## Satz 6.12 (Satz von Trakhtenbrot, 1950)

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

Für jede Signatur $\sigma$, die mindestens ein Relationssymbol der Stelligkeit $\geq 2$ enthält, ist das Erfüllbarkeitsproblem für $\mathrm{FO}[\sigma]$ auf FIN unentscheidbar.

Beweis:

Wir beweisen hier, dass das Erfüllbarkeitsproblem für $\mathrm{FO}[\sigma]$ auf FIN unentscheidbar ist für die spezielle Signatur

$$(*) \qquad \sigma := \{ \underset{2}{\leq}, \underset{2}{succ}, \underset{Konst.}{0}, \underset{3}{B}, \underset{2}{K}, \underset{2}{Z} \},$$

wobei

- $\leq$ und succ zwei 2-stellige Relationssymbole,
- 0 ein Konstantensymbol,
- B ein 3-stelliges Relationssymbol, und
- K und Z zwei 2-stellige Relationssymbole sind.

Die allgemeine Aussage von Satz 6.12 erhält man dann, indem man endliche $\sigma$-Strukturen (wobei $\sigma$ gemäß (*) gewählt ist), auf geeignete Weise durch endliche Graphen repräsentiert (Details: Übung).

Um die Unentscheidbarkeit des Erfüllbarkeitsproblems für FO[σ] auf FIN nachzuweisen, nutzen wir die Tatsache, dass das Halteproblem $H_\varepsilon$ unentscheidbar ist. Das Halteproblem $H_\varepsilon$ ist dabei wie folgt definiert:

> Halteproblem $H_\varepsilon$
>
> Eingabe: Eine deterministische 1-Band-Turingmaschine $M$
>
> Frage: Hält $M$ bei Eingabe des leeren Worts $\varepsilon$ nach endlich vielen Schritten?

Zum Beweis des Satzes von Trakhtenbrot nehmen wir an, dass das Erfüllbarkeitsproblem für FO[σ] auf FIN entscheidbar wäre, und zeigen, dass dann auch das Halteproblem $H_\varepsilon$ entscheidbar ist (↯ WIDERSPRUCH). Dazu wird die Berechnung einer beliebigen deterministischen 1-Band Turingmaschine $M$, von der wir wissen wollen, ob sie bei leerer Eingabe hält, durch einen FO[σ]-Satz $\varphi_M$ kodiert, für den gilt:

$\varphi_M$ hat ein endliches Modell (d.h. es gibt eine endliche $\sigma$-Struktur $\mathfrak{A}$ mit $\mathfrak{A} \models \varphi_M$) $\iff$ M hält bei Eingabe des leeren Worts $\varepsilon$ nach endlich vielen Schritten an.

Sei also $M = (Q, \Gamma, \delta, q_0, F)$ eine beliebige deterministische 1-Band Turingmaschine mit

- Zustandsmenge $Q = \{0, 1, \dots, s_Q\}$ für ein $s_Q \in \mathbb{N}$, Anfangszustand $q_0 = 0$ und Endzustandsmenge $F \subseteq Q$,
- Arbeitsalphabet $\Gamma = \{0, 1, \dots, s_\Gamma\}$ für ein $s_\Gamma \in \mathbb{N}$ und $\Box := 0$ als "Blank-Symbol" (d.h. $\Box$ ist das Leerzeichen, das anfangs auf allen Zellen des Bandes steht), und
- Überführungsfunktion
$$\delta : (Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{-1, 0, 1\}$$
($\delta(q, a) = (q', a', b)$ besagt folgendes: Wenn M in Zustand $q$ ist und ihr Schreib-/Lesekopf das

Symbol a liest, soll sie in Zustand $q'$ wechseln, das gelesene Symbol a durch das Symbol $a'$ ersetzen und anschließend den Schreib-/Lesekopf

- eine Position nach rechts bewegen, falls $b = 1$ ist
- – – – – – – – – – links – – – – – – – $b = -1$ – –
- da lassen, wo er gerade ist, falls $b = 0$ ist.)

Wir setzen $s := \max\{s_Q, s_\Gamma\}$ und nehmen o.B.d.A an, dass die Berechnung von M bei Eingabe $\varepsilon$ mehr als s Schritte durchführt.

