

Vorlesungsskript
Komplexitätstheorie

Wintersemester 2008/09

Prof. Dr. Johannes Köbler
Humboldt-Universität zu Berlin
Lehrstuhl Komplexität und Kryptografie

24. Oktober 2008

Inhaltsverzeichnis

1	Einführung	1
2	Rechenmodelle	3
2.1	Deterministische Turingmaschinen	3
2.2	Nichtdeterministische Berechnungen	4
2.3	Zeitkomplexität	5
2.4	Platzkomplexität	5
3	Grundlegende Beziehungen	7
3.1	Robustheit von Komplexitätsklassen	7

1 Einführung

In der Komplexitätstheorie werden algorithmische Probleme daraufhin untersucht, welche Rechenressourcen zu ihrer Lösung benötigt werden. Naturgemäß bestehen daher enge Querbezüge zu

- Algorithmen (obere Schranken)
- Automatentheorie (Rechenmodelle)
- Berechenbarkeit (Was ist überhaupt algorithmisch lösbar?)
- Logik (liefert viele algorithmische Probleme, mit ihrer Hilfe kann auch die Komplexität von Problemen charakterisiert werden)
- Kryptographie (Wieviel Rechenressourcen benötigt ein Gegner, um ein Kryptosystem zu brechen?)

Zur weiteren Motivation betrachten wir eine Reihe von konkreten algorithmischen Problemstellungen.

Erreichbarkeitsproblem in Graphen (REACH):

Gegeben: Ein gerichteter Graph $G = (V, E)$ mit $V = \{1, \dots, n\}$ und $E \subseteq V \times V$.

Gefragt: Gibt es in G einen Weg von Knoten 1 zu Knoten n ?

Zur Erinnerung: Eine Folge $(v_1, \dots, v_k)$ von Knoten heißt **Weg** in G , falls für $j = 1, \dots, k-1$ gilt: $(v_j, v_{j+1}) \in E$.

Da als Antwort nur “ja” oder “nein” möglich ist, handelt es sich um ein **Entscheidungsproblem**. Ein solches lässt sich formal durch eine Sprache beschreiben, die alle positiven (mit “ja” zu beantwortenden) Problemeingaben enthält:

$$\text{REACH} = \{G \mid \text{in } G \text{ ex. ein Weg von 1 nach } n\}.$$

Hierbei setzen wir eine Kodierung von Graphen durch Wörter über einem geeigneten Alphabet Σ voraus. Wir können G beispielsweise durch eine Binärfolge der Länge n^2 kodieren, die aus den n Zeilen der Adjazenzmatrix von G gebildet wird.

Wir entscheiden REACH durch einen Wegsuche-Algorithmus. D.h. wir markieren nach und nach alle Knoten, die vom Knoten 1 aus erreichbar sind. Dabei speichern wir alle markierten Knoten solange in einer Menge S bis auch ihre Nachbarknoten markiert sind. Genauer ist folgendem Algorithmus zu entnehmen:

Algorithmus suche-Weg(G)

```

1  Input: Gerichteter Graph  $G = (V, E)$  mit  $V = \{1, \dots, n\}$ 
2   $S := \{1\}$ 
3  markiere Knoten 1
4  repeat
5      wähle einen Knoten  $u \in S$ 
6       $S := S - \{u\}$ 
7      for all  $(u, v) \in E$  do
8          if  $v$  ist nicht markiert then
9              markiere  $v$ 
10              $S := S \cup \{v\}$ 
11 until  $S = \emptyset$ 
12 if  $n$  ist markiert then accept else reject

```

Es ist üblich, den Ressourcenverbrauch von Algorithmen (wie z.B. Rechenzeit oder Speicherplatz) in Abhängigkeit von der Größe der Problemeingabe zu messen. Falls die Eingabe aus einem Graphen besteht, kann beispielsweise die Anzahl n der Knoten (oder auch die Anzahl m der Kanten) als Bezugsgröße dienen. Genau genommen hängt die Eingabegröße davon ab, welche Kodierung wir für die Eingaben verwenden.

