9.3 FO-Definierbarkeit der berechenbaren Funktionen

Definition 9.14 (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. 6.3):

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

(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.

<u>Notation 9.15</u> (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 $\forall x \leq t \, (\neg x = t \to \varphi)$

<u>Definition 9.16</u> (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 zum Beweis von Gödels Unvollständigkeitssätzen. Das Lemma besagt, dass man Folgen natürlicher Zahlen durch einzelne Zahlen kodieren kann — und zwar so, dass diese Kodierung durch eine beschränkte $FO[\sigma_{Ar}]$-Formel definiert werden kann.

Lemma 9.17 (Das Lemma über die β-Funktion)

Es gibt eine Δ_0-definierbare Funktion

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

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 $s \geq \max\{1, n_0, \dots, n_{\ell-1}\}$, 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)

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

<u>Beweis:</u> Sei $\ell \in \mathbb{N}$ mit $\ell \geq 1$ und

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

Sei p die kleinste Primzahl mit

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

Sei

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

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

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

<u>Behauptung 1:</u> Für alle $i \in \{0, \ldots, \ell-1\}$ 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

<u>(1)</u> $t = m_0 + m_1 \cdot ((i+1) + n \cdot p + m_2 \cdot p^2)$,

<u>(2)</u> $n < p$,

<u>(3)</u> $m_0 < m_1$ und

<u>(4)</u> es gibt ein $j \leq m_1$ so dass $m_1 = p^{2j}$.

Beweis von Beh. 1:

"$\Rightarrow$": Wähle

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

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

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

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

- $2j = 2i$, dh $j = i$ 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. $i \in \{0, \dots, l-1\}$ 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:

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

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

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

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

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

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

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

<u>Beweis:</u> 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:

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

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

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

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

Beweis: 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.

Behauptung 4: 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 $\beta'(p,t,i) = n_i$

Beweis: Folgt unmittelbar aus der Konstruktion der Formel ψ.

□ Beh 4.

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

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

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:

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

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 und der Tatsache, dass $g(p,t) \geq t$ ist ($\nearrow$ Beh 5).

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

Ein formales Berechnungsmodell:

Im Folgenden wollen wir zeigen, dass alle berechenbaren Funktionen und rekursiv aufzählbaren Relationen durch $\text{FO}[\sigma_{Ar}]$-Formeln definiert werden können (im Sinne von Def. 9.14)

(— 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 <u>deterministische 1-Band-Turingmaschinen</u>

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

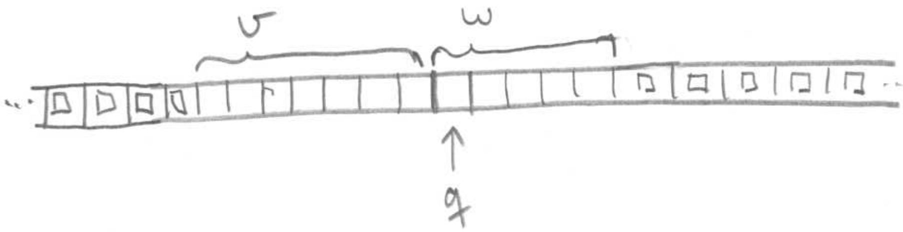
$$M = (\underset{\substack{\uparrow \\ \text{Menge der Zustände}}}{Q}, \underset{\substack{\uparrow \\ \text{Bandalphabet}}}{A_{TM}}, \underset{\substack{\uparrow \\ \text{Überführungsfunktion}}}{\delta}, \underbrace{q_0}_{\text{Startzustand}}, \underbrace{F}_{\text{Endzustände}})$$

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 $K = vqw \in (A_{TM} \cup Q)^*$, wobei $v, w \in A_{TM}^*$ und $q \in Q$ ist.

$K = vqw$ 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 $K \xrightarrow[M]{} K'$, um auszudrücken, dass K' die <u>Nachfolgekonfiguration</u> von K ist.

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

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

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

die <u>Unärdarstellung von n</u>.

<u>Definition 9.18</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

$$q_0\, |^{m_1} \# |^{m_2} \# \cdots \# |^{m_k} \xrightarrow[M]{*} |^n q .$$

<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 $\mathrm{Def}(f_R) = R$ und $f_R(m_1, \dots, m_k) = 1$, f.a. $(m_1, \dots, m_k) \in R$ TM-berechenbar ist.