Wir geben im Folgenden FO[$\sigma$]-Formeln an, die in ihren Modellen $\mathfrak{A}$ die folgenden Interpretationen der Symbole aus $\sigma$ erzwingen:

(1) $\leq^{\mathfrak{A}}$ ist eine lineare Ordnung,
$0^{\mathfrak{A}}$ ist ein beliebiges Element und
$succ^{\mathfrak{A}}$ ist die Nachfolger-Relation (engl: successor) bzgl $\leq^{\mathfrak{A}}$, d.h.

$$(a,b) \in succ^{\mathfrak{A}} \iff \begin{array}{l} a \leq^{\mathfrak{A}} b \text{ und } a \neq b \text{ und} \\ \text{für alle } c \text{ gilt} \\ c \leq^{\mathfrak{A}} a \text{ oder } b \leq^{\mathfrak{A}} c \end{array}$$

(2) $(t, p, \gamma) \in B^{\mathfrak{A}} \iff$

auf Bandposition $p$ steht zum Zeitpunkt $t$ der Berechnung von $M$ bei leerem Eingabewort das Symbol $\gamma$

(3) $(t, p) \in K^{\mathfrak{A}} \iff$

der Schreib-/Lesekopf von $M$ steht zum Zeitpunkt $t$ (der Berechnung bei leerem Eingabewort) auf Bandposition $p$

(4) $(t, q) \in Z^{\mathfrak{A}} \iff$

$M$ ist zum Zeitpunkt $t$ (der Berechnung bei leerem Eingabewort) in Zustand $q$.

Die $\sigma$-Struktur $\mathfrak{A}_M$, die die Berechnung von $M$ bei leerer Eingabe kodiert, ist wie folgt definiert.

- Das Universum $A_M$ ist

$$A_M := \begin{cases} \{0,1,\dots,n\} \cup \left\{p \in \mathbb{Z} : \begin{array}{l} \text{Bandposition } p \\ \text{wird bei der} \\ \text{Berechnung von } M \text{ bei} \\ \text{Eingabe } \varepsilon \text{ betreten} \end{array} \right\}, & \text{falls } M \text{ bei Eingabe } \varepsilon \text{ nach genau } n \text{ Schritten anhält} \\[2ex] \mathbb{N} \cup \left\{p \in \mathbb{Z} : \begin{array}{l} \text{Bandposition } p \\ \text{wird bei der Berechnung} \\ \text{von } M \text{ bei Eingabe } \varepsilon \text{ betreten} \end{array} \right\}, & \text{falls } M \text{ bei Eingabe } \varepsilon \text{ nie anhält} \end{cases}$$

- $\leq^{\mathfrak{A}_M}$, $succ^{\mathfrak{A}_M}$ und $0^{\mathfrak{A}_M}$ sind die natürliche lineare Ordnung auf $A_M$, deren Nachfolger-Relation und die Zahl 0

- $B^{\mathfrak{A}_M}$, $K^{\mathfrak{A}_M}$ und $Z^{\mathfrak{A}_M}$ sind genau so gewählt, wie in den Punkten (2), (3) und (4) beschrieben.

Insbes. gilt: $A_M$ ist endlich $\iff$ M hält bei Eingabe $\varepsilon$.

Nun zur Definition des $FO[\sigma]$-Satzes $\varphi_M$:

$\varphi_M$ soll in seinen Modellen $\mathfrak{A}$ erzwingen, dass $\mathfrak{A}$ die Struktur $\mathfrak{A}_M$ als Substruktur enthält.

Punkt (1) wird durch folgende Formel gewährleistet:

$$
\begin{aligned}
\varphi_{\leq, succ, 0} := \ & \forall x \forall y \forall z \Big( \\
& x \leq x && \text{(reflexiv)} \\
\wedge\ & \big( (x \leq y \wedge y \leq z) \rightarrow x \leq z \big) && \text{(transitiv)} \\
\wedge\ & \big( (x \leq y \wedge y \leq x) \rightarrow x = y \big) && \text{(antisymmetrisch)} \\
\wedge\ & ( x \leq y \vee y \leq x ) && \text{(konnex)} \\
\wedge\ & \big( succ(x,y) \leftrightarrow (x \leq y \wedge \neg x = y \wedge \forall u\, (u \leq x \vee y \leq u)) \big) && \text{(succ ist Nachfolger-relation bzgl. } \leq) \\
\wedge\ & \forall u \big( \exists v\, succ(u,v) \vee \forall w\, w \leq u \big) && \text{(jedes Element, das nicht das größte bzgl. } \leq \text{ ist, hat einen Nachfolger)} \\
\wedge\ & \forall u \big( \exists v\, succ(v,u) \vee \forall w\, u \leq w \big) && \text{(jedes Element, das nicht das kleinste bzgl. } \leq \text{ ist, hat einen Vorgänger)}
\end{aligned}
$$

In jedem Modell $\mathfrak{A}$ des Satzes $\varphi_{\leq, succ, 0}$

können wir die Elemente $a_0, a_1, a_2, a_3, \dots$,

für die $a_0 = 0^{\mathfrak{A}}$ und $(a_0, a_1) \in succ^{\mathfrak{A}}$ und

$(a_1, a_2) \in succ^{\mathfrak{A}}$ und $(a_2, a_3) \in succ^{\mathfrak{A}}$, ...

mit den natürlichen Zahlen $0, 1, 2, 3, \dots$ identifizieren.