Komplexitätsbetrachtungen:

- REACH ist in Zeit n^3 entscheidbar.

- REACH ist nichtdeterministisch in Platz $\log n$ entscheidbar (und daher deterministisch in Platz $\log^2 n$; Satz von Savitch).

Als nächstes betrachten wir das Problem, einen maximalen Fluss in einem Netzwerk zu bestimmen.

Maximaler Fluß (MAXFLOW):

Gegeben: Ein gerichteter Graph $G = (V, E)$ mit $V = \{1, \dots, n\}$, $E \subseteq V \times V$ und einer Kapazitätsfunktion $c : E \rightarrow \mathbb{N}$.

Gesucht: Ein Fluss $f : E \rightarrow \mathbb{N}$ von 1 nach n in G , d.h.

- $\forall e \in E : f(e) \leq c(e)$ und
- $\forall v \in V - \{1, n\} : \sum_{(v,u) \in E} f(v, u) = \sum_{(u,v) \in E} f(u, v)$,

mit maximalem Wert $w(f) = \sum_{(1,v) \in E} f(1, v)$.

Da hier nach einer Lösung (Fluss) mit optimalem Wert gesucht wird, handelt es sich um ein **Optimierungsproblem** (genauer: Maximierungsproblem). Im Gegensatz hierzu wird bei vielen Entscheidungsproblemen nach der Existenz einer Lösung (mit gewissen Eigenschaften) gefragt.

Komplexitätsbetrachtungen:

- MAXFLOW ist in Zeit n^5 lösbar.
- MAXFLOW ist in Platz n^2 lösbar.

Das folgende Problem scheint zwar auf den ersten Blick nur wenig mit dem Problem MAXFLOW gemein zu haben. In Wirklichkeit entpuppt es sich jedoch als ein Spezialfall von MAXFLOW.

Perfektes Matching in bipartiten Graphen (MATCHING):

Gegeben: Ein bipartiter Graph $G = (U, V, E)$ mit $U = V = \{1, \dots, n\}$ und $E \subseteq U \times V$.

Gefragt: Besitzt G ein perfektes Matching?

Zur Erinnerung: Eine Kantenmenge $M \subseteq E$ heißt **Matching**, falls für alle Kanten $e = (u, v), e' = (u', v') \in M$ mit $e \neq e'$ gilt: $u \neq u'$ und $v \neq v'$. Gilt zudem $\|M\| = n$, so heißt M **perfekt**.

Komplexitätsbetrachtungen:

- MATCHING ist in Zeit n^3 entscheidbar.
- MATCHING ist in Platz n^2 entscheidbar.

Die bisher betrachteten Probleme können in deterministischer Polynomialzeit gelöst werden und gelten daher als effizient lösbar. Zum Schluss dieses Abschnitts betrachten wir ein Problem, für das vermutlich nur ineffiziente Algorithmen existieren.

Travelling Salesman Problem (TSP):

Gegeben: Eine symmetrische $n \times n$ -Distanzmatrix $D = (d_{ij})$ mit $d_{ij} \in \mathbb{N}$.

Gesucht: Eine kürzeste Rundreise, d.h. eine Permutation $\pi \in S_n$ mit minimalem Wert $w(\pi) = \sum_{i=1}^n d_{\pi(i), \pi(i+1)}$, wobei wir $\pi(n+1) = \pi(1)$ setzen.

Komplexitätsbetrachtungen:

- TSP ist in Zeit $n!$ lösbar (Ausprobieren aller Rundreisen).
- TSP ist in Platz n lösbar (mit demselben Algorithmus, der TSP in Zeit $n!$ löst).
- Durch dynamisches Programmieren^a lässt sich TSP in Zeit $n^2 \cdot 2^n$ lösen, der Platzverbrauch erhöht sich dabei jedoch auf $n \cdot 2^n$ (siehe Übungen).

