Satz 166 (Rice)

Sei $\mathcal{R}$ die Menge aller (TM)-berechenbaren Funktionen und $\mathcal{S}$ eine nichttriviale Teilmenge von $\mathcal{R}$ (also $\mathcal{S} \neq \mathcal{R}$, $\mathcal{S} \neq \emptyset$). Dann ist

$$G(\mathcal{S}) := \{w \in \{0,1\}^*;\ \ \textit{die von } M_w \textit{ berechnete Funktion ist in } \mathcal{S}\}$$

unentscheidbar.

Beweis:
Sei Ω die total undefinierte Funktion.

1. Fall: $\Omega \in \mathcal{S}$

Sei $q \in \mathcal{R} - \mathcal{S}$ (es gibt ein derartiges q, da $\mathcal{S}$ nichttrivial), Q eine TM für q.
Zu $w \in \{0,1\}^*$ sei $f(w) \in \{0,1\}^*$ Gödelnummer einer TM, für die gilt:

1. bei Eingabe x ignoriert $M_{f(w)}$ diese zunächst und verhält sich wie M_w auf leerem Band.
2. wenn obige Rechnung hält, dann verhält sich $M_{f(w)}$ wie Q auf der Eingabe x.

f ist total und berechenbar.

Beweis:

Sei Ω die total undefinierte Funktion.

1. Fall: $\Omega \in \mathcal{S}$

$$\begin{aligned} w \in H_0 \quad &\Leftrightarrow M_w \text{ hält auf leerem Band} \\ &\Leftrightarrow M_{f(w)} \text{ berechnet die Funktion } q \ (\neq \Omega) \\ &\Leftrightarrow \text{die von } M_{f(w)}\text{-berechnete Funktion ist nicht in } \mathcal{S} \\ &\Leftrightarrow f(w) \notin G(\mathcal{S}) \end{aligned}$$

Also: $\bar{H}_0 \hookrightarrow_f G(\mathcal{S})$.

H_0 unentscheidbar (nicht rekursiv) $\Rightarrow$ $\bar{H}_0$ unentscheidbar $\Rightarrow$ $G(\mathcal{S})$ unentscheidbar.

Wir zeigen hier nur diesen Satz. Setzt man weitere Eigenschaften von $\mathcal{S}$ voraus, kann man sogar zeigen, dass $G(\mathcal{S})$ nicht einmal rekursiv aufzählbar ist.

Beweis:

Sei Ω die total undefinierte Funktion.

2. Fall: $\Omega \notin \mathcal{S}$

Seien $q \in \mathcal{S}, Q, f$ wie im Fall 1.

$$\begin{aligned} w \in H_0 \quad &\Leftrightarrow M_{f(w)} \text{ berechnet die Funktion } q\ (\neq \Omega) \\ &\Leftrightarrow \text{die von } M_{f(w)} \text{ berechnete Funktion ist in } \mathcal{S} \\ &\Leftrightarrow f(w) \in G(\mathcal{S}) \end{aligned}$$

Also: $H_0 \hookrightarrow_f G(\mathcal{S})$.

H_0 unentscheidbar $\Rightarrow G(\mathcal{S})$ unentscheidbar. $\square$

3. Anwendung der Unentscheidbarkeitsresultate auf kontextfreie Sprachen

Wie wir gesehen haben, gilt:

1. die regulären Sprachen sind unter allen Booleschen Operationen abgeschlossen.
2. die kontextfreien Sprachen sind nicht unter Komplement und Durchschnitt abgeschlossen.

Können wir entscheiden, ob der Durchschnitt zweier kontextfreier Sprachen leer ist?

Sei M eine (beliebige) TM (mit nur einem Band) mit Bandalphabet Σ und Zustandsmenge Q, sei $\# \notin \Sigma \cup Q$.

Definition 167

Definiere die Sprachen

$$C_M^{(0)} := \{c_0\#c_1^R\#c_2\#c_3^R \ldots c_m^{\pm R};\quad m \geq 0,\ c_i \text{ ist Konfiguration von } M,\ c_0 \text{ ist Anfangskonfiguration auf leerem Band, } c_m \text{ ist Endkonfiguration, und } c_{2j+1} \text{ ist Nachfolgekonfiguration von } c_{2j} \text{ für alle } j\}$$

$$C_M^{(1)} := \{c_0\#c_1^R\#c_2\#c_3^R \ldots c_m^{\pm R};\quad \text{wie oben, jetzt aber: } c_{2j} \text{ ist Nachfolgekonfiguration von } c_{2j-1} \text{ für alle zutreffenden } j \geq 1\}$$

Bemerkung: Hier steht $c_m^{\pm R}$ für c_m^R, falls m ungerade ist, und für c_m sonst.

Bemerkung: $C_M^{(0)}$ enthält nicht nur „echte“ Rechnungen von M, da $c_{2j-1} \to c_{2j}$ nicht unbedingt ein Schritt sein muss; das fordern wir jeweils nur für $c_{2j} \to c_{2j+1}$.

