Kapitel 9: Die Grenzen der Berechenbarkeit

9.1 Entscheidbarkeit und rekursive Aufzählbarkeit

Zur Erinnerung: Definition 9.0:

Sei M eine abzählbare Menge.

(a) Eine Menge $L \subseteq M$ heißt entscheidbar, falls es einen Algorithmus gibt, der bei Eingabe eines $m \in M$ nach endlich vielen Schritten anhält und ausgibt

- "JA", falls $m \in L$
- "NEIN", falls $m \notin L$.

(b) Eine Menge $L \subseteq M$ heißt semi-entscheidbar, falls es einen Algorithmus gibt, der bei Eingabe eines $m \in M$

- nach endlich vielen Schritten anhält und dann "JA" ausgibt, falls $m \in L$ ist
- nie anhält, falls $m \notin L$ ist.

(c) Eine Menge $L \subseteq M$ heißt rekursiv aufzählbar (engl.: recursively enumerable, kurz: r.e.), falls es einen Algorithmus gibt, der nach und nach sämtliche Elemente in L ausgibt

(d) Sei M' eine Menge.
Eine Funktion $f: M \to M'$ heißt berechenbar, falls es einen Algorithmus gibt, der bei Eingabe eines $m \in M$ nach endlich vielen Schritten anhält und den Wert $f(m)$ ausgibt.

Bemerkung:
Ist $M = A^*$, wobei A ein endliches Alphabet ist, so kann man leicht sehen, dass folgendes gilt:

(a) Eine Menge $L \subseteq M$ ist semi-entscheidbar genau dann, wenn sie rekursiv aufzählbar ist

(b) Jede entscheidbare Menge $L \subseteq M$ ist rekursiv aufzählbar

(c) Sind $L_1 \subseteq M$ und $L_2 \subseteq M$ zwei rekursiv aufzählbare Mengen, so ist auch die Menge $L_1 \cap L_2$ rekursiv aufzählbar.

(d) Sind $L \subseteq M$ und $\overline{L} := M \setminus L \subseteq M$ rekursiv aufzählbar, so ist $L \subseteq M$ entscheidbar.

Vereinbarungen zur Kodierung der Syntax von FO[σ]-Formeln:

- In diesem Kapitel sei σ eine abzählbare entscheidbare Signatur.
  Die Symbole aus σ sind kodiert als Wörter über einem endlichen Alphabet, etwa dem ASCII-Alphabet
- Wir kodieren σ-Terme und FO[σ]-Formeln als Wörter über einem endlichen Alphabet
- Wir erweitern die Kodierung auf endliche Mengen von σ-Termen und FO[σ]-Formeln
- Wir kodieren Ableitungen im Sequenzenkalkül $\mathfrak{S}$ (vgl. Kapitel 7) als Wörter über einem endlichen Alphabet

Sei $\mathbb{A}$ das endliche Alphabet, das wir zur Kodierung von Symbolen (aus σ), Termen, Formeln, endlichen Mengen von Termen und Formeln sowie Beweisen (in $\mathfrak{S}$) verwenden.

Seien $Y, V, T, L, S, G, B \subseteq A^*$

die Mengen der kodierten

- Symbole aus σ (Y)
- Variablen (V)
- Terme (T)
- $FO[\sigma]$-Formeln (L)
- $FO[\sigma]$-Sätze (S)
- endlichen Formelmengen (G)
- Beweise (dh Ableitungen in $\mathfrak{S}$) (B).

Wir gehen im Folgenden davon aus, dass unsere Kodierung die folgenden Eigenschaften hat

<u>Annahme 9.1</u>:

Unsere Kodierung hat die folgenden Eigenschaften:

<u>(a)</u> Die Mengen $Y, V, T, L, S, G, B \subseteq A^*$ sind entscheidbar.

(b) Die logischen Operationen

- Negation
- Disjunktion
- Konjunktion
- existentielle Quantifizierung
- universelle Quantifizierung,

aufgefasst als 1- bzw 2-stellige partielle Funktionen auf $\mathbb{A}^*$, sind berechenbar.

(c) Die beiden Funktionen, die jeder $FO[\sigma]$-Formel die (endliche) Menge ihrer Variablen bzw die (endliche) Menge ihrer Subformeln zuordnen, sind berechenbar.

(d) Die Substitution einer Variablen durch einen Term in einer Formel, aufgefasst als 3-stellige partielle Funktion auf $\mathbb{A}^*$, ist berechenbar.

(e) Die 2-stellige Relation

$$\{ (f, g) \in \mathbb{A}^* \times \mathbb{A}^* :$$

$f \in L$ ist die Kodierung einer Formel $\varphi \in FO[\sigma]$ und

$g \in G$ ist die Kodierung einer endlichen

Menge Γ von $FO[\sigma]$-Formel mit $\varphi \in \Gamma$ $\}$

ist entscheidbar.

(f) Die 3-stellige Relation

$$\{ (b, g, f) \in (\mathbb{A}^*)^3 :$$

$g \in G$ ist die Kodierung einer endlichen Menge Γ von $FO[\sigma]$-Formeln,

$f \in L$ ist die Kodierung einer $FO[\sigma]$-Formel φ,

$b \in B$ ist die Kodierung einer Ableitung $\Gamma \vdash \varphi$ im Sequenzenkalkül $\}$

ist entscheidbar.

<u>Bemerkung</u>: In Abschnitt 9.2 werden wir eine Kodierung angeben, die die in Annahme 9.1 aufgelisteten Eigenschaften hat.

Vereinbarung:

Für den Rest dieses Kapitels unterscheiden wir nicht mehr zwischen syntaktischen Objekten (wie $FO(\sigma)$-Formeln) und ihren Kodierungen. Zum Beispiel sprechen wir direkt von entscheidbaren Formelmengen (und meinen dabei eigentlich entscheidbare Mengen von Kodierungen von Formeln).

Lemma 9.2 (Aufzählbarkeit der beweisbaren Sätze)

Sei σ eine abzählbare, entscheidbare Signatur.

Sei $\Phi \subseteq FO[\sigma]$ eine rekursiv aufzählbare Formelmenge.

Dann ist auch die Menge

$$\{ \varphi \in FO[\sigma] \;:\; \Phi \models \varphi \}$$

rekursiv aufzählbar.

Beweis: Gemäß Vollständigkeitssatz gilt:

$$\{ \varphi \in FO[\sigma] : \Phi \models \varphi \} = \{ \varphi \in FO[\sigma] : \Phi \vdash_{\mathfrak{S}} \varphi \}.$$

Daher zählt der folgende Algorithmus nach und nach sämtliche Elemente aus $\{ \varphi \in FO[\sigma] : \Phi \models \varphi \}$ auf:

1) Für $n = 1, 2, 3, \ldots$ tue folgendes:

2) zähle die ersten n Formeln $\varphi_1, \ldots, \varphi_n$ aus Φ auf (... mit dem Algor., den es laut Voraussetzung gibt)

3) zähle die ersten n Kodierungen von Beweisen in $\mathcal{S}$, etwa $b_1, \ldots, b_n$ auf (... mit dem Algor., den es laut Annahme 9.1 (a) gibt)

4) Prüfe für jedes b_i, ob es eine Sequenz $\Gamma \vdash \varphi$ mit $\Gamma \subseteq \{\varphi_1, \ldots, \varphi_n\}$ beweist.
Wenn ja, gib φ aus.

$\square$

Als unmittelbare Folgerung aus Lemma 9.2 erhalten wir:

> **Korollar 9.3:** Sei σ eine abzählbare, entscheidbare Signatur. Dann gilt:
> Die Menge aller allgemeingültigen $FO[\sigma]$-Formeln ist rekursiv aufzählbar.

Bemerkung: Dies ist die Formalisierung der auf Seite 201 angekündigten Aussage.

9.2 Gödelisierung von $FO[\sigma_{Ar}]$

Notation 9.4 (Arithmetik)

- Wir betrachten nun die Signatur

$$\sigma_{Ar} = \{ \leq, +, \times, 0, 1 \}.$$

- ~~Statt $T_{\sigma_{Ar}}$ und $FO[\sigma_{Ar}]$ schreiben wir kurz T_{Ar} und FO_{Ar}. Wir schreiben S_{Ar} um die Menge aller $FO[\sigma_{Ar}]$-Sätze zu bezeichnen.~~

- $\mathcal{N}$ bezeichnet wie üblich das Standardmodell $(\mathbb{N}, \leq^{\mathcal{N}}, +^{\mathcal{N}}, \times^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}})$ der Arithmetik

- Für Terme $t, u \in T_{\sigma_{Ar}}$ schreiben wir

$$t < u$$

als Abkürzung für die $FO[\sigma_{Ar}]$-Formel

$$(t \leq u \wedge \neg t = u)$$

Definition 9.5 (Die Zahlterme $\underline{n}$)

Die Zahlterme $\underline{n}$, für $n \in \mathbb{N}$, seien die folgendermaßen definierten σ_{Ar}-Terme:

$\underline{0} := 0$, und f.a. $n \in \mathbb{N}$ sei

$\underline{n+1} := (\underline{n} + 1)$; präzise: $\underline{n+1} := +(\underline{n}, 1)$ (vgl Def 1.14)

Bsp: $\underline{0} = 0$, $\underline{1} \mathrel{\hat{=}} (\underline{0}+1) \mathrel{\hat{=}} +(0,1)$, $\underline{2} \mathrel{\hat{=}} (\underline{1}+1) \mathrel{\hat{=}} +(\underline{1},1) = +(+(0,1),1)$,
$\underline{3} \mathrel{\hat{=}} (\underline{2}+1) \mathrel{\hat{=}} +(\underline{2},1) = +(+(+(0,1),1),1)$

Arithmetisierung:

- Wir kodieren syntaktische Objekte wie Symbole aus σ_{Ar}, Formeln aus $FO[\sigma_{Ar}]$ usw. durch natürliche Zahlen in Hexadezimaldarstellung, die wir als Wörter über dem Alphabet

  $$A_{HEX} := \{0, \dots, 9, a, \dots, f\}$$

  auffassen.