^aHierzu berechnen wir für alle Teilmengen $S \subseteq \{2, \dots, n\}$ und alle $j \in S$ die Länge $l(S, j)$ eines kürzesten Pfades von 1 nach j , der alle Städte in S genau einmal besucht.

2 Rechenmodelle

2.1 Deterministische Turingmaschinen

Definition 1 (Mehrband-Turingmaschine).

Eine **deterministische k -Band-Turingmaschine** (k -DTM oder einfach **DTM**) ist ein Quadrupel $M = (Q, \Sigma, \Gamma, \delta, q_0)$. Dabei ist

- Q eine endliche Menge von **Zuständen**,
- Σ eine endliche Menge von Symbolen (das **Eingabealphabet**) mit $\sqcup, \triangleright \notin \Sigma$ ($\sqcup$ heißt **Blank** und $\triangleright$ heißt **Anfangssymbol**,
- Γ das **Arbeitsalphabet** mit $\Sigma \cup \{\sqcup, \triangleright\} \subseteq \Gamma$,
- $\delta : Q \times \Gamma^k \rightarrow (Q \cup \{q_h, q_{ja}, q_{nein}\}) \times (\Gamma \times \{L, R, N\})^k$ die **Überföhrungsfunktion** (q_h heißt **Haltezustand**, q_{ja} **akzeptierender** und q_{nein} **verwerfender Endzustand**
- und q_0 der **Startzustand**.

Befindet sich M im Zustand $q \in Q$ und stehen die Schreib-Lese-Köpfe auf Feldern mit den Inschriften $a_1, \dots, a_k$ (a_i auf Band i), so geht M bei Ausführung der Anweisung $\delta : (q, a_1, \dots, a_k) \mapsto (q', a'_1, D_1, \dots, a'_k, D_k)$ in den Zustand q' über, ersetzt auf Band i das Symbol a_i durch a'_i und bewegt den Kopf gemäß D_i (im Fall $D_i = L$ um ein Feld nach links, im Fall $D_i = R$ um ein Feld nach rechts und im Fall $D_i = N$ wird der Kopf nicht bewegt).

Außerdem verlangen wir von δ , dass für jede Anweisung $(q, a_1, \dots, a_k) \mapsto (q', a'_1, D_1, \dots, a'_k, D_k)$ mit $a_i = \triangleright$ die Bedingung $a'_i = \triangleright$ und $D_i = R$ erfüllt ist (d.h. das Anfangszeichen $\triangleright$ darf nicht durch ein anderes Zeichen überschrieben werden und der Kopf muss nach dem Lesen von $\triangleright$ immer nach rechts bewegt werden).

Definition 2. Eine **Konfiguration** ist ein $(2k + 1)$ -Tupel $K = (q, u_1, v_1, \dots, u_k, v_k) \in Q \times (\Gamma^* \times \Gamma^+)^k$ und besagt, dass

- q der momentane Zustand und
- $u_i v_i \sqcup \sqcup \dots$ die Inschrift des i -ten Bandes ist, und dass
- sich der Kopf auf Band i auf dem ersten Zeichen von v_i befindet.

Definition 3. Eine Konfiguration $K' = (q', u'_1, v'_1, \dots, u'_k, v'_k)$ heißt **Folgekonfiguration** von $K = (q, u_1, a_1 v_1, \dots, u_k, a_k v_k)$ (kurz: $K \xrightarrow{M} K'$), falls eine Anweisung

$$(q, a_1, \dots, a_k) \mapsto (q', a'_1, D_1, \dots, a'_k, D_k)$$

in δ und $b_1, \dots, b_k \in \Gamma$ existieren, so dass für $i = 1, \dots, k$ jeweils eine der folgenden drei Bedingungen gilt:

1. $D_i = N$, $u'_i = u_i$ und $v'_i = a'_i v_i$,
2. $D_i = L$, $u_i = u'_i b_i$ und $v'_i = b_i a'_i v_i$,
3. $D_i = R$, $u'_i = u_i a'_i$ und $v'_i = \begin{cases} \sqcup, & v_i = \varepsilon, \\ v_i, & \text{sonst,} \end{cases}$

Wir schreiben $K \xrightarrow{M}^t K'$, falls Konfigurationen $K_0, \dots, K_t$ existieren mit $K_0 = K$ und $K_t = K'$, sowie $K_i \xrightarrow{M} K_{i+1}$ für $i = 0, \dots, t - 1$. Die reflexive, transitive Hülle von $\xrightarrow{M}$ bezeichnen wir mit $\xrightarrow{M}^*$, d.h. $K \xrightarrow{M}^* K'$ bedeutet, dass ein $t \geq 0$ existiert mit $K \xrightarrow{M}^t K'$.

Definition 4. Sei $x \in \Sigma^*$ eine Eingabe. Die zugehörige **Startkonfiguration** ist

$$K_x = (q_0, \varepsilon, \triangleright x, \underbrace{\varepsilon, \triangleright, \dots, \varepsilon, \triangleright}_{(k-1)\text{-mal}}).$$

Definition 5. Eine Konfiguration $K = (q, u_1, v_1, \dots, u_k, v_k)$ mit $q \in \{q_h, q_{ja}, q_{nein}\}$ heißt **Endkonfiguration**. Im Fall $q = q_{ja}$ (bzw. $q = q_{nein}$) heißt K **akzeptierende** (bzw. **verwerfende**) **Endkonfiguration**.

Definition 6.

Eine DTM M **hält bei Eingabe** $x \in \Sigma^*$ **im Zustand** q (kurz: $M(x)$ hält im Zustand q), falls $q \in \{q_h, q_{ja}, q_{nein}\}$ ist und es eine Endkonfiguration $K = (q, u_1, v_1, \dots, u_k, v_k)$ gibt mit

$$K_x \xrightarrow[M]{*} K.$$

Weiter definieren wir das **Resultat** $M(x)$ der Rechnung von M bei Eingabe x ,

$$M(x) = \begin{cases} ja, & M(x) \text{ hält im Zustand } q_{ja}, \\ nein, & M(x) \text{ hält im Zustand } q_{nein}, \\ y, & M(x) \text{ hält im Zustand } q_h, \\ \uparrow \text{ (undefiniert),} & \text{sonst.} \end{cases}$$

Dabei ergibt sich y aus $u_k v_k$, indem das erste Symbol $\triangleright$ und sämtliche Blanks am Ende entfernt werden, d. h. $u_k v_k = \triangleright y \sqcup^i$. Für $M(x) = ja$ sagen wir auch „ $M(x)$ akzeptiert“ und für $M(x) = nein$ „ $M(x)$ verwirft“.

Definition 7. Die von einer DTM M **akzeptierte Sprache** ist

$$L(M) = \{x \in \Sigma^* \mid M(x) \text{ akzeptiert}\}.$$

Eine DTM, die eine Sprache L akzeptiert, darf also bei Eingaben $x \notin L$ unendlich lange rechnen. In diesem Fall heißt L **rekursiv aufzählbar**. Dagegen muss eine DTM, die eine Sprache L entscheidet, bei jeder Eingabe halten.

Definition 8. Sei $L \subseteq \Sigma^*$. Eine DTM M **entscheidet** L , falls für alle $x \in \Sigma^*$ gilt:

$$\begin{aligned} x \in L &\Rightarrow M(x) \text{ akz.} \\ x \notin L &\Rightarrow M(x) \text{ verw.} \end{aligned}$$

In diesem Fall heißt L **entscheidbar** (oder **rekursiv**).

Definition 9. Sei $f : \Sigma^* \rightarrow \Sigma^*$ eine Funktion. Eine DTM M **berechnet** f , falls für alle $x \in \Sigma^*$ gilt:

$$M(x) = f(x).$$

f heißt dann **berechenbar** (oder **rekursiv**).

