Grundlagen der diskreten Komplexitätstheorie I

Turingmaschinen, Asymptotik und Komplexitätsklassen

Markus Schwagenscheidt

02.05.2011

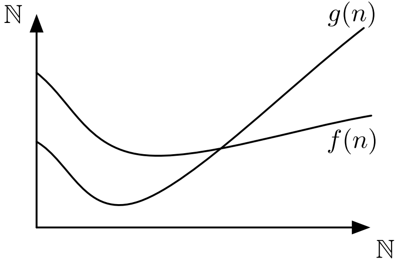
1. Berechenbarkeitstheorie
   - $\mathcal{O}$-Notation
   - Deterministische Turingmaschinen
   - Berechnungsablauf einer DTM
   - Erweiterungen der DTM
   - Nichtdeterministische Turingmaschinen
   - Berechenbare Funktionen und entscheidbare Sprachen
   - Universelle Turingmaschinen

2. Komplexitätstheorie
   - Zeit- und Platzkomplexitätsklassen
   - Komplexität von 1-Band-DTM vs. k-Band-DTM
   - Linear Speedup
   - Die Klassen P, NP und EXP
   - Wichtige Platzkomplexitätsklassen

$\mathcal{O}$-Notation

Seien $f, g : \mathbb{N} \to \mathbb{N}$ Funktionen. Wir schreiben:

$$
\begin{aligned}
f(n) = \mathcal{O}(g(n)) \quad &\Leftrightarrow \quad \exists c, N\ \forall n \geq N : \ f(n) \leq cg(n). \\
f(n) = \Omega(g(n)) \quad &\Leftrightarrow \quad g(n) = \mathcal{O}(f(n)) \\
&\Leftrightarrow \quad \exists c, N\ \forall n \geq N : \ f(n) \geq (1/c)g(n). \\
f(n) = \Theta(g(n)) \quad &\Leftrightarrow \quad f(n) = \mathcal{O}(g(n)) \ \wedge \ f(n) = \Omega(g(n)).
\end{aligned}
$$

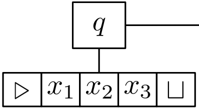


Deterministische Turingmaschinen

Definition

Eine *deterministische Turingmaschine* (DTM) ist ein Viertupel $M = (Q, \Sigma, \Gamma, \delta)$, bestehend aus

- einer endlichen *Zustandsmenge* Q, wobei Q den Startzustand s enthält,
- einem endlichen *Eingabealphabet* Σ, wobei Σ die Symbole $\sqcup, \triangleright$ nicht enthält,
- einem endlichen *Bandalphabet* Γ, wobei Γ die Symbole $\sqcup, \triangleright$ enthält und $\Sigma \subseteq \Gamma$ gilt,
- einer *Übergangsfunktion* $\delta : Q \times \Gamma \to (Q \cup \{h, q_{accept}, q_{reject}\}) \times \Gamma \times \{L, R, N\}$.

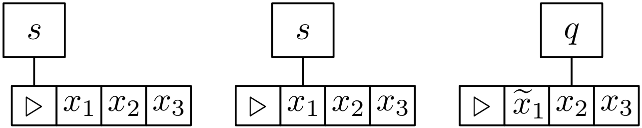


$q \in Q$	$x \in \Gamma$	$\delta(q, x)$
s	$\triangleright$	$(s, \triangleright, R)$
s	$\sqcup$	$(s, 1, R)$
s	0	$(q, 1, L)$
...	...	...

Berechnungsablauf einer DTM bei Eingabe $x \in \Sigma^*$

Informelle Beschreibung der Rechnung:

- Zu Beginn steht auf dem Band der String $\triangleright x$ und der Kopf befindet sich auf der ersten Zelle im Zustand s.
- Kopfbewegungen gemäß δ.
- Berechnung endet, falls einer der *Haltezustände* $h, q_{accept}, q_{reject}$ erreicht wird, oder die Berechnung terminiert nicht (Endlosschleife).



- Der Kopf darf nicht über das linke Ende hinauslaufen.
- Nach rechts ist das Band unbeschränkt und mit $\sqcup$s beschrieben.

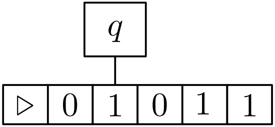
Konfigurationen

Formale Beschreibung der Rechnung durch Konfigurationen.