  Für eine Zahl $n \in \mathbb{N}$ schreiben wir $[n]_{HEX}$, um ihre Hexadezimaldarstellung zu bezeichnen.
  Für ein $w \in A_{HEX}^{+}$ schreiben wir $[w]_{\mathbb{N}}$, um die natürliche Zahl zu bezeichnen, die durch w in Hexadezimaldarstellung repräsentiert wird.
- Unser Ziel ist eine Kodierung, die alle Eigenschaften aus Annahme 9.1 besitzt.

- Weil für $w \in A_{Hex}^*$ die Wörter w und $0w$ dieselbe Zahl darstellen, vermeiden wir Kodewörter, die mit 0 beginnen.

- Die Kodierung eines Objekts o werden wir stets mit $\langle o \rangle$ bezeichnen.

Zur Erinnerung

σ_{Ar}-Terme und $FO[\sigma_{Ar}]$-Formeln sind Wörter über dem Alphabet

$$A_{\sigma_{Ar}} = Var \cup \{\neg, \wedge, \vee, \exists, \forall, (,), =\} \cup \{\leq, +, \times, 0, 1\} \cup \{,\}$$

Definition 9.6 (Kodierung von $A_{\sigma_{Ar}}$)

Wir kodieren die Elemente des Alphabets $A_{\sigma_{Ar}}$ durch Worte über dem Alphabet A_{Hex} wie folgt:

- Variablen: für jedes $n \in \mathbb{N}$ ist

$$\langle v_n \rangle := 1\underbrace{0 \cdots 0}_{n\text{-mal}} = [16^n]_{Hex}$$

- <u>Logische Symbole:</u>
  - $\langle \neg \rangle := 2 = [2]_{Hex}$
  - $\langle \wedge \rangle := 3 = [3]_{Hex}$
  - $\langle \vee \rangle := 4 = [4]_{Hex}$
  - $\langle \exists \rangle := 5 = [5]_{Hex}$
  - $\langle \forall \rangle := 6 = [6]_{Hex}$
  - $\langle (\rangle := 7 = [7]_{Hex}$
  - $\langle) \rangle := 8 = [8]_{Hex}$
  - $\langle = \rangle := 9 = [9]_{Hex}$
  - $\langle , \rangle := f = [15]_{Hex}$
- <u>Arithmetische Symbole:</u>
  - $\langle \leq \rangle := a = [10]_{Hex}$
  - $\langle + \rangle := b = [11]_{Hex}$
  - $\langle \times \rangle := c = [12]_{Hex}$
  - $\langle 0 \rangle := d = [13]_{Hex}$
  - $\langle 1 \rangle := e = [14]_{Hex}$

Definition 9.7 (Kodierung von Termen, Formeln und Beweisen)

(a) Für jedes Wort $w = w_1 \cdots w_\ell \in A^+_{\sigma_{Ar}}$ ist $\langle w \rangle := \langle w_1 \rangle \langle w_2 \rangle \cdots \langle w_\ell \rangle$.

Insbesondere gilt:

- Für jeden Term $t \in T_{\sigma_{Ar}}$, etwa $t = s_1 \cdots s_\ell \in A^*_{\sigma_{Ar}}$ ist
$$\langle t \rangle = \langle s_1 \rangle \langle s_2 \rangle \cdots \langle s_\ell \rangle$$

- Für jede Formel $\varphi \in \mathrm{FO}[\sigma_{Ar}]$, etwa $\varphi = s_1 \cdots s_\ell \in A^*_{\sigma_{Ar}}$ ist
$$\langle \varphi \rangle = \langle s_1 \rangle \langle s_2 \rangle \cdots \langle s_\ell \rangle$$

(b) Für eine endliche nicht-leere Formelmenge $\Phi \subseteq \mathrm{FO}[\sigma_{Ar}]$ sei
$$\langle \Phi \rangle := \langle \varphi_1 \rangle ff \langle \varphi_2 \rangle ff \cdots ff \langle \varphi_\ell \rangle,$$
falls $\Phi = \{\varphi_1, \dots, \varphi_\ell\}$ mit
$[\langle \varphi_1 \rangle]_{\mathbb{N}} \leq [\langle \varphi_2 \rangle]_{\mathbb{N}} \leq \cdots \leq [\langle \varphi_\ell \rangle]_{\mathbb{N}}$, wobei $<$ hier die natürliche lineare Ordnung auf $\mathbb{N}$ bezeichnet.

Beachte: $ff \in A^2_{Hex}$ wird hier als "Trennsymbol" verwendet.

Ferner sei $\langle \emptyset \rangle := 0 = [0]_{Hex}$

(d) Für eine Sequenz $\Gamma \vdash \varphi$ sei

$$\langle \Gamma \vdash \varphi \rangle := fff \langle \Gamma \rangle fff \langle \varphi \rangle fff .$$

(e) Für eine Folge $(S_1, \dots, S_e)$ von Sequenzen (also insbes. auch für eine Ableitung im Sequenzenkalkül) sei

$$\langle (S_1, \dots, S_e) \rangle := \langle S_1 \rangle \cdots \langle S_e \rangle .$$

Lemma 9.8

Die in Definition 9.6 und 9.7 eingeführte Kodierung besitzt alle Eigenschaften aus Annahme 9.1.

Ferner gilt für alle syntaktischen Objekte o (d.h. für Terme, Formeln, Formelmengen, Sequenzen, Beweise), dass entweder $\langle o \rangle = 0$ ist oder $\langle o \rangle$ mit einem Zeichen in $\{1, \dots, 9, a, \dots, f\}$ beginnt.

Daher lässt sich jedes Kodewort $\langle o \rangle$ als Hexadezimaldarstellung der natürlichen Zahl $[\langle o \rangle]_{\mathbb{N}}$ auffassen.

Beweis: Übung.

Bemerkung 3.9 (Gödelisierung)

Die Kodierung von Formeln durch natürliche Zahlen bezeichnet man auch als Gödelisierung.

Für eine Formel $\varphi \in FO[\sigma_{Ar}]$ bezeichnet man die Zahl $n_\varphi := [\langle\varphi\rangle]_{\mathbb{N}} \in \mathbb{N}$ als die Gödelnummer von φ.

Analog bezeichnen wir für eine Term $t \in T_{\sigma_{Ar}}$ die Zahl $n_t := [\langle t \rangle]_{\mathbb{N}} \in \mathbb{N}$ als die Gödelnummer von t.

Lemma 9.10

Die Funktion $f: \mathbb{N} \to \mathbb{N}$ mit $f(n) := [\langle \underline{n} \rangle]_{\mathbb{N}}$

(f.a. $n \in \mathbb{N}$) ist berechenbar.

D.h.: Es gibt einen Algorithmus, der bei Eingabe einer Zahl $n \in \mathbb{N}$ die Gödelnummer des Terms $\underline{n}$ ausgibt.

Beweis: Gemäß Def. 9.7 gilt:

$\underline{0} = 0 \in \sigma_{Ar}$, und f.a. $n \in \mathbb{N}$ gilt:

$\underline{n+1} = (\underline{n} + 1)$ — bzw. präzise: $\underline{n+1} = +(\underline{n}, 1)$.

Man sieht leicht, dass f.a. $n \in \mathbb{N}$ mit $n \geq 1$ gilt:

$$\underline{n} = \underbrace{+(+(\cdots +(}_{n \text{ mal } "+("} 0 \underbrace{,1),1),\cdots,1)}_{n \text{ mal } ",1)"}$$

Gemäß Def. 9.8 gilt: $\langle + \rangle = b$, $\langle (\rangle = 7$, $\langle 0 \rangle = d$,
$\langle , \rangle = f$, $\langle 1 \rangle = e$, $\langle) \rangle = 8$.

Somit ist für $n \geq 1$:

$$\langle \underline{n} \rangle = \underbrace{b7\, b7 \cdots b7}_{n \text{ mal } "b7"}\, d\, \underbrace{fe8\, fe8 \cdots fe8}_{n \text{ mal } "fe8"}.$$

Dies ist die Hexadezimaldarstellung der Zahl $[\langle \underline{n} \rangle]_{\mathbb{N}} \in \mathbb{N}$.

Man kann leicht einen Algorithmus angeben, der bei Eingabe einer Zahl $n \in \mathbb{N}$ zunächst den Term $\underline{n}$, dann das Kodewort $\langle \underline{n} \rangle$ und daraus die Zahl $[\langle \underline{n} \rangle]_{\mathbb{N}}$ berechnet. $\square$

Übungsaufgabe: Berechnen Sie die Gödelnummern der Terme $\underline{0}$, $\underline{1}$ und $\underline{2}$.

Lemma 9.11 (Definierbare Zahlenmengen)

Sei Φ eine entscheidbare Menge von $FO[\sigma_{Ar}]$-Sätzen, und sei $\varphi(x)$ eine $FO[\sigma_{Ar}]$-Formel. Dann gilt:

(a) Die Menge $\{ n \in \mathbb{N} : \Phi \models \varphi(\underline{n}) \}$ ist rekursiv aufzählbar.

(b) Die Menge $\{ n \in \mathbb{N} : \Phi \models \neg\varphi(\underline{n}) \}$ ist rekursiv aufzählbar.

