Vorlesungsmitschrift

Algorithmen und Berechenbarkeit

Vorlesung 13

Letztes Update: 2018/01/10 - 12:27 Uhr

Universelle Turingmaschine

Die bisher behandelten TMs wurden für jeweils ein spezifisches Problem entworfen. Reale Computer können jedoch programmiert werden und somit verschiedene Probleme lösen.

Die Universelle Turingmaschine $\mathcal{U}$ simuliert eine beliebige andere TM $\mathcal{M}$ auf einer beliebigen Eingabe w. Als Eingabe bekommt $\mathcal{U}$ einen String $< M >< w >$.

$\rightarrow$ $< w >$ ist die Kodierung der Eingabe für $\mathcal{M}$.

$\rightarrow$ $< M >$ ist die Kodierung der zu simulierenden TM $\mathcal{M}$. $< M >$ bezeichnet man auch als *Gödelnummer*.

Gödelnummerierung

Als Gödelnummerierung bezeichnet man ein injektive Abbildung aus der Menge aller TMs in $\{0,1\}^*$. TM-Kodierungen haben bestimmte Voraussetzungen, um als Gödelnummer zu gelten. Die zu kodierende TM habe:

- Zustandsmenge $Q = \{q_1, q_2, \cdots, q_t\}$
- Startzustand q_1
- Endzustand q_2
- Bandalphabet $\Gamma\{$ `0` , `1` , `B` $\}$
  - $\rightarrow$ `0`: Erstes Zeichen
  - $\rightarrow$ `1`: Zweites Zeichen
  - $\rightarrow$ `B`: Drittes Zeichen
- Bewegungen des SLK
  - $\rightarrow$ `L`: Erste Bewegung
  - $\rightarrow$ `N`: Zweite Bewegung
  - $\rightarrow$ `R`: Dritte Bewegung

Da jede TM in diese Form gebracht werden kann, ist bis hierher noch keine Einschränkung gegeben. Im Prinzip kommt es auf die Kodierung der Übergangsfunktionen δ an.
Ein Übergang

$$\delta(q_i, X_j) = (q_k, X_l, D_m)$$

$X_j \rightarrow$ j-te Zeichen im Alphabet

$D_m \rightarrow$ m-te Bewegung

wird codiert als

$$0^i 1 0^j 1 0^k 1 0^l 1 0^m \mid i, j, k, l, m \geq 1$$

Sei `code(t)` die Kodierung des `t`-ten Übergangs. Die Kodierung der gesamten TM ist dann

$$< M > = \texttt{code(1)}11\texttt{code(2)}11 \cdots \texttt{code(s)}111$$

Die universelle TM $\mathcal{U}$ erhält als Eingabe ein Wort $< M >< w >$ und simuliert $\mathcal{M}$ auf der Eingabe w. Außerdem übernimmt $\mathcal{U}$ auch das Akzeptanzverhalten von $\mathcal{M}$.

Simulation mit einer 3-Band-TM

Im Folgenden werden die Schritte einer Simulation punktuell aufgelistet.

- Beschreibung der Bänder:
  - Band 1: Auf Band 1 steht das, was $\mathcal{M}$ auf seinem Band stehen hätte.
  - Band 2: Auf Band 2 steht die Beschreibung $< M >$.
  - Band 3: Auf Band 3 steht der Zustand, den $\mathcal{M}$ gerade hätte.
- Initialisierung:
  - Man überprüft, ob $< M >$ eine gültige Kodierung einer TM darstellt.
  - Man schreibt $< M >$ auf Band 2.
  - Man schreibt die Kodierung des Anfangszustandes q_1 auf Band 3.
- Rechenschritt: Die Simulation beginnt mit dem SLK auf dem ersten Zeichen von w auf Band 1.
  - Man sucht auf Band 2 den Übergang des Zeichens, das zu dem Zeichen unter dem SLK auf Band 1 und zum Zustand auf Band 3 passt.
  - Man aktualisiert den Bandinhalt entsprechend auf Band 1.
  - Man ändert den Zustand entsprechend auf Band 3.

Unter der Annahme, dass $< M >$ konstant groß ist, kann ein Schritt von $\mathcal{M}$ in konstanter Zeit von $\mathcal{U}$ simuliert werden.
Die universelle 3-Band-TM kann mittels einer 1-Band-TM simuliert werden, was zur Folge hätte, dass ein Schritt nicht mehr in konstanter Zeit ablaufen würde (quadratischer Overhead). Mit einigen Tricks (Siehe Skript?) kann aber auch der entstehende quadratische Overhead quasi vermieden werden.

Jede TM $\mathcal{M}$ kann auf $\mathcal{U}$ simuliert werden. $< M >$ entspricht sozusagen einem *Programm*.