Die folgende Formel erzwingt in ihren Modellen, dass die Variablen $z_0, z_1, z_2, \dots, z_s$ mit diesen Elementen $a_0, a_1, \dots, a_s$ (also im Gründe mit den natürlichen Zahlen $0, 1, \dots, s$) belegt werden:

$$\varphi_{Zahlen}(z_0, z_1, \dots, z_s) := z_0 = 0 \wedge \bigwedge_{i=1}^{s} succ(z_{i-1}, z_i)$$

Der $FO[\sigma]$-Satz $\varphi_M$ wird nun folgendermaßen gewählt:

$$\varphi_M := \varphi_{succ, \leq, 0} \wedge \exists z_0 \cdots \exists z_s \Big( \varphi_{Zahlen}(z_0, \dots, z_s) \wedge \varphi_{Band} \wedge \varphi_{Kopf} \wedge \varphi_{Zustand} \wedge \varphi_{Start} \wedge \varphi_{Schritt} \Big),$$

wobei die Formeln der letzten Zeile wie folgt gewählt sind:

$\varphi_{Band}$ besagt, dass zu jedem Zeitpunkt auf jeder Bandposition genau ein Symbol des Arbeitsalphabets $\Gamma = \{0, \ldots, s_\Gamma\}$ steht:

$$\varphi_{Band} := \forall x \Big( 0 \leq x \rightarrow \forall y \exists z \Big( B(x,y,z) \wedge \bigvee_{i=0}^{s_\Gamma} z = z_i \wedge$$
$$\forall z' \big( B(x,y,z') \rightarrow z' = z \big) \Big)\Big).$$

$\varphi_{Kopf}$ besagt, dass zu jedem Zeitpunkt der Schreib-/Lesekopf auf genau einer Bandposition steht.

$$\varphi_{Kopf} := \forall x \Big( 0 \leq x \rightarrow \exists y \Big( K(x,y) \wedge \forall y' \big( K(x,y') \rightarrow y' = y \big)\Big)\Big).$$

$\varphi_{Zustand}$ besagt, dass $M$ zu jedem Zeitpunkt in genau einem Zustand aus der Zustandsmenge $Q = \{0, 1, \ldots, s_Q\}$ ist.

$$\varphi_{Zustand} := \forall x \Big( 0 \leq x \rightarrow \exists z \Big( Z(x,z) \wedge \bigvee_{i=0}^{s_Q} z = z_i \wedge$$
$$\forall z' \big( Z(x,z') \rightarrow z' = z \big) \Big)\Big)$$

$\varphi_{start}$ besagt, dass $M$ zum Zeitpunkt $0$ in der Anfangskonfiguration bei Eingabe des leeren Worts ist, d.h. sie ist im Startzustand $q_0 = 0$, ihr Schreib-/Lesekopf steht auf Bandposition $0$, und auf jeder Bandposition steht das Blank-Symbol $\Box = 0$:

$$\varphi_{start} := \left( Z(0,0) \wedge K(0,0) \wedge \forall y\, B(0,y,0) \right).$$

Die Formel $\varphi_{schritt}$ besagt für jeden Zeitpunkt $t$: Falls $M$ zum Zeitpunkt $t$ nicht in einem Endzustand ist, so ist sie zum Zeitpunkt $t' := t+1$ in dem durch die Überführungsfunktion $\delta$ festgelegten Zustand und hat das entsprechende Symbol auf's Band geschrieben, den Kopf an die richtige Stelle bewegt und die Beschriftung aller anderen Bandpositionen nicht verändert.