(c) Wenn für alle $n \in \mathbb{N}$ gilt: $\Phi \models \varphi(\underline{n})$ oder $\Phi \models \neg\varphi(\underline{n})$, so ist die Menge $\{ n \in \mathbb{N} : \Phi \models \varphi(\underline{n}) \}$ entscheidbar.

Beweis:

(a) Wegen Lemma 9.8 erfüllt unsere Kodierung die Annahme 9.1.

Wegen Lemma 9.10 und Annahme 9.1 (c) ist daher die Funktion

$$n \mapsto \langle \varphi(\underline{n}) \rangle \quad (\text{f.a. } n \in \mathbb{N}) \quad (*)$$

berechenbar,
d.h. es gibt einen Algorithmus, der bei Eingabe einer Zahl n die Kodierung der Formel $\varphi\frac{\underline{n}}{x}$ $(= \varphi(\underline{n}))$ ausgibt.

Daher ist die Menge $\{ \langle \varphi(\underline{n}) \rangle : n \in \mathbb{N} \}$ rekursiv aufzählbar.

Laut Voraussetzung ist Φ entscheidbar.
Aus Lemma 9.2 folgt, dass $\{ \varphi \in FO[\sigma_{Ar}] : \Phi \models \varphi \}$ rekursiv aufzählbar ist. Daher ist auch die Menge $\{ \langle \psi \rangle : \psi \text{ ist ein } FO[\sigma_{Ar}]\text{-Satz mit } \Phi \models \psi \}$ rekursiv aufzählbar.

Somit sind die beiden Mengen
$\{ \langle \varphi(\underline{n}) \rangle : n \in \mathbb{N} \}$ und $\{ \langle \psi \rangle : \psi \text{ ist } FO[\sigma_{Ar}]\text{-Satz}, \Phi \models \psi \}$
rekursiv aufzählbar.

Da der Durchschnitt zweier rekursiv aufzählbarer Mengen rekursiv aufzählbar ist, ist auch die Menge

$$\{ \langle \varphi(\underline{n}) \rangle : n \in \mathbb{N}, \ \Phi \models \varphi(\underline{n}) \}$$

rekursiv aufzählbar.

Wegen (*) ist daher auch die Menge

$$\{ n \in \mathbb{N} : \Phi \models \varphi(\underline{n}) \}$$

rekursiv aufzählbar.

(b) folgt aus (a) mit $\neg\varphi$ an Stelle von φ

(c) folgt direkt aus (a), (b) und der Voraussetzung in (c)

(Details: Übung).

∎

9.3 FO-Definierbarkeit der berechenbaren Funktionen

9.3.1 Δ_0-Formeln und das Lemma über die β-Funktion

Definition 9.12 (Arithmetische Relationen)

Sei $\Phi \subseteq FO[\sigma_{Ar}]$ eine Menge von $FO[\sigma_{Ar}]$-Formeln und sei $k \in \mathbb{N}$.

(a) Eine Relation $R \subseteq \mathbb{N}^k$ heißt Φ-definierbar, wenn es eine Formel $\varphi_R(x_1,\dots,x_k) \in \Phi$ mit $R = \varphi_R(\mathcal{N})$ gibt.

Zur Erinnerung (vgl. Def 3.3):

$$\varphi_R(\mathcal{N}) = \{ (n_1,\dots,n_k) \in \mathbb{N}^k : \mathcal{N} \models \varphi_R[n_1,\dots,n_k] \}$$

(b) Eine partielle Funktion f von $\mathbb{N}^k$ nach $\mathbb{N}$ heißt Φ-definierbar, wenn ihr Graph

$$\{ (n_1,\dots,n_k,m) \in \mathbb{N}^{k+1} : f(n_1,\dots,n_k) = m \}$$

eine Φ-definierbare Relation ist.

Notation 9.13 (beschränkte Quantoren)

Für $x \in Var$, $t \in T_{\sigma_{Ar}}$ und $\varphi \in FO[\sigma_{Ar}]$ schreiben wir

- $\exists x \leq t \ \varphi$ an Stelle von $\exists x (x \leq t \land \varphi)$
- $\forall x \leq t \ \varphi$ an Stelle von $\forall x (x \leq t \to \varphi)$.

Wir bezeichnen $\underline{\exists x \leq t}$ und $\underline{\forall x \leq t}$ als <u>beschränkte Quantoren</u>.

Wir schreiben auch

- $\exists x < t \ \varphi$ als Abkürzung für $\exists x \leq t (\neg x = t \land \varphi)$
- $\forall x < t \ \varphi$ als Abkürzung für $\forall x \leq t (\neg x = t \to \varphi)$

Definition 9.14 (Δ_0: Klasse aller beschränkten $FO[\sigma_{Ar}]$-Formeln)

Die Klasse Δ_0 aller <u>beschränkten</u> $FO[\sigma_{Ar}]$-Formeln ist rekursiv wie folgt definiert:

- Für jede <u>atomare</u> $FO[\sigma_{Ar}]$-Formel φ gilt: $\varphi \in \Delta_0$
- Sind $\varphi \in \Delta_0$ und $\psi \in \Delta_0$, so gilt auch: $\neg\varphi \in \Delta_0$, $(\varphi \land \psi) \in \Delta_0$, $(\varphi \lor \psi) \in \Delta_0$
- Sind $\varphi \in \Delta_0$, $x \in Var$ und $t \in T_{\sigma_{Ar}}$, so gilt: $\exists x \leq t \ \varphi \in \Delta_0$ und $\forall x \leq t \ \varphi \in \Delta_0$.

Das folgende Lemma liefert einen wichtigen Schlüssel zur Kodierung von Berechnungen durch Formeln der Logik erster Stufe. Das Lemma besagt, dass man Folgen natürlicher Zahlen durch einzelne Zahlen kodieren kann — und zwar so, dass diese Kodierung durch eine beschränkte $\mathrm{FO}[\sigma_{Ar}]$-Formel definiert werden kann.

<u>Lemma 9.15</u> (Das Lemma über die β-Funktion)

Es gibt eine Δ_0-definierbare Funktion

$$\beta : \mathbb{N}^2 \to \mathbb{N}$$

mit der folgenden Eigenschaft:

Für jedes $\ell \in \mathbb{N}_{\geq 1}$ und jede Folge $(n_0, \dots, n_{\ell-1}) \in \mathbb{N}^\ell$ gibt es ein $s \in \mathbb{N}$ mit $s \geq \max\{\ell, n_0, \dots, n_{\ell-1}\}$, so dass f.a. $i \in \{0, \dots, \ell-1\}$ gilt:

$$\beta(s, i) = n_i$$

(d.h.: s repräsentiert die Folge $(n_0, \dots, n_{\ell-1})$, und $\beta(s,i)$ liefert die Komponente n_i)

<u>Notation:</u> Im Folgenden bezeichnet β immer die Funktion aus Lemma 9.17; und für $s, \ell \in \mathbb{N}$ ist $B(s,\ell) := (\beta(s,0), \dots, \beta(s,\ell-1))$.

Beweis: Sei $\ell \in \mathbb{N}$ mit $\ell \geq 1$ und

Sei $(n_0, \dots, n_{\ell-1}) \in \mathbb{N}^\ell$.

Sei p die kleinste Primzahl mit

$$p > \max\{\ell, n_0, \dots, n_{\ell-1}\}.$$

Sei

$$\begin{aligned} t := \; & 1 \cdot p^0 + n_0 \cdot p^1 \\ + \; & 2 \cdot p^2 + n_1 \cdot p^3 \\ + \; & 3 \cdot p^4 + n_2 \cdot p^5 \\ + \; & \dots \\ + \; & (i+1) \cdot p^{2i} + n_i \cdot p^{2i+1} \\ + \; & \dots \\ + \; & \ell \cdot p^{2(\ell-1)} + n_{\ell-1} \cdot p^{2(\ell-1)+1} \end{aligned}$$

D.h. t ist die natürliche Zahl, deren p-adische Darstellung folgendermaßen aussieht:

$$\begin{array}{cccccccccccccc} n_{\ell-1} & \ell & n_{\ell-2} & (\ell-1) & \cdots & n_i & (i+1) & \cdots & n_2 & 3 & n_1 & 2 & n_0 & 1 \\ \uparrow & \uparrow & \uparrow & \uparrow & & \uparrow & \uparrow & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ p^{2\ell-1} & p^{2\ell-2} & p^{2\ell-3} & p^{2(\ell-2)} & & p^{2i+1} & p^{2i} & & p^5 & p^4 & p^3 & p^2 & p^1 & p^0 \end{array}$$

Behauptung 1: Für alle $i \in \{0, \dots, \ell-1\}$ und alle $n \in \mathbb{N}$ gilt:

$n = n_i \iff$ Es gibt nat. Zahlen $m_0, m_1, m_2 \leq t$ so dass
- (1) $t = m_0 + m_1 \cdot ((i+1) + n \cdot p + m_2 \cdot p^2)$,
- (2) $n < p$,
- (3) $m_0 < m_1$ und
- (4) es gibt ein $j \leq m_1$ so dass $m_1 = p^{2j}$.

Beweis von Beh. 1:

"$\Rightarrow$": Wähle

$$m_0 := 1\cdot p^0 + n_0\cdot p^1 + \dots + i\cdot p^{2(i-1)} + n_{i-1}\cdot p^{2i-1} \qquad (< p^{2i})$$

$$m_1 := p^{2i}$$

$$m_2 := (i+2)\cdot p^{2(i+1)-2i-2} + n_{i+1}\cdot p^{2i+3-2i-2} + \dots + \ell\cdot p^{2(\ell-1)-2i-2} + n_{\ell-1}\cdot p^{2\ell-1-2i-2}$$

Klar: Damit sind (1), (3), (4) erfüllt.
(2) gilt, da $n_i < p$.