Lemma 168

Die Sprachen $C_M^{(0)}$ und $C_M^{(1)}$ sind deterministisch kontextfrei.

Beweis:

Es ist einfach, jeweils einen DPDA dafür zu konstruieren.

Bemerkung: Ein Kellerautomat ist lange nicht so mächtig wie eine Turingmaschine. Aber zwei Kellerautomaten (oder eine endliche Kontrolle mit zwei Kellern) sind so mächtig wie eine Turingmaschine (siehe Übung).

Lemma 169

$$w \in H_0 \Leftrightarrow C_{M_w}^{(0)} \cap C_{M_w}^{(1)} \neq \emptyset$$

Beweis:

Unmittelbar aus der Definition der beiden Sprachen!

Bemerkung: Falls M_w deterministisch ist und $w \in H_0$, dann enthält $C_{M_w}^{(0)} \cap C_{M_w}^{(1)}$ genau ein Element, nämlich die eine Rechnung von M_w auf leerem Band.

Satz 170

Das Schnittproblem für kontextfreie Sprachen ist unentscheidbar!

Beweis:

siehe oben.

Wir haben sogar gezeigt: Das Schnittproblem für deterministisch kontextfreie Sprachen ist unentscheidbar!

Sei M eine (beliebige) TM (wiederum mit nur einem Band) mit Bandalphabet Σ und Zustandsmenge Q, und sei $\# \notin \Sigma \cup Q$.

Lemma 171

Die Sprache

$$\bar{C}_M := \overline{C_M^{(0)} \cap C_M^{(1)}}$$

ist kontextfrei.

Beweis:

Es ist $w \in \bar{C}_M$, falls einer der folgenden Fälle zutrifft:

1. w hat nicht die Form $c_0\#c_1^R\#c_2\#c_3^R \ldots c_m^{\pm R}$;
2. c_0 stellt keine Anfangskonfiguration dar;
3. c_m stellt keine Endkonfiguration dar;
4. c_{i+1} ist nicht Nachfolgekonfiguration von c_i für ein i.

Für die ersten drei Fälle genügt eine reguläre Sprache, für den vierten Fall genügt die Vereinigung zweier kontextfreier Sprachen.

(Alternativ: $\bar{C}_M$ ist die Vereinigung der Komplemente zweier deterministisch-kontextfreier Sprachen!)

Satz 172

Für eine gegebene CFG G ist es allgemein unentscheidbar, ob

$$L(G) = \Sigma^* \,.$$

Beweis:

Für die im vorherigen Lemma betrachtete Sprache $\bar{C}_M$ kann eine kontextfreie Grammatik G effektiv konstruiert werden. Dann gilt:

$$L(G) = \Sigma^* \Leftrightarrow L(M) = \emptyset$$

Satz 173

Sei M eine TM, die auf jeder Eingabe mindestens zwei Schritte ausführt. Dann ist $C_M^{(0)} \cap C_M^{(1)}$ kontextfrei gdw $L(M)$ endlich ist.

Beweis:

„$\Leftarrow$" ist klar.

„$\Rightarrow$": Sei $L(M)$ unendlich. Angenommen, $C_M^{(0)} \cap C_M^{(1)}$ ist kontextfrei. Dann gibt es Wörter in $L(M)$, für die c_1 länger als die in Ogdens Lemma geforderte Konstante ist, so dass c_1 gepumpt werden kann, ohne c_0 und c_2 zu pumpen. Widerspruch!

Die Unentscheidbarkeit des Durchschnittsproblems kontextfreier Sprachen wird in der Literatur üblicherweise mit dem Post'schen Korrespondenzproblem (PCP) bewiesen, das nach Emil Post (1897–1954) benannt ist.

Definition 174 (Post'sches Korrespondenzproblem)

Gegeben: $(x_1, y_1), (x_2, y_2), \ldots (x_n, y_n)$ mit $x_i, y_i \in \Sigma^+$
Frage: gibt es eine Folge von Indizes $i_1\ (= 1), i_2, \ldots i_r \in \{1, \ldots, n\}$, so dass

$$x_{i_1} x_{i_2} \ldots x_{i_r} = y_{i_1} y_{i_2} \ldots y_{i_r}\ ?$$

Satz 175

PCP ist unentscheidbar.

Beweis:

Wir skizzieren, wie man mit Hilfe des PCP die Berechnung einer (det.) TM simulieren kann. Wir haben dazu (u.a.) Paare

$$\begin{aligned} (a,a) \quad & \text{für alle } a \in \Sigma \\ (u_1u_2u_3, aqb) \quad & \text{gemäß der inversen Übergangsfkt} \\ & \text{der TM, mit } a,b \in \Sigma, q \in Q \text{ und} \\ & u_1,u_2,u_3 \in \Sigma \cup Q \end{aligned}$$

Dies bedeutet, dass die TM bei der lokalen Konfiguration aqb diese im nächsten Schritt zu $u_1u_2u_3$ ändert.