Über ein anderes Rechenmodell, die **Registermaschine**, soll sich im Skript? informiert werden. Wichtig ist insbesondere der Punkt der Äquivalenz TM $\Leftrightarrow$ Registermaschine.

Church-Turing-These

Ohne Beweis: Die Klasse der Probleme, die *intuitiv berechenbar* sind, ist äquivalent mit der Klasse der Probleme, die von einer TM berechenbar sind.

Unentscheidbarkeit

Es soll nun gezeigt werden, dass es zu viele Sprachen gibt, als dass es für jede dieser Sprachen ein TM geben könnte, die sie entscheidet.

Zur Erinnerung: Eine TM $\mathcal{M}$ entscheidet eine Sprache $L \subseteq \Sigma^*$, falls $\mathcal{M}$ auf jeder Eingabe $w \in \Sigma^*$ hält und genau dann akzeptiert, wenn $w \in L$ und verwirft wenn $w \notin L$.

Abzählbare Menge: Eine Menge heißt abzählbar, falls es eine surjektive Funktion $C : N \to H$ gibt. Nicht abzählbare Mengen heißen *überabzählbar*.

Im Falle einer abzählbar unendlichen Menge gibt es immer auch eine bijektive Abbildung $C : \mathbb{N} \to H$, da Wiederholungen übersprungen werden können. So eine Abbildung kann auch als Nummerierung der Menge H interpretiert werden.

$\Rightarrow$ Die Menge der ganzen Zahlen $\mathbb{Z}$ hat dieselbe Mächtigkeit wie $\mathbb{N}$ (abzählbar unendlich), da

$$c(i) = \begin{cases} \frac{i}{2} & \text{falls } i \text{ gerade} \\ -\frac{i+1}{2} & \text{falls } i \text{ ungerade} \end{cases}$$

eine bijektive Funktion $C : \mathbb{N} \to \mathbb{Z}$ ist.

$\Rightarrow$ Die Menge aller Wörter über $\{0,1\}^*$

$$\{\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, \cdots\}$$

ist ebenfalls überabzählbar unendlich (*Binärzahlen ausgedrückt durch w sind problematisch:* $001 \Leftrightarrow 1$).

$\Rightarrow$ Die Menge der TMs ist abzählbar (z.B. indem man $< M >$ als Binärzahl interpretiert mit dem signifikantesten Bit an letzter Stelle).

Satz: Die Potenzmenge $\mathcal{P}(\mathbb{N})$ ist überabzählbar.

Beweis durch Widerspruch: Angenommen, $\mathcal{P}(\mathbb{N})$ ist abzählbar. Das würde bedeuten, dass eine Funktion $C : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ existiert.
Sei S_i nun die i-te Menge in $\mathcal{P}(\mathbb{N})$ und sei die Matrix $(A_{ij})_{i,j \in \mathbb{N}}$ definiert mit

$$A_{ij} = \begin{cases} 1 & \text{falls } j \in S_i \\ 0 & \text{sonst} \end{cases}$$

A ist also zum Beispiel (wenn $S_0 = \{0, 1, 4, \cdots\}$ und $S_1 = \{1, 2, 3, \cdots\}$)

i \ S	0	1	2	3	4	$\cdots$
S_0	1	1	0	0	1	$\cdots$
S_1	0	1	1	1	0	$\cdots$
S_2						$\cdots$
S_3						$\cdots$

Sei nun eine spezielle Teilmenge $S_{diagonal}$ definiert mit

$$S_{diagonal} = \{i \in \mathbb{N} \mid A_{i,i} = 1\}$$

Das Komplement $\overline{S_{diagonal}}$ ist dann

$$\overline{S_{diagonal}} = \{i \in \mathbb{N} \mid A_{i,i} = 0\}$$

In der Nummerierung von $\mathcal{P}(\mathbb{N})$ sei $\overline{S_{diagonal}}$ die k-te Menge, also

$$\overline{S_{diagonal}} = S_k$$

Es gilt nun zwei Fälle zu unterscheiden:

1. Falls $A_{k,k} = 1$, dann muss $k \in S_k$. Aber wegen $S_k = \overline{S_{diagonal}}$ gilt $k \notin S_k$.
2. Falls $A_{k,k} = 0$, dann muss $k \notin S_k$. Aber wegen $S_k = \overline{S_{diagonal}}$ gilt $k \in S_k$.

$\Rightarrow$ $\mathcal{P}(\mathbb{N})$ ist nicht abzählbar. $\square$

Korollar: Die Menge der Sprachen über $\{0,1\}^*$ ist überabzählbar (die Menge der Sprachen entspricht hier der Potenzmenge von $\{0,1\}$). Das heißt, es gibt **echt** mehr Sprachen als TMs.