"$\Leftarrow$": Wähle m_0, m_1, m_2 so, dass (1) – (4) erfüllt sind;
ferner sei j s.d. $m_1 = p^{2j}$. Dann gilt gemäß (1):

$$t = m_0 + (i+1)\cdot p^{2j} + n\cdot p^{2j+1} + m_2\cdot p^{2j+2}.$$

Gemäß (3) gilt: $m_0 < p^{2j}$

Gemäß Wahl von p gilt: $(i+1) < p$

Wegen (2) gilt: $n < p$

Wegen der Eindeutigkeit der p-adischen Darstellung folgt aus der Definition von t daher, dass

- $2j = 2i$, d.h. $j = i$ und
- $n = n_i$

$\square$ Beh 1

Im Folgenden nutzen wir Beh 1, um eine Δ_0-Formel $\varphi(u, v, w, y)$ zu definieren, so dass f.a. $i \in \{0, \dots, \ell-1\}$ und alle $n \in \mathbb{N}$ gilt:

$$n = n_i \iff \mathcal{N} \models \varphi[p, t, i, n]$$

In der folgenden Formel $\varphi(u,v,w,y)$ spielt die Variable

- u die Rolle der Primzahl p
- v die Rolle der Zahl t
- w die Rolle der Zahl i
- y die Rolle der Zahl n
- v_0, v_1, v_2 die Rolle der Zahlen m_0, m_1, m_2 in den Bedingungen (1)-(4) aus Beh. 1.

Sei $\varphi(u,v,w,y)$ nun die folgende Δ_0-Formel:

$$\varphi(u,v,w,y) :=$$

$$\exists v_0 \leq v \;\; \exists v_1 \leq v \;\; \exists v_2 \leq v \;\; \Big($$

$$v = v_0 + v_1 \times \big((w+1) + y \times u + v_2 \times u \times u \big) \;\; \wedge \qquad (\underline{1})$$

$$y < u \;\; \wedge \qquad (\underline{2})$$

$$v_0 < v_1 \;\; \wedge \qquad (\underline{3})$$

$$\underbrace{\exists z \leq v_1 \;\; z \times z = v_1}_{v_1 \text{ ist Quadratzahl}} \;\; \wedge \;\; \underbrace{\forall z \leq v_1 \Big(\overbrace{\exists z' \leq v_1 \;\; z \times z' = v_1}^{z \text{ ist Teiler von } v_1} \rightarrow \underbrace{\exists z' \leq z \;\; u \times z' = z}_{u \text{ ist Teiler von } z} \Big)}_{v_1 \text{ ist Potenz von } u} \qquad (\underline{4})$$

Behauptung 2: $\varphi(u,v,w,y)$ ist eine Δ_0-Formel, so dass für alle $i \in \{0, \dots, \ell-1\}$ und alle $n \in \mathbb{N}$ gilt: $n = n_i \iff \mathcal{N} \models \varphi[p,t,i,n]$

Beweis: Folgt direkt aus Beh 1 und der Definition von φ.

$\square$ Beh 2

Sei nun $\psi(u,v,w,y)$ die folgende Δ_0-Formel:

$$\psi(u,v,w,y) :=$$

$$\Big(\big(\varphi(u,v,w,y) \wedge y \leq v \wedge \neg\exists z < y\ \varphi(u,v,w,z) \big) \vee$$

$$\big(y = 0 \wedge \neg\exists z \leq v\ \varphi(u,v,w,z) \big) \Big)$$

<u>Behauptung 3:</u> $\psi(u,v,w,y)$ definiert eine totale Funktion $\beta': \mathbb{N}^3 \to \mathbb{N}$ (im Sinne von Def. 9.14 (b))

<u>Beweis:</u> Für alle natürlichen Zahlen $p,t,i \in \mathbb{N}$ gibt es genau ein $n \in \mathbb{N}$, so dass $\mathcal{N} \models \psi[p,t,i,n]$, nämlich:

- n ist die kleinste nat Zahl $\leq t$ mit $\mathcal{N} \models \varphi[p,t,i,n]$, falls es eine solche Zahl gibt
- n ist 0, falls es keine nat Zahl $n' \leq t$ mit $\mathcal{N} \models \varphi[p,t,i,n']$ gibt.

□ Beh 3.

<u>Behauptung 4:</u> Für alle $\ell \in \mathbb{N}_{\geq 1}$ und alle $(n_0,\dots,n_{\ell-1}) \in \mathbb{N}^\ell$ gibt es Zahlen $p,t \in \mathbb{N}$, so dass gilt

- $t \geq \max\{\ell, n_0,\dots,n_{\ell-1}\}$, und
- f.a. $i \in \{0,\dots,\ell-1\}$ ist $\beta'(p,t,i) = n_i$

<u>Beweis:</u> Folgt unmittelbar aus der Konstruktion der Formel ψ.

□ Beh 4.

Behauptung 5: Die Funktion $g : \mathbb{N}^2 \to \mathbb{N}$ mit

$$g(y_1, y_2) := \frac{1}{2}(y_1 + y_2 + 1) \cdot (y_1 + y_2) + y_2 \quad (\text{f.a. } y_1, y_2 \in \mathbb{N})$$

ist bijektiv.

Beweis: Übung.

Die folgende Δ_0-Formel $\gamma(y_1, y_2, z)$ definiert die Funktion g aus Beh 5:

$$\gamma(y_1, y_2, z) := (1+1) \times z = (y_1 + y_2 + 1) \times (y_1 + y_2) + (1+1) \times y_2.$$

Sei nun $\varphi_\beta(z, w, y)$ die folgendermaßen definierte Δ_0-Formel:

$$\varphi_\beta(z, w, y) = \exists u \le z \; \exists v \le z \; \big(\gamma(u, v, z) \wedge \psi(u, v, w, y)\big)$$

Behauptung 6: Die Δ_0-Formel $\varphi_\beta(z, w, y)$ definiert eine Funktion $\beta : \mathbb{N}^2 \to \mathbb{N}$, die die Bedingungen von Lemma 9.17 erfüllt.

Beweis: Die Formel $\varphi_\beta(z, w, y)$ definiert die Funktion $\beta : \mathbb{N}^2 \to \mathbb{N}$ mit $\beta(g(p,t), i) = \beta'(p, t, i)$, f.a. $p, t, i \in \mathbb{N}$ (da g bijektiv ist, ist β wohldefiniert). Beh 6 folgt unmittelbar aus Beh. 4 u. d. der Tatsache, dass $g(p,t) \ge t$ ist ($\nearrow$ Beh 5).

$\square_{\text{Beh 6}}$ $\quad\square$ Lemma 9.17

9.3.2 Ein formales Berechnungsmodell:

Im Folgenden wollen wir zeigen, dass alle berechenbaren Funktionen und rekursiv aufzählbaren Relationen durch $FO[\sigma_{Ar}]$-Formeln definiert werden können (im Sinne von Def. 9.12)

(– daraus werden wir dann z.B. folgern, dass $Th(\mathcal{N})$ nicht rekursiv aufzählbar ist).

Dazu müssen wir allerdings einen präzisen Berechnungs-Begriff verwenden. Gemäß der Church-Turing-These könnten wir dazu jedes "sinnvolle" Berechnungsmodell wählen (z.B. Turingmaschinen, Registermaschinen, WHILE-Programme ...).

Für unsere Zwecke besonders bequem ist, das folgende formale Berechnungsmodell zu verwenden:

Wir betrachten deterministische 1-Band-Turingmaschinen

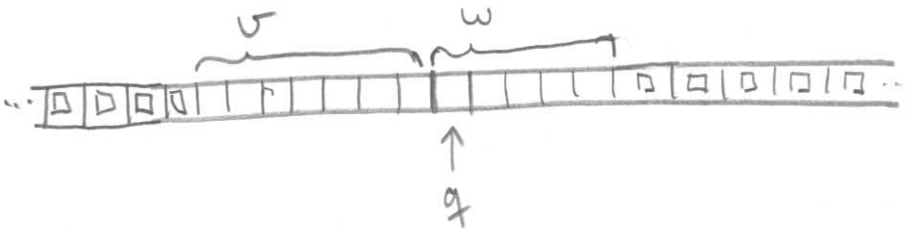
$\boxed{\delta : Q \setminus F \times A_{TM} \to Q \times A_{TM} \times \{\leftarrow, \downarrow, \rightarrow\}}$

$$M = (\underset{\text{Menge der Zustände}}{Q},\ \underset{\text{Bandalphabet}}{A_{TM}},\ \underset{\text{Überführungsfunktion}}{\delta},\ \underset{\text{Startzustand}}{q_0},\ \underset{\text{Endzustände}}{F})$$

über dem festen Alphabet $A_{TM} := \{ |, \#, \square \}$, wobei $|$ zur unären Darstellung natürlicher Zahlen dient, $\#$ als Trennsymbol und $\square$ als Leerzeichen (Blank) verwendet wird. OBdA gelte stets: $Q \cap A_{TM} = \emptyset$.

<u>Konfigurationen</u> von M beschreiben wir als Wörter $\mathcal{K} = vqw \in (A_{TM} \cup Q)^*$, wobei $v, w \in A_{TM}^*$ und $q \in Q$ ist.

$\mathcal{K} = vqw$ beschreibt folgende Konfiguration von M:



D.h.: q ist der aktuelle Zustand,
vw ist der nicht-leere Teil der Bandbeschriftung und
der Schreib-/Lesekopf steht auf dem ersten Symbol von w (bzw., falls $w = \varepsilon$ das leere Wort ist, so steht der Schreib-/Lesekopf auf dem ersten Blank-Symbol $\square$ rechts von der aktuellen Beschriftung v des Bandes).