Definition

Eine *Konfiguration* von M ist ein Tripel $(q, u, w) \in Q \times \Gamma^* \times \Gamma^*$ mit folgenden Bedeutungen:

- q ist der aktuelle Zustand von M.
- u ist der String links des Kopfes. Der Kopf steht auf der letzten Zelle von u.
- w ist der String rechts des Kopfes ist. w kann das leere Wort ε sein.



$(q, \triangleright 01, 011)$

Konfigurationen

Für zwei Konfigurationen $(q, u, w), (q', u', w')$ schreiben wir:

- $(q, u, w) \rightarrow (q', u', w')$, falls (q', u', w') durch einmalige Anwendung von δ aus der Konfiguration (q, u, w) erreicht werden kann.
- $(q, u, w) \rightarrow^k (q', u', w')$, falls (q', u', w') durch k-malige Anwendung von δ aus (q, u, w) erreicht werden kann.
- $(q, u, w) \rightarrow^* (q', u', w')$, falls es ein $k \in \mathbb{N}$ gibt mit $(q, u, w) \rightarrow^k (q', u', w')$.

Der Berechnungsablauf einer DTM M bei Eingabe $x \in \Sigma^*$ wird nun formal beschrieben durch Folge von Konfigurationen

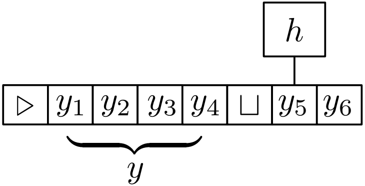
$$(s, \rhd, x) \rightarrow (q, u, w) \rightarrow \cdots \rightarrow (q', u', w').$$

M hält, falls es $u, w \in \Gamma^*$ und $q \in \{h, q_{accept}, q_{reject}\}$ gibt mit

$$(s, \rhd, x) \rightarrow^* (q, u, w).$$

Ausgabe einer DTM bei Eingabe $x \in \Sigma^*$

- Eine DTM M *akzeptiert* (bzw. *verwift*) die Eingabe $x \in \Sigma^*$, falls M im Zustand q_{accept} (bzw. q_{reject}) hält. Wir schreiben $M(x) = Yes$ (bzw. $M(x) = No$).
- Hält die DTM M bei Eingabe $x \in \Sigma^*$ im Zustand h, so betrachten wir den längsten, am weitesten links stehenden String y, der nicht mit einem $\sqcup$ endet, als *Ausgabe* von M. Wir schreiben $M(x) = y$.

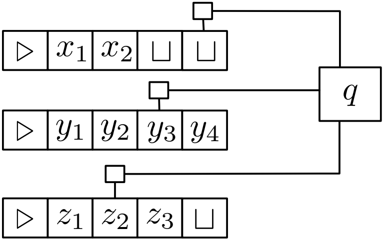


Mehrband-DTM

Definition

Eine deterministische *k-Band-Turingmaschine* ist eine DTM mit Übergangsfunktion

$$\delta : Q \times \Gamma^k \to (Q \cup \{h, q_{accept}, q_{reject}\}) \times (\Gamma \times \{L, R, N\})^k$$



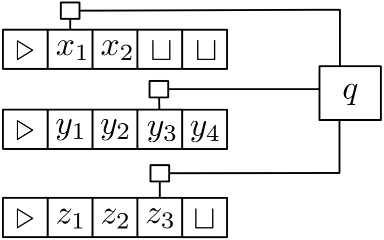
Konfigurationen haben die Form $(q, u_1, w_1, \ldots, u_k, w_k)$.

DTM mit Eingabe- und Ausgabeband

Definition

Eine *DTM mit Eingabe und Ausgabe* ist eine k-Band-DTM ($k \geq 3$), so dass gilt:

- Das erste Band (*Eingabeband*) darf nur gelesen werden.
- Die Bänder 2 bis $k-1$ (*Arbeitsbänder*) können wie üblich genutzt werden.
- Der Kopf des k-ten Bandes (*Ausgabeband*) darf sich nicht nach links bewegen.