Beweis:

Die allgemeine Situation sieht dann so aus, dass eine geeignete Indexfolge $i_1, \ldots, i_k$ folgende Zeichenreihen erzeugt:

x	c_1	$\ldots$	c_{r-1}	x_1	$\ldots$	x_{i-1}	q	x_i	x_{i+1}	$\ldots$	x_s
y	c_1	$\ldots$	c_{r-1}								

Es müssen nun die einzelnen x_i durch Paare der Form (a, a) gematcht werden, lediglich $x_{i-1}qx_i$ kann nur durch (genau bzw. höchstens) ein Paar der zweiten Form gematcht werden.

Damit ergibt sich wieder die allgemeine Situation wie oben, mit r um 1 erhöht, und man kann das Argument per Induktion abschließen.

Wir überlassen es als Übungsaufgabe herauszufinden, wie auch Anfang (u.a. soll o.B.d.A. als erster Index $i_1 = 1$ verwendet werden) und Ende der TM-Berechnung geeignet durch das PCP simuliert werden können. $\square$

Kapitel III Komplexität — Laufzeit und Speicherplatz

1. Notation und Grundlagen

Wir untersuchen grundlegende Eigenschaften von allgemeinen Maschinenmodellen (insbesondere der k-Band-Turingmaschine) in Bezug auf ihre Laufzeit und ihren Platzbedarf, sowie Beziehungen dieser Komplexitätsmaße beim Übergang zwischen der deterministischen (DTM) und der nichtdeterministischen (NDTM) Variante dieses Maschinenmodells.

Die k-Band-TM hat ein read-only Eingabeband, ein write-only Ausgabeband sowie k Arbeitsbänder.

Sei $L \subseteq \Sigma^*$ ein Problem/eine Sprache, und sei $w \in L$ eine Instanz von L. Sei weiterhin M eine TM für Problem L.

Definition 176

1. M deterministisch:

$$
\begin{aligned}
\text{(D)TIME}_M(w) &= \text{Anzahl der Schritte von } M \text{ bei Eingabe } w \\
&\quad \text{(ggf } \infty\text{)} \\
\text{(D)TIME}_M(n) &= \max\{\text{DTIME}_M(w);\ |w| = n\};\ n \in \mathbb{N}_0 \\
\text{(D)SPACE}_M(w) &= \text{max. Anzahl der Arbeitsbandfelder, die } M \\
&\quad \text{bei Eingabe } w \text{ pro Arbeitsband} \\
&\quad \text{besucht (ggf } \infty\text{)} \\
\text{(D)SPACE}_M(n) &= \max\{\text{DSPACE}_M(w);\ |w| = n\};\ n \in \mathbb{N}_0
\end{aligned}
$$

Definition 176

2. M nichtdeterministisch:

$$
\begin{aligned}
\mathsf{NTIME}_M(w) &= \text{Anzahl der Schritte einer kürzesten akzeptie-} \\
&\quad \text{renden Berechnung von } M \text{ bei Eingabe } w \\
&\quad (\text{ggf } \infty) \\
\mathsf{NTIME}_M(n) &= \max\{\mathsf{NTIME}_M(w);\ |w| = n\};\ n \in \mathbb{N}_0 \\
\mathsf{NSPACE}_M(w) &= \text{Anzahl der Arbeitsbandfelder, die eine} \\
&\quad \text{akzeptierende Berechung von } M \text{ bei} \\
&\quad \text{Eingabe } w \text{ pro Arbeitsband mindestens besucht} \\
&\quad (\text{ggf } \infty) \\
\mathsf{NSPACE}_M(n) &= \max\{\mathsf{NSPACE}_M(w);\ |w| = n\};\ n \in \mathbb{N}_0
\end{aligned}
$$

Bemerkungen:

1. Im nichtdeterministischen Fall gibt es auch eine strikte Variante der Komplexitätsmaße, die alle Berechnungen auf einer Eingabe zugrundelegt, nicht nur die akzeptierenden.
2. Der Platzbedarf einer k-Band-TM ist stets ≥ 1; Platzkomplexität $S(n)$ bedeutet daher eigentlich $\max\{S(n), 1\}$.
3. Die Laufzeit einer TM beträgt im Normalfall (andere TMs betrachten wir nicht) mindestens $n + 1$, d.h. die gesamte Eingabe wird gelesen; Zeitkomplexität $T(n)$ bedeutet daher eigentlich $\max\{T(n), n + 1\}$.

Beispiel 177

Die Sprache

$$L = \{w\#w^R;\ w \in \{0,1\}^*\}$$

kann jeweils von einer deterministischen TM in

1. Zeit $n + 1$
2. Platz $\log n$ (falls das Eingabeband bidirektional gelesen werden kann)

erkannt werden.