Wir schreiben $\mathcal{K} \to_M \mathcal{K}'$, um auszudrücken, dass $\mathcal{K}'$ die <u>Nachfolgekonfiguration</u> von $\mathcal{K}$ ist.

Eine <u>Berechnung von M</u> ist eine endliche Folge von aufeinanderfolgenden Konfigurationen.
Wir schreiben $\mathcal{K} \to_M^* \mathcal{K}'$, um auszudrücken, dass es eine Berechnung gibt, die $\mathcal{K}$ in $\mathcal{K}'$ überführt.

<u>Notation</u>: Für $n \in \mathbb{N}$ sei

$$|^n := \underbrace{||\cdots|}_{n\text{-mal}} \in A_{TM}^*$$

die <u>Unärdarstellung</u> von n.

<u>Definition 9.16</u>

<u>(a)</u> Eine partielle Funktion f von $\mathbb{N}^k$ nach $\mathbb{N}$ heißt <u>TM-berechenbar</u>, wenn es eine deterministische 1-Band-Turingmaschine $M = (Q, A_{TM}, \delta, q_0, F)$ gibt, so dass für alle $m_1, \dots, m_k, n \in \mathbb{N}$ gilt:

$f(m_1, \dots, m_k) = n \iff$ es gibt ein $q \in F$ so dass

(insbes.: $(m_1, \dots, m_k) \in Def(f)$) $\qquad q_0\, |^{m_1} \# |^{m_2} \# \cdots \# |^{m_k} \xrightarrow[M]{*} |^n q$.

<u>Beachte</u>: Für $(m_1, \dots, m_k) \in \mathbb{N}^k \setminus Def(f)$ gilt: es gibt kein $n \in \mathbb{N}$, $q \in F$ s.d. $q_0 |^{m_1} \# |^{m_2} \# \dots |^{m_k} \xrightarrow[M]{*} |^n q$.

<u>(b)</u> Eine Relation $R \subseteq \mathbb{N}^k$ heißt <u>TM-rekursiv aufzählbar</u>, wenn die partielle Funktion f_R von $\mathbb{N}^k$ nach $\mathbb{N}$ mit $Def(f_R) = R$ und $f_R(m_1, \dots, m_k) = 1$, f.a. $(m_1, \dots, m_k) \in R$ TM-berechenbar ist.

Die Church-Turing-These besagt, dass die TM-berechenbaren partiellen Funktion (und die TM-rekursiv aufzählbaren Relation) genau die berechenbaren partiellen Funktionen (bzw die rekursiv aufzählbaren Relationen) sind.

9.3.3 FO-Definierbarkeit von TM-Berechnungen und die Unentscheidbarkeit der Arithmetik

Im Folgenden werden wir zeigen, dass jede (TM-) berechenbare partielle Funktion durch eine FO[σ_{Ar}]-Formel definiert werden kann.

Vereinbarung 9.17

Wir identifizieren das Symbol $\square$ mit der Zahl 0, das Symbol | mit der Zahl 1 und das Symbol # mit der Zahl 2.

Außerdem nehmen wir immer an, dass die Zustandsmengen Q unserer Turingmaschinen endliche Teilmengen von $\mathbb{N} \setminus \{0,1,2\}$ sind.

Dadurch können jede Konfiguration $K = vqw \in (A_{TM} \cup Q)^*$ als eine endliche Folge natürlicher Zahlen auffassen, die wir mit der β-Funktion durch eine nat. Zahl kodieren können.

<u>Lemma 9.18</u>: ("Kodierungen von Konfigurationen sind Δ_0-definierbar")

Sei $M = (Q, A_{TM}, \delta, q_0, F)$ eine deterministische 1-Band-Turingmaschine.

Dann gibt es eine Δ_0-Formel $\varphi^M_{Konf}(x,y)$, so dass für alle $s, \ell \in \mathbb{N}$ gilt:

$$\mathcal{N} \models \varphi^M_{Konf}[s,\ell] \iff B(s,\ell) \text{ repräsentiert eine Konfiguration von } M$$

(zur Erinnerung: $B(s,\ell) := (\beta(s,0), \dots, \beta(s,\ell-1))$)

<u>Beweis</u>: Sei φ_β die Δ_0-Formel, die gemäß Lemma 9.17 die Funktion $\beta: \mathbb{N}^2 \to \mathbb{N}$ definiert.

Wir wählen

$$\varphi^M_{Konf}(x,y) := \exists z < y \ \exists w \leq x \ \Big($$

<u>Zeile 2</u>: $$\varphi_\beta(x,z,w) \wedge \bigvee_{q \in Q} w = q \quad \wedge$$

<u>Zeile 3</u>: $$\forall z' < y \ \Big(z' \neq z \rightarrow \big(\varphi_\beta(x,z',\underline{0}) \vee \varphi_\beta(x,z',\underline{1}) \vee \varphi_\beta(x,z',\underline{2}) \big)\Big)\Big)$$

In Zeile 2 wird gesagt, dass es in der von x kodierten Folge der Länge y eine Position z gibt, an der ein Zustand (w) steht. In Zeile 3 wird gesagt, dass an allen anderen Positionen in der Folge eins der Symbole 0, 1 oder 2 steht.

Lemma 9.19 (Δ_0-Definierbarkeit von TM-Berechnungen)

Sei $M = (Q, A_{TM}, \delta, q_0, F)$ eine Turingmaschine

(c) Es gibt eine Δ_0-Formel $\varphi^M_{Schritt}(x, y, x', y')$ s.d. f.a. $s, \ell, s', \ell' \in \mathbb{N}$ gilt:

$$\mathcal{N} \models \varphi^M_{Schritt}[s, \ell, s', \ell'] \iff$$

$B(s,\ell)$ und $B(s',\ell')$ kodieren Konfigurationen $\mathcal{K}$ und $\mathcal{K}'$ von M s.d. $\mathcal{K} \xrightarrow[M]{} \mathcal{K}'$ (d.h. $\mathcal{K}'$ ist Nachfolgekonfiguration von $\mathcal{K}$)

(a) Für jedes $k \in \mathbb{N}_{\geq 1}$ gibt es eine Δ_0-Formel $\varphi^M_{Start,k}(x, y, z_1, \dots, z_k)$ s.d. f.a. $s, \ell, m_1, \dots, m_k \in \mathbb{N}$ gilt:

$$\mathcal{N} \models \varphi^M_{Start,k}[s, \ell, m_1, \dots, m_k] \iff$$

$B(s,\ell)$ kodiert die Konfiguration $q_0 |^{m_1} \# \cdots \# |^{m_k}$ (also die Startkonfiguration von M bei Eingabe $(m_1, \dots, m_k) \in \mathbb{N}^k$)

(b) Es gibt eine Δ_0-Formel $\varphi^M_{Stopp}(x, y, z)$ s.d. f.a. $s, \ell, n \in \mathbb{N}$ gilt:

$$\mathcal{N} \models \varphi^M_{Stopp}[s, \ell, n] \iff$$

es gibt ein $q \in F$ s.d. $B(s,\ell)$ die Konfiguration $|^n q$ kodiert.

Beweis

(c) $\varphi^M_{\text{Schritt}}(x, y, x', y')$ besagt:

- $B(x,y)$ und $B(x',y')$ repräsentieren Konfigurationen (nutze dazu Lemma 9.18)
- An allen Stellen außer der Kopfposition und unmittelbar daneben sind die beiden Konfigurationen identisch
- An der Kopfposition und direkt daneben unterscheiden sich die beiden Konfigurationen gemäß der Übergangsfunktion δ

Details: Übung

(a) $\varphi^M_{\text{Start}}(x, y, z_1, \dots, z_k)$ besagt:

- $B(x,y)$ repräsentiert eine Konfiguration,
- deren erste Position ist q_0,
- danach folgen z_1 viele Striche, dann kommt ein #,
- danach folgen z_2 viele Striche, dann kommt ein #,
- usw

Details: Übung.

(b) Analog zu (a)

$\square$ Lemma 9.19

Definition 9.20 (Die Klasse $\Sigma_1 \subseteq FO[\sigma_{Ar}]$)

Die Menge Σ_1 besteht aus allen $FO[\sigma_{Ar}]$-Formeln der Form $\exists x\, \varphi$, wobei $x \in Var$ und $\varphi \in \Delta_0$.

Satz 9.21 (Σ_1-Definierbarkeit der berechenbaren partiellen Funktionen und der rek. aufzählbaren Relationen)

(a) Jede TM-berechenbare partielle Funktion f von $\mathbb{N}^k$ nach $\mathbb{N}$ (für $k \in \mathbb{N}_{\geq 1}$ beliebig) ist Σ_1-definierbar.

(b) Jede TM-rekursiv aufzählbare Relation $R \subseteq \mathbb{N}^k$ (f.a. $k \in \mathbb{N}$) ist Σ_1-definierbar.

Beweis: Klar: (b) folgt leicht aus (a). Beweis zu (a):

Sei M eine Turingmaschine, die f berechnet (im Sinne von Definition 9.16).

Im Folgenden konstruieren wir eine Σ_1-Formel $\varphi_f(x_1, \ldots, x_k, y)$ s.d. f.a. $m_1, \ldots, m_k \in \mathbb{N}^k$ und f.a. $n \in \mathbb{N}$ gilt:

$$\mathcal{N} \models \varphi_f[m_1, \ldots, m_k, n] \iff f(m_1, \ldots, m_k) = n$$

(insbes. $(m_1, \ldots, m_k) \in Def(f)$)

$$\overset{\text{Def. 9.16}}{\iff} \text{es gibt ein } q \in F \text{ s.d. } q_0 1^{m_1} \# \cdots \# 1^{m_k} \xrightarrow[M]{*} 1^n q.$$

In der folgenden Formel φ_f repräsentiert die Variable u die Kodierung einer Berechnung von M,

wobei an jeder <u>geraden</u> Stelle des durch u kodierten Tupels natürlicher Zahlen die Kodierung einer Konfiguration steht, und an der darauffolgenden (nächstgrößeren) <u>ungeraden</u> Stelle die Länge dieser Konfiguration steht.

