 1.$$

Zusammen gilt also insbesondere

$$I(p)(\mu(x_{i1} \dots x_{ik}), \mu(y_{i1} \dots y_{ik})) = 1.$$

- Da aber $x_{i1} \dots x_{ik} = y_{i1} \dots y_{ik}$, folgt

$$I(p)(u, u) = 1 \quad \text{mit} \quad u = \mu(x_{i1} \dots x_{ik}).$$

Es folgt

$$\mathcal{M} \models \exists z : p(z, z).$$

Damit gilt

$$\mathcal{M} \models f(I).$$

$\square$