Komplexitätstheorie

Gelesen von Prof. Dr. Rolf Wanka
an der FAU Erlangen

Neu gesetzt im Sommersemester 2024

2. Mai 2024

Inhaltsverzeichnis

Die vorläufige URL unter der die neuste Version von diesem Dokument gefunden werden kann, sollte https://wwwcip.cs.fau.de/~oj14ozun/kt.pdf sein.

Die offizielle Webseite findet sich auf der Webseite des Informatik Lehrstuhls *Hardware-Software-Co-Design*, https://www.cs12.tf.fau.de/lehre/lehrveranstaltungen/vorlesungen/komplexitaetsthorie/

KAPITEL 1

Einleitung

TODO

KAPITEL 2

Turingmaschinen, Komplexitätsklassen und universelle Turingmaschinen

TODO

Definition 2.1. Eine *Gödelisierung* einer 1-band Turingmanschine M besteht aus Wörtern $w_{i,j,\ell,m}$ für jede Regel $\delta(q_i, a_j) = (q_k, a_\ell, d_m)$ der Übergangsfunktion δ von M. Dabei repräsentieren wir $w_{i,j,\ell,m}$ durch

$$\mathrm{bin}(i)\,\texttt{\#}\,\mathrm{bin}(j)\,\texttt{\#}\,\mathrm{bin}(k)\,\texttt{\#}\,\mathrm{bin}(\ell)\,\texttt{\#}\,\mathrm{bin}(m).$$

Die verschiedenen $w_{i,j,\ell,m}$ sind durch `##` getrennt. Ende der *Gödelnummer*: `###`. Die TM mit Gödelnummer u hießt M_u. Die Gödelisürung von M hießt $G(M)$.

Definition 2.2. Eine 1-Band-TM M_0 heißt *universelle Turingmaschine*, falls gilt

$$f_{M_0}(x) = \begin{cases} f_{M_0}(v) & x = u\,\texttt{\#}\,v,\ u \text{ ist Gödelnummer} \\ \text{undef.} & \textit{sonst} \end{cases}$$

M_0 gestartet mit $u\,\texttt{\#}\,v$ hält genau dann, wenn M_u gestartet mit v hällt.

Satz 2.1. Es gibt eine universelle 1-Band-TM M_0 mit:

$$T_{M_0}(u\,\texttt{\#}\,v) = O(T_{M_O}(v))$$

und

$$S_{M_0}(u\,\texttt{\#}\,v) = O(S_{M_u}(v))$$

u wird als konstant lang angesehen.

Satz 2.2. Sei $s : \mathbb{N} \to \mathbb{N}$ berechenbar. Dann ist

$$H^{S(n)} := \{u\,\texttt{\#}\,v \mid M_u \text{ gestartet mit } v \text{ hält und benutzt höchstens } s(|v|) \text{ Zellen}\}$$

entscheidbar.

Lemma 2.1. Falls M eine $s(n)$-bandbeschränkte 1-Band-TM ist und gestartet mit x echt mehr als $|Q| \cdot s(|x|) \cdot |\Gamma|^{s(|x|)}$ Schritte macht, so hällt M gestartet mit x nicht.

Beweis. $|w_1 w_2| \le s(|x|)$. D.h.

- Es gibt höchstens $|\Gamma|^{s(|x|)}$ viele verscheide mögliche Bandinhalte.
- Der Kopf kann an $s(|x|)$ vielen Stellen vorkommen.
- Je Kopfposition höchstens $|Q|$ Zustände.

  $|\Gamma|^{s(|x|)} \cdot s(|x|) \cdot |Q|$

ist die Maximalzahl an Konfigurationen. ■

Beweis von Satz 2.2. $H^{s(n)}$ wird folgendermaßen entschieden:

- Teste ob $x = u\,\texttt{\#}\,v$ ist, u Gödelnummer einer TM M_u. Falls nein, verwerfe x und stop.
- Berechne $n \coloneqq |v|$.
- Berechne $s(n)$. (Geht, da $s(n)$ berechenbar ist nach Voraussetzung)
- Berechne $p = |Q| \cdot s(n) \cdot |\Gamma|^{s(n)}$
- Benutze die universelle TM zur Simulation von M_u gestartet mit v. Benutze Zähler, der von p in jedem Schritt eine 1 abzieht.
- Verwerfe, falls M_u mit Eingabe v mehr als $s(n)$ Speicherplatz benutzt oder mehr als p Schritte macht. Sonst akzeptieren.

■

KAPITEL 3

Eine untere Schranke für 1-Band-TM

$$L := \left\{ w\,\#^{|w|}\,w \mid w \in \{0,1\}^* \right\}$$

Beispiel `010###010` $\in L$.

Satz 3.1. Für L gilt:

1. $L \in \mathrm{DTIME}_1(n^n)$
2. $L \in \mathrm{DTIME}_2(n)$
3. $L \notin \mathrm{DTIME}_1(t(n))$ für alle $t(n) = o\left(n^n\right)$

Beweis. Item 1 und Item 2 gilt trivial.

Zu Item 3: Sei M eine 1-Band-TM mit Zustandsmenge Q. Die Eingabe für M stehe zu Beginn in den Zellen $0, 1, \ldots, n-1$. Am Ende stehe der Kopf von M auf Zelle 0.