Nichtdeterministische Turingmaschinen

Definition

Eine *nichtdetermistische Turingmaschine* (NTM) ist ein Viertupel $N = (Q, \Sigma, \Gamma, \delta)$, bestehend aus

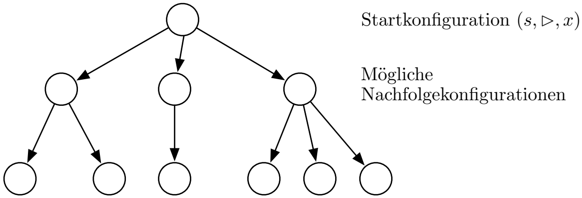
- endlichen Mengen Q, Σ, Γ wie bei einer DTM und
- einer *Übergangsrelation*
  $$\delta \subseteq (Q \times \Gamma) \times \Big((Q \cup \{h, q_{accept}, q_{reject}\}) \times \Gamma \times \{L, R, N\}\Big).$$

Es ist jede DTM auch eine NTM. Die DMTs sind genau diejenigen NTMs, deren Übergangsrelation eine Funktion ist.

Man kann Mehrband-NTMs und NTMs mit Eingabe/Ausgabe wie für DTMs definieren.

Rechnung und Ausgabe einer NTM

- Eine NTM N *akzeptiert* die Eingabe $x \in \Sigma^*$, falls N einen Berechnungspfad hat, der im Zustand q_{accept} hält. Wir schreiben $N(x) = Yes$.
- Eine NTM N *verwirft* die Eingabe $x \in \Sigma^*$, falls N auf jedem Berechnungspfad im Zustand q_{reject} hält. Wir schreiben $N(x) = No$.
- Hält die NTM N bei Eingabe $x \in \Sigma^*$ im Zustand h, so betrachten wir den längsten, am weitesten links stehenden String y, der nicht mit einem $\sqcup$ endet, als *Ausgabe* von M. Die Ausgabe ist nicht eindeutig.

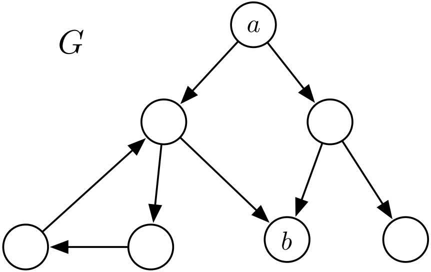


REACHABILITY: DTM und NTM Algorithmen

Gegeben ein Graph $G = (V, E)$ mit $|V| = n$ und zwei Knoten $a, b \in V$. Gibt es Pfad von a nach b?

- DTM: Breitensuche / Tiefensuche.
- NTM: Wiederhole höchstens n-mal oder bis Sackgasse:
  - Wähle Nachfolger v von a.
  - Ist $v = b$ akzeptiere. Sonst suche Weg von v nach b.

  Sind n Schritte verbraucht, verwerfe.



- Sei $L \subseteq \Sigma^*$. Eine (partielle) Funktion $f : L \to \Sigma^*$ heißt *berechenbar*, falls es eine DTM M gibt, die f berechnet. Das bedeutet, dass M für jede Eingabe $x \in L$ im Zustand h hält und $f(x)$ ausgibt, und für Eingaben $x \notin L$ nicht hält.
- Eine Sprache $L \subseteq \Sigma^*$ heißt *semi-entscheidbar* oder *rekursiv aufzählbar*, falls es eine DTM M gibt, die jedes $w \in L$ akzeptiert und jedes $w \notin L$ nicht akzeptiert.
- Eine Sprache $L \subseteq \Sigma^*$ heißt *entscheidbar*, falls es eine DTM M gibt, die jedes $w \in L$ akzeptiert und jedes $w \notin L$ verwirft.

Zusammenhänge

- Jede entscheidbare Sprache ist auch semi-entscheidbar.
- Eine Sprache L ist genau dann entscheidbar, wenn ihre charakteristische Funktion

$$\chi_L(x) = \begin{cases} 1, & \text{falls } x \in L \\ 0, & \text{falls } x \notin L \end{cases}$$

  berechenbar ist.
- Es existieren nicht-berechenbare Funktionen sowie nicht-(semi-)entscheidbare Sprachen (z.B. Halteproblem).
- Churchsche These: *Eine Funktion ist genau dann intuitiv berechenbar, wenn sie durch eine Turingmaschine berechenbar ist.*

Die Menge $\mathcal{M}$ aller Turingmaschinen ist abzählbar. Es gibt eine *Gödelisierung* von $\mathcal{M}$, also eine Abbildung

$$\langle\cdot\rangle : \mathcal{M} \to \mathbb{N}, M \mapsto \langle M \rangle,$$

wobei gilt:

- $\langle\cdot\rangle$ ist injektiv und berechenbar.
- Es gibt eine berechenbare Funktion $?\langle\cdot\rangle$, die für jede $n \in \mathbb{N}$ prüft, ob $n \in \text{image}(\langle\cdot\rangle)$ gilt.
- Die Umkehrfunktion $\langle\cdot\rangle^{-1} : \text{image}(\langle\cdot\rangle)$ ist berechenbar.