Aus dem Grundstudium wissen wir, dass eine nichtleere Sprache $L \subseteq \Sigma^*$ genau dann rekursiv aufzählbar ist, wenn eine rekursive Funktion $f : \Sigma^* \rightarrow \Sigma^*$ existiert, deren Bild $\text{range}(f) = \{f(x) \mid x \in \Sigma^*\}$ die Sprache L ist.

2.2 Nichtdeterministische Berechnungen

Anders als eine DTM, für die in jeder Konfiguration höchstens eine Anweisung ausführbar ist, hat eine nichtdeterministische Turingmaschine in jedem Rechenschritt die Wahl unter einer endlichen Anzahl von Anweisungen.

Definition 10. Eine **nichtdeterministische k -Band-Turingmaschine** (kurz k -NTM oder einfach NTM) ist ein 5-Tupel $M = (Q, \Sigma, \Gamma, \delta, q_0)$, wobei Q, Σ, Γ, q_0 genau wie bei einer k -DTM definiert sind und

$$\delta : Q \times \Gamma^k \rightarrow \mathcal{P}(Q \cup \{q_h, q_{ja}, q_{nein}\} \times (\Gamma \times \{R, L, N\})^k)$$

die Eigenschaft hat, dass für $(q', a'_1, D_1, \dots, a'_k, D_k) \in \delta(q, a_1, \dots, a_k)$ im Fall $a_i = \triangleright$ immer $a'_i = \triangleright$ und $D_i = R$ gilt.

Die Begriffe **Konfiguration**, **Start-** und **Endkonfiguration** übertragen sich unmittelbar von DTMs auf NTMs. Der Begriff der **Folgekonfiguration** lässt sich übertragen, indem wir $\delta(q, a_1, \dots, a_k) = (q', a'_1, D_1, \dots, a'_k, D_k)$ durch $(q', a'_1, D_1, \dots, a'_k, D_k) \in \delta(q, a_1, \dots, a_k)$ ersetzen (in beiden Fällen schreiben wir auch oft

$$\delta : (q, a_1, \dots, a_k) \mapsto (q', a'_1, D_1, \dots, a'_k, D_k)$$

oder einfach $(q, a_1, \dots, a_k) \mapsto (q', a'_1, D_1, \dots, a'_k, D_k)$.

Wir werden NTMs nur zum Erkennen von Sprachen (d.h. als Akzeptoren) und nicht zum Berechnen von Funktionen benutzen.

Definition 11.

- a) Sei M eine NTM. Wir sagen $M(x)$ **akzeptiert**, falls $M(x)$ nur endlich lange Rechnungen ausführt und eine akzeptierende Endkonfiguration K existiert mit $K_x \rightarrow^* K$.
- b) Akzeptiert $M(x)$ nicht und hat $M(x)$ nur endlich lange Rechnungen, so **verwirft** $M(x)$.
- c) Falls $M(x)$ unendlich lange Rechnungen ausführt, ist $M(x) = \uparrow$ (undefiniert).
- d) Die von M **akzeptierte Sprache** ist

$$L(M) = \{x \in \Sigma^* \mid M(x) \text{ akzeptiert}\}.$$

- e) M **entscheidet** $L(M)$, falls M alle Eingaben $x \notin L(M)$ verwirft.

2.3 Zeitkomplexität

Der Zeitverbrauch $time_M(x)$ einer Turingmaschine M bei Eingabe x ist die maximale Anzahl an Rechenschritten, die M ausgehend von der Startkonfiguration K_x ausführen kann (bzw. undefiniert oder ∞ , falls unendlich lange Rechnungen existieren).

Definition 12.

- a) Sei M eine TM und sei $x \in \Sigma^*$ eine Eingabe. Dann ist

$$time_M(x) = \max\{t \geq 0 \mid \exists K : K_x \vdash^t K\}$$

die **Rechenzeit** von M bei Eingabe x , wobei $\max \mathbb{N} = \infty$ ist.