Definition 3.1. Sei x eine Eingabe für M, i die Nummer einer Zelle. Die *Crossing-Sequenz* $\mathrm{CS}(x, i)$ auf Zelle i für Eingabe x ist die Folge der Zustände, die bei der Rechnung von M gestartet mit x jeweils direkt nach Kopfbewegungen von Zelle $i-1$ nach i oder umgekehrt auftreten.

Lemma 3.1. Seien $u, v, w, y \in \{0, 1, \#\}^*$ so gewählt, daß $\mathrm{CS}(uv, |u|) = \mathrm{CS}(wy, |w|)$ ist. Dann gilt

$$uv \in L \iff uy \in L.$$

Beweis. Es reicht, $uv \in L \implies wy \in L$ zu zeigen. ∎

∎

Wir haben eine feste Form, TM aufzuschreiben. Wort $w \in 0, 1^*$ kann beschreiben werden durch $G(M)z$, so daß M gestartet mit z das Wort w ausgibt.

Definition 3.2. Für $w \in 0, 1^*$ bezeichnet $K(w) := \min\{|G(M)z| \mid M \text{ gestartet mit } z \text{ berechnet } w\}$. die *Kolmogorov-Komplexität* von w.

Lemma 3.2. Für jedes $m \in \mathbb{N}$ gibt es ein $w \in \{0,1\}^m$ mit $K(w) \geq m$.

Beweis. Sonst wäre die Komplexität $K(w) < m$ für alle $w \in 0,1^m$. Dann würde es für jedes $w \in \{0,1\}^m$ ein $u = G(M)z$, $|u| < m$, so daß M gestartet mit z die Ausgabe w berechnet. Da zu verschiedenen w auch verschiedene $G(M)z \in 0,1^*$ gehören, wäre

$$2^m - 1 = \sum_{i=0}^{m-1} 2^i = |u \in 0,1^* \mid |u| \lneq m \geq |0,1^*| = 2^m \qquad \lightning$$

∎

Lemma 3.3. Wir nehmen $M = (Q, \Sigma, \Gamma, \delta, q_0, F)$ sei 1-Band-TM die L entscheidet. Sei $m \in \mathbb{N}$ fest. Sei $\hat{w} \in 0,1^m$ so, daß $K(\hat{w}) \geq m$ ist (Wegen lemma 3.2 gibt es $\hat{w}$; $\hat{w}$ hießt *Kolmogorov-zufällig*). Dann hat bezüglich M für jedes $i \in m, \dots, 2m-1$ die Crossing-Sequenz $CS(\hat{w}\,\#^m\,\hat{w}, i)$ die Länge $\Omega(m)$.

Beweis. Sei $M = (Q, \Sigma, \Gamma, \delta, q_0, F)$ sei die 1-Band-TM, die $L = \{w\,\#^{|w|}\,w | w \in 0,1^*\}$ entscheidet. Sei $m \in \mathbb{N}$ fest. Sei $w \in 0,1^m$. Ist auch nur eine Crossing-Sequenz $CS(w\,\#^m\,w, i)$ kurz, so ist $K(w)$ klein. Wir rekonstruieren aus Crossing-Sequenzen die Eingabe $w\,\#^m\,w$ für m. Für Kolmogorov-zufälliges $\hat{w}$ erhalten wir somit lange Crossing-Sequenzen:

Die TM $\tilde{M}$ bekommt die Eingabe $z \in 0,1^*$, die als Binärkodierung einer Folge $q_1, \dots, q_\ell$ von Zuständen von M interpretiert wird. Gestartet mit $q_1, \dots, q_\ell$ arbeitet $\tilde{M}$ folgendermaßen:

> $\tilde{M}$ zählt nacheinander alle $w \in 0,1^*$ auf. Für jedes solche w startet sie M mit $w\,\#^{|w|}\,w$. $\tilde{M}$ notiert dabei die Crossing-Sequenz $\mathrm{CS}(w\,\#^{|w|}\,w, i)$ für $i \in m, \dots, 2m-1$. Falls eine davon mit $q_\ell, \dots, q_\ell$ übereinstimmt, gibt $\tilde{M}w$ aus (da sie auh $w\,\#^{|w|}\,w$ "gefunden" hat) und stoppt.

1. $|z| \leq \lfloor \log(|Q|) + 1 \rfloor \cdot \ell$
2. $|G(\tilde{M}) = \mathcal{O}(1)$
3. Für jedes $w \in 0,1^m$ gilt: $\tilde{M}$ gestartet mit $q_1, \dots, q_\ell = \mathrm{CS}(w\,\#^m\,w, i)$ für irgendein $i \in m, \dots, 2m-1$ gibt w aus.

Sei

$$\ell(w) = \min_{m \leq i \leq 2m-1} |\mathrm{CS}(w\,\#^m\,w, i)|,$$

dann folgt aus den Ausführungen

$$K(w) = O(|G(\tilde{M})| + \ell(w)) = \mathcal{O}(1 + \ell(w))$$

Für Kolmogorov-zufällig gilt: $m \leq K(\hat{w}) = \mathcal{O}(1 + \ell(\hat{w}))$, d.h. $\ell(\hat{w}) = \Omega(m)$. ∎

Daraus folgt, m "#" ergeben Laufzeit von mindestens $\Omega(n^2)$.

Index