D.h: Eine Folge $\mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_r$ von Konfigurationen der Längen $\ell_1, \ell_2, \dots, \ell_r$ wird kodiert durch ein Tupel

$(s_1, \ell_1, s_2, \ell_2, \dots, s_r, \ell_r)$ nat. Zahlen,

s.d. f. a. $i \in \{1, \dots, r\}$ gilt: $B(s_i, \ell_i)$ kodiert die Konfiguration $\mathcal{K}_i$.

Die Variable u repräsentiert diejenige nat. Zahl s, für die gilt:

$$B(s, 2r) = (s_1, \ell_1, \dots, s_r, \ell_r)$$

Position: $s_1 \to 0$, $\ell_1 \to 1$, ……, $s_r \to 2r-2 = 2(r-1)$, $\ell_r \to 2r-1 = 2(r-1)+1$

Die Zahl $r-1$ wird durch die Variable z repräsentiert.

Die Variablen v und v' repräsentieren zwei Konfigurationen, die Variablen w und w' repräsentieren die Längen dieser beiden Konfigurationen.

$$\varphi_f(x_1,\dots,x_k,y) \quad := \quad \exists u \; \exists z \leq u \; \Big($$

Zeile 1 $\quad \exists v \leq u \; \exists w \leq u \; \big(\varphi_\beta(u,\underline{0},v) \wedge \varphi_\beta(u,\underline{1},w) \wedge \varphi^M_{\mathrm{Start},k}(v,w,x_1,\dots,x_k) \big)\big)$

Zeile 2 $\quad \wedge \; \exists v \leq u \; \exists w \leq u \; \big(\varphi_\beta(u,\underline{2}\times z,v) \wedge \varphi_\beta(u,\underline{2}\times z+1,w) \wedge \varphi^M_{\mathrm{Stopp}}(v,w,y) \big)$

Zeile 3 $\quad \wedge \; \forall v \leq u \; \forall w \leq u \; \forall v' \leq u \; \forall w' \leq u \; \forall z' \leq z \; \big(\underline{2}\times z' + \underline{3} \leq \underline{2}\times z + \underline{1} \rightarrow$

Zeile 4 $\quad \Big(\big(\varphi_\beta(u,\underline{2}\times z',v) \wedge \varphi_\beta(u,\underline{2}\times z'+1,w) \wedge \varphi_\beta(u,\underline{2}\times z'+\underline{2},v') \wedge \varphi_\beta(u,\underline{2}\times z'+\underline{3},w') \big)\Big)$

Zeile 5 $\quad \rightarrow \; \varphi^M_{\mathrm{Schritt}}(v,w,v',w') \big)\big)\big)\big)$

- Zeile 1 besagt, dass die ersten beiden Einträge in der durch u kodierten Folge die Startkonfiguration von M bei Eingabe von $(x_1,\dots,x_k) \in \mathbb{N}^k$ repräsentiert.
- Zeile 2 besagt, dass die letzten beiden Einträge in der durch u kodierten Folge (der Länge $2\times z+2$) eine Stopp-Konfiguration von M mit Ausgabe y repräsentiert
- Zeile 3 besagt, dass jedes Paar von aufeinanderfolgenden Konfigurationen in der durch u kodierten Folge einen Berechnungsschritt von M repräsentiert

Somit ist φ_f eine Δ_0-Formel, die die partielle Funktion f definiert. $\square$ Satz 9.21

Bemerkung 9.22

Die Umkehrung von Satz 9.21 gilt ebenfalls

~~(hier ohne Beweis)~~

D.h: Eine partielle Funktion f von $\mathbb{N}^k$ nach $\mathbb{N}$ (bzw eine Relation $R \subseteq \mathbb{N}^k$) ist genau dann berechenbar (bzw rekursiv aufzählbar), wenn sie Σ_1-definierbar ist.

Details: Übung!

Als einfache Folgerung von Satz 9.21 erhalten wir:

Satz 9.22 (Unentscheidbarkeit der Arithmetik)

$Th(\mathcal{N})$ ist nicht rekursiv aufzählbar.

D.h: Es gibt keinen Algorithmus, der nach und nach alle in der Standardarithmetik $\mathcal{N} = (\mathbb{N}, \leq^{\mathcal{N}}, +^{\mathcal{N}}, \times^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}})$ gültigen Sätze der Logik erster Stufe ausgibt.

Beweis:

Sei $M \subseteq \mathbb{N}$ eine Menge, die rekursiv aufzählbar aber nicht entscheidbar ist. (Eine solche Menge gibt es — z.B. indem die Zahlen in M genau diejenigen Turingmaschinen repräsentieren, die bei leerer

Eingabe nach endlich vielen Schritten anhalten).

Da M rekursiv aufzählbar ist, gibt es gemäß Satz 9.21 (b) eine Σ_1-Formel $\varphi_M(x)$, die M definiert, d.h. f.a. $n \in \mathbb{N}$ gilt: $n \in M \iff \mathcal{N} \models \varphi_M[n]$.

Insbes. gilt f.a. $n \in \mathbb{N}$, dass

$$n \in M \iff \mathcal{N} \models \varphi_M \frac{\underline{n}}{x} . \quad (*)$$

Angenommen, $Th(\mathcal{N})$ ist rekursiv aufzählbar.
Dann ist $Th(\mathcal{N})$ sogar entscheidbar (denn: um zu testen, ob $\varphi \in Th(\mathcal{N})$ liegt, kann man $Th(\mathcal{N})$ aufzählen, bis entweder φ oder $\neg\varphi$ ausgegeben wird).

Gemäß Lemma 9.11 (c) ist dann die Menge $\{ n \in \mathbb{N} : Th(\mathcal{N}) \models \varphi_M \frac{\underline{n}}{x} \}$ entscheidbar.

Beachte: $\{ n \in \mathbb{N} : Th(\mathcal{N}) \models \varphi_M \frac{\underline{n}}{x} \} = \{ n \in \mathbb{N} : \varphi_M \frac{\underline{n}}{x} \in Th(\mathcal{N}) \}$

$$= \{ n \in \mathbb{N} : \mathcal{N} \models \varphi_M \frac{\underline{n}}{x} \} \underset{(*)}{=} M .$$

Somit ist M entscheidbar.

$\lightning$ Widerspruch zur Wahl von M.

$\square_{\text{Satz 9.22}}$

9.4 Der Satz von Trakhtenbrot

Boris A. Trakhtenbrot: russisch-israelischer Mathematiker, * 1921.
Alternative Schreibweisen: Trachtenbrot, Trahenbrot
Original-Schreibweise (kyrillisch): Трахтенброт

Definition 9.23

Sei σ eine Signatur.

(a) Ein FO[σ]-Satz φ heißt <u>im Endlichen erfüllbar</u>, falls es eine <u>endliche</u> σ-Struktur $\mathfrak{A}$ gibt, die φ erfüllt.

(b) Das <u>endliche Erfüllbarkeitsproblem für FO[σ]</u> (kurz: <u>endl-Erf-FO[σ]</u>) ist das wie folgt definierte Berechnungsproblem:

<u>Eingabe</u>: Ein FO[σ]-Satz φ

<u>Frage</u>: Ist φ im Endlichen erfüllbar?

<u>Formal</u>: endl-Erf-FO[σ] := $\{\varphi : \varphi$ ist ein im Endlichen erfüllbarer FO[σ]-Satz$\}$

Unter Verwendung des Satzes von Gaifman (oder, alternativ, des Satzes von Hanf), sieht man leicht, dass folgendes gilt:

Satz 9.24
Ist σ eine relationale Signatur, die ausschließlich aus Relationssymbolen der Stelligkeit 1 besteht, so ist das <u>endliche Erfüllbarkeitsproblem für FO[σ]</u> <u>entscheidbar</u>.

<u>Beweis</u>: Übung

Der Satz von Trakhtenbrot besagt, dass Satz 9.24 nicht für Signaturen gilt, die mind. ein Relationssymbol der Stelligkeit ≥ 2 enthalten:

Satz 9.25 (Satz von Trakhtenbrot, 1950)

Ist σ eine Signatur, die mindestens ein Relationssymbol der Stelligkeit ≥ 2 enthält, so ist das endliche Erfüllbarkeitsproblem für $FO[\sigma]$ rekursiv aufzählbar, aber nicht entscheidbar.

Beweis: Die Semi-Entscheidbarkeit erhält man durch einen Algorithmus, der bei Eingabe eines $FO[\sigma]$-Satzes φ nach und nach für $n = 1, 2, 3, \ldots$ sämtliche σ-Strukturen $\mathfrak{A}$ mit Universum $\{1, \ldots, n\}$ erzeugt und für jede dieser Strukturen testet, ob sie φ erfüllen.
Da ein Problem genau dann rekursiv aufzählbar ist, wenn es semi-entscheidbar ist, folgt damit, dass endl-Erf-$FO[\sigma]$ rekursiv aufzählbar ist.

Die Unentscheidbarkeit von endl-Erf-$FO[\sigma]$ zeigen wir hier für den Spezialfall, dass $\sigma = \tilde{\sigma}_{Ar}$ ist, wobei $\tilde{\sigma}_{Ar} := \{ \underset{2}{\leq}, \underset{3}{R_+}, \underset{3}{R_\times}, \underset{1}{R_0}, \underset{1}{R_1} \}$.