- b) Sei $t : \mathbb{N} \rightarrow \mathbb{N}$ eine monoton wachsende Funktion. Dann ist M **$t(n)$ -zeitbeschränkt**, falls für alle $x \in \Sigma^*$ gilt:

$$time_M(x) \leq t(|x|).$$

Alle Sprachen, die in (nicht-)deterministischer Zeit $t(n)$ entscheidbar sind, fassen wir in den Komplexitätsklassen

$$DTIME(t(n)) = \{L(M) \mid M \text{ ist eine } t(n)\text{-zeitbeschränkte DTM}\}$$

bzw.

$$NTIME(t(n)) = \{L(M) \mid M \text{ ist eine } t(n)\text{-zeitbeschränkte NTM}\}$$

zusammen. Ferner sei

$$FTIME(t(n)) = \left\{ f \mid \begin{array}{l} f \text{ wird von einer } t(n)\text{-zeitbe-} \\ \text{schränkten DTM berechnet} \end{array} \right\}.$$

Die wichtigsten Zeitkomplexitätsklassen sind

$$\begin{aligned} LINTIME &= DTIME(O(n)) = \bigcup_{c \geq 1} DTIME(cn) && \text{„Linearzeit“}, \\ P &= DTIME(n^{O(1)}) = \bigcup_{c \geq 1} DTIME(n^c) && \text{„Polynomialzeit“}, \\ E &= DTIME(2^{O(n)}) = \bigcup_{c \geq 1} DTIME(2^{cn}) && \text{„Lineare Exponentialzeit“}, \\ EXP &= DTIME(2^{n^{O(1)}}) = \bigcup_{c \geq 1} DTIME(2^{n^c}) && \text{„Exponentialzeit“}. \end{aligned}$$

Die Klassen NP, NE, NEXP und FP, FE, FEXP sind analog definiert.

2.4 Platzkomplexität

Zur Definition von Platzkomplexitätsklassen verwenden wir so genannte Offline-Turingmaschinen und Transducer. Diese haben die

Eigenschaft, dass sie das erste Band nur als Eingabeband (also nur zum Lesen) bzw. das k -te Band nur als Ausgabeband (also nur zum Schreiben) benutzen. Der Grund für diese Einschränkungen liegt darin, sinnvolle Definitionen für Komplexitätsklassen mit einem sublinearen Platzverbrauch zu erhalten.

Definition 13. Eine TM M heißt **Offline-TM**, falls für jede Anweisung $(q, a_1, \dots, a_k) \mapsto (q', a'_1, D_1, \dots, a'_k, D_k)$ die Implikation

$$a'_1 = a_1 \wedge a_1 = \sqcup \Rightarrow D_1 = L$$

gilt. Gilt weiterhin immer $D_k \neq L$ und ist M eine DTM, so heißt M **Transducer**.

Dies bedeutet, dass eine Offline-TM nicht auf das Eingabeband schreiben darf (*read-only*). Beim Transducer dient das letzte Band als Ausgabeband, auch hier können keine Berechnungen durchgeführt werden (*write-only*).

Der Zeitverbrauch $time_M(x)$ von Offline-TMs und von Transducern ist genauso definiert wie bei DTMs. Als nächstes definieren wir den Platzverbrauch einer TM als die maximale Summe aller während einer Rechnung besuchten Bandfelder.