Definition

Eine *universelle Turingmaschine* U ist eine DTM, die als Eingabe die Kodierung $\langle M \rangle$ einer DTM M zusammen mit der Kodierung $\langle x \rangle$ einer Eingabe $x \in \Sigma^*$ erhält, und die Berechnung von M bei Eingabe von x simuliert. Es gilt also $U(\langle M \rangle; \langle x \rangle) = M(x)$.

1. Berechenbarkeitstheorie
   - $\mathcal{O}$-Notation
   - Deterministische Turingmaschinen
   - Berechnungsablauf einer DTM
   - Erweiterungen der DTM
   - Nichtdeterministische Turingmaschinen
   - Berechenbare Funktionen und entscheidbare Sprachen
   - Universelle Turingmaschinen
2. Komplexitätstheorie
   - Zeit- und Platzkomplexitätsklassen
   - Komplexität von 1-Band-DTM vs. k-Band-DTM
   - Linear Speedup
   - Die Klassen P, NP und EXP
   - Wichtige Platzkomplexitätsklassen

Zeit- und Platzbedarf von DTM und NTM

Sei M eine DTM mit Eingabe/Ausgabe. Wir definieren:

- M ist $f(n)$-*zeitbeschränkt*, wenn M für jedes $n \in \mathbb{N}$ und jede Eingabe $x \in \Sigma^*$ mit $|x| \leq n$ nach höchstens $f(n)$ Schritten hält.
- M ist $f(n)$-*platzbeschränkt*, wenn M für jedes $n \in \mathbb{N}$ und jede Eingabe $x \in \Sigma^*$ mit $|x| \leq n$ höchstens $f(n)$ Bandzellen auf den Arbeitsbändern benutzt. Die benutzten Zellen auf Eingabe- und Ausgabeband werden also nicht mitgezählt.

Sei N eine NTM. Wir definieren:

- N ist $f(n)$-*zeitbeschränkt*, wenn N für jedes $n \in \mathbb{N}$ und jede Eingabe $x \in \Sigma^*$ mit $|x| \leq n$ auf jedem Berechnungspfad nach höchstens $f(n)$-Schritten hält. Das heißt, N hat keinen Berechnungspfad, der länger als $f(n)$ ist.
- N ist $f(n)$-*platzbeschränkt*, wenn N für jedes $n \in \mathbb{N}$ und jede Eingabe $x \in \Sigma^*$ mit $|x| \leq n$ auf jedem Berechnungspfad höchstens $f(n)$ Bandzellen auf den Arbeitsbändern benutzt.

Sei $f : \mathbb{N} \to \mathbb{N}$ eine monoton wachsende Funktion. Wir definieren:

$$DTIME(f(n)) := \left\{ L \subseteq \Sigma^* : \begin{array}{c} L \text{ wird von einer } \mathcal{O}(f(n))\text{-zeit-} \\ \text{beschränkten DTM entschieden} \end{array} \right\}$$

$$DSPACE(f(n)) := \left\{ L \subseteq \Sigma^* : \begin{array}{c} L \text{ wird von einer } \mathcal{O}(f(n))\text{-platz-} \\ \text{beschränkten DTM entschieden} \end{array} \right\}$$

Die Klassen $NTIME(f(n))$ und $NSPACE(f(n))$ für nichtdeterministische Turingmaschinen sind analog definiert.

Komplexität von 1-Band-DTM vs. k-Band-DTM

Vergleich der Zeitkomplexität

Wird $L \subseteq \Sigma^*$ von einer $f(n)$-zeitbeschränkten k-Band-DTM M entschieden, so gibt es auch eine $\mathcal{O}(f(n)^2)$-zeitbeschränkte 1-Band-DTM $\widetilde{M}$, die L entscheidet.

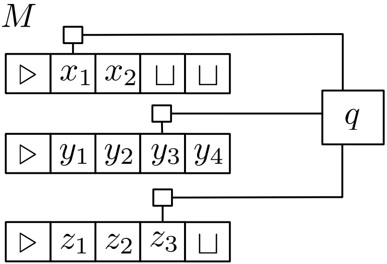
Vergleich der Platzkomplexität

Wird $L \subseteq \Sigma^*$ von einer $f(n)$-platzbeschränkten k-Band-DTM entschieden, so gibt es auch eine $\mathcal{O}(f(n))$-platzbeschränkte 1-Band-DTM, die L entscheidet.