Beachte: Für $\sigma := \sigma_{Ar}$ ist $\tilde{\sigma}_{Ar} = \sigma_{rel}$ gemäß Definition 2.18

Die allgemeine Aussage (für beliebige Signaturen, die mind. ein Relationssymbol der Stelligkeit ≥ 2 enthalten, erhält man dann, indem man endliche $\tilde{\sigma}_{Ar}$-Strukturen auf geeignete Weise durch endliche gerichtete Graphen repräsentiert (Details: Lösung).

Um die Unentscheidbarkeit von endl-Erf-FO[$\tilde{\sigma}_{Ar}$] nachzuweisen, betrachten wir eine Menge $H \subseteq \mathbb{N}$, die rekursiv aufzählbar, aber nicht entscheidbar ist. (Eine solche Menge gibt es – z.B. indem die Zahlen in H genau diejenigen Turingmaschinen repräsentieren, die bei leerer Eingabe nach endlich vielen Schritten anhalten).

Da H r.e. ist, gibt es gemäß Satz 9.21 (b) eine Σ_1-Formel $\varphi_H(x)$, die H definiert. D.h.: F.a. $n \in \mathbb{N}$ gilt: $n \in H \iff \mathcal{N} \models \varphi_H[n]$.

Betrachte nun für jedes $n \in \mathbb{N}$ den FO[σ_{Ar}]-Satz

$$\varphi_n := \varphi_H(\underline{n}) = \varphi_H \frac{\underline{n}}{x} .$$

Offensichtlicherweise gilt f.a. $n \in \mathbb{N}$:

1) $\mathcal{N} \models \varphi_n \iff n \in H$, und

2) φ_n ist ein Σ_1-Satz, d.h. es gibt eine Variable y und eine Δ_0-Formel $\psi_n(y)$, so dass $\varphi_n = \exists y\, \psi_n(y)$.

Ziel: Wir nutzen im Folgenden φ_n, um einen $FO[\sigma_{Ar}]$-Satz $\tilde{\varphi}_n$ zu konstruieren, für den gilt:

$$\circledast_0: \boxed{\tilde{\varphi}_n \text{ ist im Endlichen erfüllbar} \iff \mathcal{N} \models \varphi_n \overset{1)}{\iff} n \in H.}$$

Daraus folgt dann direkt, dass das endliche Erfüllbarkeitsproblem für $FO[\sigma_{Ar}]$ nicht entscheidbar ist. (Denn sonst wäre H entscheidbar, indem man bei Eingabe einer Zahl n zunächst die Formel $\tilde{\varphi}_n$ erzeugt und dann testet, ob $\tilde{\varphi}_n$ im Endlichen erfüllbar ist).

Die Konstruktion der Formel $\tilde{\varphi}_n$ erfolgt in mehreren Schritten.

Schritt 1: Sei z eine Variable, die nicht in der Formel $\varphi_n = \exists y\, \psi_n(y)$ vorkommt.

Sei $\varphi_n' := \exists z\, \exists y < z\, \psi_n'(y,z)$, wobei

$\psi_n'(y,z)$ die Formel ist, die aus der

Δ_0-Formel $\psi_n(y)$ entsteht, indem zunächst

- jede Teilformel der Form $\exists v \leq t\, \chi$ (bzw. $\forall v \leq t\, \chi$) ersetzt wird durch die Formel $\exists v < z\, (v \leq t \wedge \chi)$ (bzw. $\forall v < z\, (v \leq t \rightarrow \chi)$), und

danach

- jede atomare Formel α, in der Terme $t_1, \dots, t_\ell$ vorkommen, ersetzt wird durch die Formel $(\alpha \wedge t_1 < z \wedge \dots \wedge t_\ell < z)$.

Man kann sich leicht davon überzeugen, dass folgendes gilt:

$$\boxed{\mathcal{N} \models \varphi_n' \iff \mathcal{N} \models \varphi_n.} \qquad (*)_1$$

Setze nun

$$\rho_n'(z) := \exists y < z \ \psi_n'(y,z)$$

und beachte, dass $\varphi_n' = \exists z \ \rho_n'(z)$.

Gemäß der in Schritt 1 durchgeführten Konstruktion ist $\rho_n'(z)$ eine Δ_0-Formel, in der jede Quantifizierung einer Variablen v beschränkt ist durch $v < z$, und in der jeder Term t beschränkt ist durch $t < z$.

<u>Schritt 2:</u> Gemäß Satz 2.19 (a) gibt es zu der $FO[\sigma_{Ar}]$-Formel $\rho_n'(z)$ eine $FO[\tilde{\sigma}_{Ar}]$-Formel $\tilde{\rho}_n'(z)$, so dass für alle $m \in \mathbb{N}$ gilt:

$$\mathcal{N} \models \rho_n'[m] \iff \mathcal{N}_{rel} \models \tilde{\rho}_n'[m],$$

wobei $\mathcal{N}_{rel}$ die $\tilde{\sigma}_{Ar}$-Struktur ist, die gemäß Definition 2.18 (b) der σ_{Ar}-Struktur $\mathcal{N}$ zugeordnet ist.
Insbes gilt für $\tilde{\varphi}_n' := \exists z \ \tilde{\rho}_n'(z)$, dass $\boxed{\mathcal{N}_{rel} \models \tilde{\varphi}_n' \iff \mathcal{N} \models \varphi_n'}$ $(*)_2$

Aufgrund der im Beweis von Satz 2.19 (a) durchgeführten Konstruktion können wir o.B.d.A annehmen, dass in der Formel $\tilde{\rho}_n'(z)$ jede

Quantifizierung einer Variablen v beschränkt ist durch $v < z$.

<u>Schritt 3:</u> Für jedes $m \in \mathbb{N}_{\geq 1}$ sei nun $\mathcal{W}_{|\{0,\dots,m\}}$ die gemäß Definition 3.27 (d) gegebene Substruktur von $\mathcal{W}_{rel}$ mit Universum $\{0,\dots,m\}$.

Da in $\tilde{\rho}'_n(z)$ alle Quantifizierungen einer Variablen v durch $v<z$ beschränkt sind, gilt f.a. $m \in \mathbb{N}_{\geq 1}$ und alle $m' \geq m$:

$$\mathcal{W}_{rel} \models \tilde{\rho}'_n[m] \iff \mathcal{W}_{|\{0,\dots,m'\}} \models \tilde{\rho}'_n[m].$$

Daraus folgt, dass für den $FO[\tilde{\sigma}_{Ar}]$-Satz

$$\tilde{\varphi}'_n := \exists z\, \tilde{\rho}'_n(z)$$

gilt:

$(*)_3$
$$\boxed{\mathcal{W}_{rel} \models \tilde{\varphi}'_n \iff \text{es gibt ein } m \in \mathbb{N}_{\geq 1}\text{, s.d. } \mathcal{W}_{|\{0,\dots,m\}} \models \tilde{\varphi}'_n .}$$

Schritt 4: Wir konstruieren nun einen $FO[\tilde{\sigma}_{Ar}]$-Satz η, so dass gilt:

$\circledast_4$ | Für jede endliche $\tilde{\sigma}_{Ar}$-Struktur $\mathfrak{A}$ gilt: $\mathfrak{A} \models \eta \iff$ es gibt ein $m \in \mathbb{N}_{\geq 1}$, s.d. $\mathfrak{A} \cong \mathcal{N}_{|\{0,\dots,m\}}$

Beachte: Dann gilt für den $FO[\tilde{\sigma}_{Ar}]$-Satz

$$\tilde{\varphi}_n := (\tilde{\varphi}'_n \wedge \eta)$$ folgendes:

$\tilde{\varphi}_n$ ist im Endlichen erfüllbar

$\overset{\circledast_4}{\iff}$ es gibt ein $m \in \mathbb{N}_{\geq 1}$ s.d. $\mathcal{N}_{|\{0,\dots,m\}} \models \tilde{\varphi}'_n$

$\overset{\circledast_3}{\iff}$ $\mathcal{N}_{rel} \models \tilde{\varphi}'_n$

$\overset{\circledast_2}{\iff}$ $\mathcal{N} \models \varphi'_n$

$\overset{\circledast_1}{\iff}$ $\mathcal{N} \models \varphi_n \overset{\circledast_1}{\iff} n \in H$.

Somit ist $\tilde{\varphi}_n$ die für $\circledast_0$ gesuchte Formel.

Um den Beweis von Satz 9.25 abzuschließen, genügt es also, die für $\circledast_4$ gesuchte Formel η zu finden.

Dazu konstruieren wir einen $FO[\tilde{\sigma}_{Ar}]$-Satz η, der in einer $\tilde{\sigma}_{Ar}$-Struktur $\mathfrak{A}$ folgendes besagt:

1) $|A| \geq 2$

2) $\leq^{\mathfrak{A}}$ ist eine diskrete lineare Ordnung mit kleinstem und größtem Element.

Im Folgenden bezeichnen wir mit 0, 1, max das kleinste, das zweitkleinste und das größte Element bzgl $\leq^{\mathfrak{A}}$.

3) $R_0^{\mathfrak{A}} = \{0\}$, $R_1^{\mathfrak{A}} = \{1\}$

4) $R_+^{\mathfrak{A}}$ ist der Graph einer partiellen Funktion $+$ von $A \times A$ nach A, die die folgenden Eigenschaften besitzt:

4.1) F.a. $(a,b) \in Def(+)$ gilt: $(b,a) \in Def(+)$ und $b+a = a+b$

4.2) F.a. $a \in A$ gilt: $(a,0) \in Def(+)$ und $a+0 = a$

4.3) F.a. $a \in A$ gilt:
- $(a,1) \in Def(+) \iff a \neq max$, und
- Falls $a \neq max$, so ist $a+1$ der Nachfolger von a bzgl $\leq^{\mathfrak{A}}$.

