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

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

die <u>Unärdarstellung</u> von n.

Definition 9.18

(a) 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 $m_1, \ldots, m_k, n \in \mathbb{N}$ gilt:

$f(m_1, \ldots, m_k) = n$ (insbes.: $(m_1, \ldots, m_k) \in Def(f)$) $\iff$ es gibt ein $q \in F$ so dass $q_0 |^{m_1} \# |^{m_2} \# \cdots \# |^{m_k} \xrightarrow[M]{*} |^n q$.

(b) 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 $f_R(m_1, \ldots, m_k) = 1$ f.a. $(m_1, \ldots, m_k) \in R$ 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.

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

Vereinbarung 3.19

Wir identifizeren 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 9.20</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>: $$\forall z' < y \left(z' \neq z \longrightarrow \left(\varphi_\beta(x,z',\underline{0}) \vee \varphi_\beta(x,z',\underline{1}) \vee \varphi_\beta(x,z',\underline{2}) \right)\right)\Big)$$

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 9.21 (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 $q_0 1^{m_1} \# \dots \# 1^{m_k}$ (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 $1^n q$ kodiert.

Beweis

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

- $B(x, y)$ und $B(x', y')$ repräsentieren Konfigurationen (nütze dazu Lemma 9.20)
- 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) $\varphi^M_{Start}(x, y, z_1, \ldots, z_k)$ 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)

Lemma 9.21

<u>Definition 9.22</u> (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 $\varphi \in \Delta_0$.

<u>Satz 9.23</u> (Σ_1-Definierbarkeit der berechenbaren partiellen Funktionen und der rek. aufzählbaren Relationen)

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

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

<u>Beweis</u>: Klar: (<u>b</u>) folgt leicht aus (a). Beweis zu (a):

Sei M eine Turingmaschine, die f berechnet (im Sinne von Definition 9.18).

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

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

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

$$\overset{\text{Def. 9.18}}{\iff} \text{es gibt ein } q \in F \text{ s.d. } q_0 1^{m_1} \# \cdots \# 1^{m_k} \xrightarrow[M]{*} 1^n q.$$

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 $\varkappa_1, \varkappa_2, \dots, \varkappa_r$ von Konfigurationen der Längen $l_1, l_2, \dots, l_r$ wird kodiert durch ein Tupel

$(s_1, l_1, s_2, l_2, \dots, s_r, l_r)$ nat. Zahlen,

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

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

$$B(s, 2r) = \begin{array}{c} (s_1, l_1, \dots, s_r, l_r) \\ \begin{array}{l} \text{Position } 0 \quad 1 \quad \dots \quad 2r-2 \quad 2r-1 \\ \qquad\qquad\qquad\qquad\; = 2(r-1) \quad = 2(r-1)+1 \end{array} \end{array}$$

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.

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

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

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

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

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

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

- 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 9.23

<u>Bemerkung 9.24</u>

Die Umkehrung von Satz 9.23 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 <u>genau dann</u> berechenbar (bzw rekursiv aufzählbar), wenn sie Σ_1-definierbar ist.

Als einfache Folgerung von Satz 9.23 erhalten wir:

<u>Satz 9.24</u> (Unentscheidbarkeit der Arithmetik)

$Th(\mathcal{N})$ ist <u>nicht</u> 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.

<u>Beweis:</u>

Sei $M \subseteq \mathbb{N}$ eine Menge, die rekursiv aufzählbar aber <u>nicht</u> 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 9.23 (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 9.13 (c) ist dann die Menge $\{ n \in \mathbb{N} : Th(\mathcal{N}) \models \varphi_M \frac{\underline{n}}{x} \}$ entscheidbar.

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

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

Somit ist M entscheidbar.

$\lightning$ Widerspruch zur Wahl von M.

$\square_{\text{Satz 9.24}}$

9.4 Die Minimale Arithmetik

<u>Definition 9.25</u>: (Die Theorie Q)

Die <u>minimale Arithmetik</u> ist die σ_{Ar}-Theorie Q, die von den folgenden $FO[\sigma_{Ar}]$-Sätzen axiomatisiert wird:

$\psi_{(Q1)} := \forall x \; \neg\, 0 = x+1$

$\psi_{(Q2)} := \forall x \forall y \; (x+1 = y+1 \rightarrow x=y)$

$\psi_{(Q3)} := \forall x \; x+0 = x$

$\psi_{(Q4)} := \forall x \forall y \; x+(y+1) = (x+y)+1$

$\psi_{(Q5)} := \forall x \; x \cdot 0 = 0$

$\psi_{(Q6)} := \forall x \forall y \; x \cdot (y+1) = (x \cdot y)+x$

$\psi_{(Q7)} := \forall x \; (x \leq 0 \leftrightarrow x=0)$

$\psi_{(Q8)} := \forall x \forall y \; (x \leq y+1 \leftrightarrow (x=y+1 \vee x \leq y))$

$\psi_{(Q9)} := \forall x \forall y \; (x \leq y \vee y \leq x)$

Lemma 9.26 ("Korrektheit" von Q)

Es gilt: $Q \subseteq Th(\mathcal{N})$,

und für alle $FO[\sigma_{Ar}]$-Formeln $\varphi(x_1,\dots,x_k)$ und alle $m_1,\dots,m_k \in \mathbb{N}$ gilt:

Falls $Q \models \varphi(\underline{m_1},\dots,\underline{m_k})$, so $\mathcal{N} \models \varphi[m_1,\dots,m_k]$.

Beweis: Man sieht leicht, dass für jedes Axiom ψ von Q gilt: $\mathcal{N} \models \psi$.

Daher gilt auch für jede Formel $\psi' \in Q$, dass $\mathcal{N} \models \psi'$. Somit gilt: $Q \subseteq Th(\mathcal{N})$.

Insbes. gilt daher f.a. Formeln $\varphi(x_1,\dots,x_k) \in FO[\sigma_{Ar}]$ und f.a. $n_1,\dots,n_k \in \mathbb{N}$ folgendes:

Falls $Q \models \varphi(\underline{n_1},\dots,\underline{n_k})$, so $\mathcal{N} \models \varphi(\underline{n_1},\dots,\underline{n_k})$,

dh $\mathcal{N} \models \varphi[n_1,\dots,n_k]$.

$\square$

<u>Gödels erster Unvollständigkeitssatz</u> besagt folgendes:

Jede σ_{Ar}-Theorie T, für die gilt:

($\underline{1}$) T ist widerspruchsfrei (d.h. erfüllbar),

($\underline{2}$) T ist effektiv axiomatisierbar (d.h. sie besitzt ein entscheidbares Axiomensystem),

und

($\underline{3}$) $T \supseteq Q$ (d.h. T umfasst die "minimale Arithmetik")

ist <u>unvollständig</u> (d.h. es gibt einen $FO[\sigma_{Ar}]$-Satz φ, so dass weder φ noch $\neg\varphi$ aus T folgt).

Um Gödels ersten Unvollständigkeitssatz beweisen zu können, müssen wir zunächst ein etwas genaueres Verständnis der "minimalen Arithmetik" Q erlangen.

Unser erstes "Etappenziel" dabei ist, den folgenden Satz zu beweisen:

<u>Satz 9.27</u> (Der Σ_1-Transfersatz)
Für jede Σ_1-Formel $\varphi(x_1,\dots,x_k)$ und f.a. $m_1,\dots,m_k \in \mathbb{N}$ gilt

$$\mathcal{N} \models \varphi[m_1,\dots,m_k] \iff Q \models \varphi(\underline{m_1},\dots,\underline{m_k})$$