Zur besseren Lesbarkeit werden in der folgenden Formel die Symbole $t, p, t', p'$ etc. benützt, um Variablen der Logik erster Stufe zu bezeichnen

Ist $q \in Q \setminus F$ und $\gamma \in \Gamma$, so schreiben wir

$q'_{q,\gamma}$, $\gamma'_{q,\gamma}$ und $m'_{q,\gamma}$, um den Zustand, das Symbol und die Bewegungsrichtung zu bezeichnen, für die gilt: $\delta(q,\gamma) = (q'_{q,\gamma}, \gamma'_{q,\gamma}, m'_{q,\gamma})$.

$$\varphi_{\text{Schritt}} := \forall t \, \forall p \bigwedge_{q \in Q \setminus F} \bigwedge_{\gamma \in \Gamma} \Bigg( \big( K(t,p) \wedge Z(t,z_q) \wedge B(t,p,z_\gamma) \big) \rightarrow$$

$$\exists t' \Big( succ(t,t') \wedge Z(t', z_{q'_{q,\gamma}})$$

$$\wedge \; B(t',p,z_{\gamma'_{q,\gamma}})$$

$$\wedge \; \forall p'' \Big( \neg p''=p \rightarrow \bigwedge_{\gamma'' \in \Gamma} \big( B(t',p'',z_{\gamma''}) \leftrightarrow B(t,p'',z_{\gamma''}) \big) \Big)$$

$$\wedge \; \exists p' \big( K(t',p') \wedge \chi_{m'_{q,\gamma}}(p,p') \big) \Big) \Bigg),$$

wobei die Formel $\chi_{m'_{q,\gamma}}(p,p')$ die jeweilige Kopfbewegung für $m'_{q,\gamma} \in \{-1,0,+1\}$ beschreibt:

$\chi_{+1}(p,p') := succ(p,p')$

$\chi_0(p,p') := p = p'$

$\chi_{-1}(p,p') := succ(p',p)$

Insgesamt sind wir nun fertig mit der Konstruktion der Formel $\varphi_M$, die die Berechnung von $M$ bei leerem Eingabewort beschreibt.

Gemäß der Konstruktion von $\varphi_M$ und $\mathfrak{A}_M$ gilt:

- $\mathfrak{A}_M \models \varphi_M$, und
- in jeder $\sigma$-Struktur $\mathfrak{A}$ mit $\mathfrak{A} \models \varphi_M$ gibt es Elemente $a_0, a_1, a_2, \dots, a_{-1}, a_{-2}, \dots$, die den Zeitpunkten bzw. Bandpositionen während der Berechnung von $M$ bei Eingabe $\varepsilon$ entsprechen, so dass $\mathfrak{A}$ eine Substruktur mit Universum

$$\{a_i : i \in A_M\},$$

enthält, die isomorph zu $\mathfrak{A}_M$ ist.

Insbesondere ist das Universum jedes Modells von $\varphi_M$ mindestens so groß wie das Universum von $\mathfrak{A}_M$. Somit gilt:

$\varphi_M$ hat ein endliches Modell $\iff$ $\mathfrak{A}_M$ ist endlich $\overset{\text{Def. von } \mathfrak{A}_M}{\iff}$ $M$ hält bei Eingabe des leeren Worts nach endlich vielen Schritten an.

Wenn das Erfüllbarkeitsproblem für $FO[\sigma]$ auf FIN entscheidbar wäre, wäre daher auch das Halteproblem $H_\varepsilon$ entscheidbar, denn bei Eingabe einer Turingmaschine $M$ könnte man zunächst den $FO[\sigma]$-Satz $\varphi_M$ konstruieren und dann auf endliche Erfüllbarkeit testen. Dies widerspricht aber der Tatsache, dass das Halteproblem $H_\varepsilon$ unentscheidbar ist.

$\square$ Satz 6.12

## Anwendungen des Satzes von Trakhtenbrot.

Unter Verwendung des Satzes von Trakhtenbrot kann man die Unentscheidbarkeit vieler konkreter Logikprobleme beweisen. Im Folgenden wird dies exemplarisch an der Eigenschaft der Ordnungsinvarianz von Formeln dargelegt.

**Definition 6.13**

Sei $\sigma$ eine Signatur und sei $\leq$ ein 2-stelliges Relationssymbol, das nicht zu $\sigma$ gehört.

Ein $FO[\sigma \cup \{\leq\}]$-Satz $\varphi$ heißt ordnungsinvariant auf FIN, falls für alle endlichen $\sigma$-Strukturen $\mathfrak{A}$ und alle linearen Ordnungen $\leq_1^{\mathfrak{A}}$ und $\leq_2^{\mathfrak{A}}$ auf $A$ gilt:

$$(\mathfrak{A}, \leq_1^{\mathfrak{A}}) \models \varphi \iff (\mathfrak{A}, \leq_2^{\mathfrak{A}}) \models \varphi .$$