Der Einsatz einer k-Band DTM verbessert die Effizienz also nicht wesentlich, da wir polynomielle Effizienzunterschiede als gering betrachten.

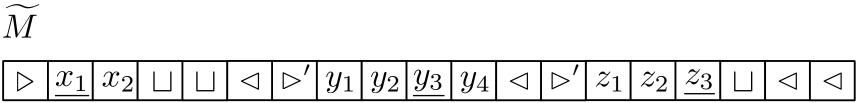
Beweis:

$\widetilde{M} = (\widetilde{Q}, \Sigma, \widetilde{\Gamma}, \widetilde{\delta})$ speichert die Einträge der k Bänder von M nacheinander. Setze $\widetilde{\Gamma} := \Gamma \cup \underline{\Gamma} \cup \{\triangleright', \triangleleft, \triangleleft'\}$.



Pro Schritt von M :

Kopfpositionen scannen	$\approx 2f(n)$
Kopfbewegungen simulieren	$\approx 2f(n) + 2k$
Rechts-Shift	$\approx 3kf(n)$



Linear Speedup Theorem

Ist $L \subseteq \Sigma^*$ eine Sprache, die von einer $f(n)$-zeitbeschränkten DTM M entschieden wird, so gibt es zu jedem $\varepsilon > 0$ eine $(\varepsilon f(n) + n + 2)$-zeitbeschränkte DTM $\widetilde{M}$, die L entscheidet.

Beweis

Die DTM M entscheide L in Zeit $f(n)$. Wir konstruieren DTM $\widetilde{M}$:

- Sei $m = \lceil \frac{6}{\varepsilon} \rceil$. Fasse je m Symbole auf dem ersten Band zu einem Symbol zusammen und schreibe es auf das zweite Band.

$\triangleright$	x_1	x_2	x_3	x_4	x_5	x_6	x_7	Eingabeband

$\triangleright$	(x_1, x_2, x_3)	(x_4, x_5, x_6)	$(x_7, \sqcup, \sqcup)$

- Simuliere m Schritte von M mit höchstens 6 Schritten:
  - Scanne linkes und rechtes Feld (4 Schritte), um die nächsten m Schritte vorherzusagen.
  - Schreibe aktuelles Feld und linkes oder rechtes Feld (2 Schritte).

$\widetilde{M}$ braucht maximal $6\lceil \frac{f(n)}{m} \rceil + n + 2 \leq \varepsilon f(n) + n + 2$ Schritte.

Die Zeitkomplexitätsklassen P, NP und EXP

Wir definieren:

$$P := \bigcup_{k \in \mathbb{N}} DTIME(n^k)$$

$$NP := \bigcup_{k \in \mathbb{N}} NTIME(n^k)$$

$$EXP := \bigcup_{k \in \mathbb{N}} DTIME(2^{n^k})$$

Zusammenhänge

Da jede DTM auch eine NTM ist, folgt:

$$P \subseteq NP.$$

Man kann außerdem zeigen: *Jede Sprache, die von einer $f(n)$-zeitbeschränkten NTM entschieden wird, wird auch von einer $\mathcal{O}(2^{f(n)})$-zeitbeschränkten 3-Band-DTM entschieden.* Daraus folgt

$$P \subseteq NP \subseteq EXP.$$

Es existiert eine Sprache, die in EXP liegt, aber nicht in P. Damit muss eine der obigen Inklusionen echt sein. Welche es ist, ist ebenso ungeklärt wie die berühmte Frage

$$P \stackrel{?}{=} NP.$$

Dies ist eines der sog. *Milleniumsprobleme*, auf deren Lösung ein Preisgeld von 1.000.000 Dollar ausgesetzt ist.

Wichtige Platzkomplexitätsklassen

Wir definieren:

$$PSPACE := \bigcup_{k \in \mathbb{N}} DSPACE(n^k)$$
$$NPSPACE := \bigcup_{k \in \mathbb{N}} NSPACE(n^k)$$
$$L := DSPACE(\log(n))$$
$$NL := NSPACE(\log(n))$$

Es gilt

$$L \subseteq NL \subseteq P \subseteq NP \subseteq PSPACE \subseteq NPSPACE \subseteq EXP.$$

Nach dem Satz von Savitch gilt außerdem

$$PSPACE = NPSPACE.$$