4.4) F.a. $(a,b) \in Def(+)$ mit $a+b \neq max$ gilt:
- $b \neq max$,
- $(a, b+1) \in Def(+)$, und
- $a+(b+1) = (a+b)+1$.

5) $R_\times^{\mathfrak{A}}$ ist der Graph einer partiellen Funktion $\cdot$ von $A \times A$ nach A, die die folgenden Eigenschaften besitzt:

5.1) F.a. $(a,b) \in Def(\cdot)$ gilt: $(b,a) \in Def(\cdot)$ und $b \cdot a = a \cdot b$

5.2) F.a. $a \in A$ gilt:
- $(a,0) \in Def(\cdot)$ und $a \cdot 0 = 0$, und
- $(a,1) \in Def(\cdot)$ und $a \cdot 1 = a$

5.3) Falls $|A| \geq 3$, so ist $(1,1) \in Def(+)$ und es gilt:

5.3.1) F.a. $a \in A$ mit $(a,a) \in Def(+)$ gilt:
- $(a, 1+1) \in Def(\cdot)$ und
- $a \cdot (1+1) = a + a$

5.3.2) F.a. $a,b \in A$ mit $(a,b) \in Def(\cdot)$ und $a \neq 0$ und $(a \cdot b, a) \in Def(+)$ gilt:
- $(b,1) \in Def(+)$,
- $(a, b+1) \in Def(\cdot)$, und
- $a \cdot (b+1) = a \cdot b + a$.

Die Bedingungen 1) – 5) können leicht durch einen $FO[\tilde{\sigma}_{Ar}]$-Satz η formalisiert werden.
Man kann zeigen (Details: Übung), dass für jede endliche $\tilde{\sigma}_{Ar}$-Struktur $\mathfrak{A}$ gilt: $\mathfrak{A}$ erfüllt die Bedingungen 1) – 5) genau dann, wenn es ein $m \in \mathbb{N}_{\geq 1}$ gibt, so dass

$$\mathfrak{A} \cong \mathcal{N}|_{\{0,\ldots,m\}}.$$

$\square$ Satz von Trakhtenbrot

Folgerungen aus dem Satz von Trakhtenbrot

Wir betrachten zunächst die folgende "endliche Variante" des Allgemeingültigkeitsproblems:

Def. 9.26:

Sei σ eine Signatur.

(a) Ein $FO[\sigma]$-Satz φ heißt im Endlichen allgemeingültig, falls für jede endliche σ-Struktur $\mathfrak{A}$ gilt: $\mathfrak{A} \models \varphi$.

(b) Das endliche Allgemeingültigkeitsproblem für $FO[\sigma]$ ist das folgende Berechnungsproblem:

Eingabe: Ein $FO[\sigma]$-Satz φ

Frage: Ist φ im Endlichen allgemeingültig?

Formal: $\text{endl-Allg-}FO[\sigma] := \{ \varphi : \varphi \text{ ist ein im Endlichen allgemeingültiger } FO[\sigma]\text{-Satz} \}$

Als Folgerung aus Satz 9.24 und Satz 9.25 erhalten wir:

Korollar 9.27: ((Un-)Entscheidbarkeit des endlichen Allgemeingültigkeitsproblems für FO[σ])

Sei σ eine Signatur.

(a) Falls σ relational ist und alle Relationssymbole in σ die Stelligkeit 1 haben, so ist das Problem endl-Allg-FO[σ] entscheidbar.

(b) Falls σ mindestens ein Relationssymbol der Stelligkeit ≥ 2 enthält, so ist das Problem endl-Allg-FO[σ] nicht rekursiv aufzählbar.

Beweis: Man beachte, dass für jeden FO[σ]-Satz φ gilt: φ ist im Endlichen erfüllbar $\iff$ $\neg\varphi$ ist im Endlichen allgemeingültig).

(a) folgt daher direkt aus Satz 9.24. Zum Beweis von (b): Falls endl-Allg-FO[{E}] r.e. wäre, so wäre auch das Komplement von endl-Erf-FO[{E}] r.e. Somit wären sowohl endl-Erf-FO[{E}] als auch das Komplement r.e., und daher wäre endl-Erf-FO[{E}] entscheidbar ↯.

Bemerkung 9.28:

Man vergleiche Kor. 9.27 (b) mit Kor. 9.3:

Die Menge aller allgemeingültigen Sätze ist rekursiv aufzählbar; die Menge aller im Endlichen allgemeingültigen Sätze nicht.

Unter Verwendung des Satzes von Trakhtenbrot kann man die Unentscheidbarkeit vieler konkreter Logikprobleme nachweisen.

Im Folgenden wird dies exemplarisch an der Eigenschaft der <u>Ordnungsinvarianz</u> von Formeln dargelegt.

<u>Definition 9.29</u> (Ordnungsinvarianz)

Sei σ eine Signatur und sei $\leq$ ein 2-stelliges Relationssymbol, das <u>nicht</u> zu σ gehört.

<u>(a)</u> Ein $FO[\sigma \cup \{\leq\}]$-Satz φ heißt <u>im Endlichen ordnungsinvariant</u>, falls für alle <u>endlichen</u> σ-Strukturen $\mathfrak{A}$ und alle linearen Ordnungen $\leq_1^{\mathfrak{A}}$ und $\leq_2^{\mathfrak{A}}$ auf A gilt: $(\mathfrak{A}, \leq_1^{\mathfrak{A}}) \models \varphi \iff (\mathfrak{A}, \leq_2^{\mathfrak{A}}) \models \varphi$.

<u>(b)</u> Das <u>endliche Ordnungsinvarianz-Problem für $FO[\sigma \cup \{\leq\}]$</u> ist das folgende Berechnungsproblem: <u>Eingabe</u>: Ein $FO[\sigma \cup \{\leq\}]$-Satz φ

<u>Frage</u>: Ist φ im Endlichen ordnungsinvariant?

<u>Formal</u>: endl-Ordinv-$FO[\sigma \cup \{\leq\}] := \{\varphi : \varphi$ ist ein im Endlichen ordnungsinvarianter $FO[\sigma \cup \{\leq\}]$-Satz$\}$

Unter Verwendung des Satzes von Trakhtenbrot kann man leicht einen Beweis für den folgenden Satz finden:

Satz 9.30 (Unentscheidbarkeit der Ordnungsinvarianz)

Sei σ eine Signatur, die mind. ein Relationssymbol R mit $ar(R) \geq 2$ und ein weiteres Rel.symbol P mit $ar(P) \geq 1$ enthält. Dann ist das Problem endl-Ordinv-FO$[\sigma \cup \{<\}]$ nicht entscheidbar.

Beweis: Aus Kor. 9.27 b) wissen wir, dass das Problem endl-Allg-FO$[\{R\}]$ nicht entscheidbar ist. Im Folgenden nehmen wir an, dass das Problem endl-Ordinv-FO$[\sigma \cup \{<\}]$ entscheidbar wäre und zeigen, dass dann auch endl-Allg-FO$[\{R\}]$ entscheidbar sein müsste.

Wir betrachten o.B.d.A. den Fall, dass $ar(P) = 1$ ist.

Bei Eingabe eines FO$[\{R\}]$-Satzes φ geht unser Algorithmus zum Entscheiden, ob φ im Endlichen allgemeingültig ist, folgendermaßen vor:

1) Teste, ob $\forall$ a. $\{R\}$-Strukturen $\mathfrak{A}$ mit $A = \{1\}$ gilt: $\mathfrak{A} \models \varphi$.
Falls nein: STOP mit Ausgabe "φ ist nicht im Endlichen allgemeingültig"
Sonst: weiter mit Schritt 2.

2) Sei $\tilde{\psi}$ der unten konstruierte $FO[\{R, P, \leq\}]$-Satz.

Teste, ob $\tilde{\psi}$ im Endlichen ordnungs-invariant ist.

Falls ja, so STOP mit Ausgabe "ψ ist im Endlichen allgemeingültig".

Sonst: STOP mit Ausgabe "ψ ist nicht im Endlichen allgemeingültig"

Die Formel $\tilde{\psi}$ ist dabei wie folgt gewählt:

$$\tilde{\psi} := (\neg\psi \rightarrow \chi),$$

wobei $\chi := \exists x \big(P(x) \wedge \forall y \; x \leq y \big)$.

Man beachte, dass f.a. endlichen $\{P\}$-Strukturen $\mathfrak{A}$ und alle linearen Ordnungen $\leq^{\mathfrak{A}}$ auf A gilt:

$(\mathfrak{A}, \leq^{\mathfrak{A}}) \models \chi \iff P^{\mathfrak{A}} = \{\min^{\mathfrak{A}}\}$, wobei $\min^{\mathfrak{A}}$ das kleinste Element in A bzgl $\leq^{\mathfrak{A}}$ ist.

Daher gilt:

$\tilde{\psi}$ ist ordnungsinvariant im Endlichen

$\iff$ f.a. (endlichen) $\{R\}$-Strukturen $\mathfrak{A}$ mit $\mathfrak{A} \models \neg\psi$ gilt: $|A| \leq 1$

$\iff$ f.a. (endlichen) $\{R\}$-Strukturen $\mathfrak{A}$ mit $|A| \geq 2$ gilt: $\mathfrak{A} \models \psi$.

Daraus folgt, dass der oben angegebene Algorithmus die korrekte Ausgabe liefert.

$\square$

<u>Bemerkung</u> 9.31

Der obige Beweis von Satz 9.30 zeigt sogar, dass das Problem endl-Ordinv-FO$[\sigma \cup \{<\}]$ <u>nicht</u> semi-entscheidbar, also nicht rekursiv aufzählbar ist.