Definition 14.

a) Sei M eine TM und sei $x \in \Sigma^*$ eine Eingabe mit $time_M(x) < \infty$. Dann ist

$$space_M(x) = \max\{s \geq 1 \mid \exists K = (q, u_1, v_1, \dots, u_k, v_k) \text{ mit } K_x \vdash^* K \text{ und } s = \sum_{i=1}^k |u_i v_i|\}$$

der **Platzverbrauch** von M bei Eingabe x . Für eine Offline-TM ersetzen wir $\sum_{i=1}^k |u_i v_i|$ durch $\sum_{i=2}^k |u_i v_i|$ und für einen Transducer durch $\sum_{i=2}^{k-1} |u_i v_i|$.

b) Sei $s : \mathbb{N} \rightarrow \mathbb{N}$ eine monoton wachsende Funktion. Dann ist M $s(n)$ -**platzbeschränkt**, falls für alle $x \in \Sigma^*$

$$space_M(x) \leq s(|x|) \text{ und } time_M(x) < \infty$$

gilt, $space_M(x)$ ist undefiniert, falls $time_M(x)$ undefiniert ist.

Alle Sprachen, die in (nicht-) deterministischem Platz $s(n)$ entscheidbar sind, fassen wir in den Komplexitätsklassen

$$DSPACE(s(n)) = \left\{ L(M) \mid \begin{array}{l} M \text{ ist eine } s(n)\text{-platzbe-} \\ \text{schränkte Offline-DTM} \end{array} \right\}$$

bzw.

$$NSPACE(s(n)) = \left\{ L(M) \mid \begin{array}{l} M \text{ ist eine } s(n)\text{-platzbe-} \\ \text{schränkte Offline-NTM} \end{array} \right\}$$

zusammen. Ferner sei

$$FSPACE(s(n)) = \left\{ f \mid \begin{array}{l} f \text{ wird von einer } t(n)\text{-platzbe-} \\ \text{schränkten DTM berechnet} \end{array} \right\}.$$

Die wichtigsten Platzkomplexitätsklassen sind

$$\begin{aligned} L &= LOGSPACE = DSPACE(\log n) \\ L^c &= DSPACE(\log^c n) \\ LINSPEACE &= DSPACE(O(n)) \\ PSPACE &= DSPACE(n^{O(1)}) \\ ESPACE &= DSPACE(2^{O(n)}) \\ EXPSPACE &= DSPACE(2^{n^{O(1)}}) \end{aligned}$$

Die Klassen NL, NLINSPEACE und NPSPACE, sowie FL, FLINSPEACE und FPSPACE sind analog definiert, wobei NPSPACE mit PSPACE zusammenfällt (wie wir bald sehen werden).

3 Grundlegende Beziehungen

In diesem Kapitel leiten wir die wichtigsten Inklusionsbeziehungen zwischen deterministischen und nichtdeterministischen Platz- und Zeitkomplexitätsklassen her. Zuerst befassen wir uns jedoch mit Robustheitseigenschaften dieser Klassen.

3.1 Robustheit von Komplexitätsklassen

Wir zeigen zuerst, dass platzbeschränkte TMs nur ein Arbeitsband benötigen.

Lemma 15 (Bandreduktion).

Sei $M = (Q, \Sigma, \Gamma, \delta, q_0)$ eine $s(n)$ -platzbeschränkte Offline-DTM. Dann ex. eine $s(n)$ -platzbeschränkte Offline-2-DTM M' mit $L(M') = L(M)$.

Beweis. Betrachte die Offline-2-DTM $M' = (Q', \Sigma, \Gamma', \delta', q'_0)$ mit $\Gamma' = \Gamma \cup (\Gamma \cup \hat{\Gamma})^{k-1}$, wobei $\hat{\Gamma}$ für jedes $a \in \Gamma$ die markierte Variante $\hat{a}$ enthält. M' hat dasselbe Eingabeband wie M , speichert aber die Inhalte von $(k-1)$ übereinander liegenden Feldern der Arbeitsbänder von M auf einem Feld ihres Arbeitsbandes. Zur Speicherung der Kopfpositionen von M werden Markierungen benutzt.

Initialisierung: In den ersten beiden Rechenschritten erzeugt M' auf ihrem Arbeitsband (Band 2) $k-1$ Spuren, die jeweils mit dem markierten Anfangszeichen $\hat{\triangleright}$ initialisiert werden:

$$K_x = (q'_0, \varepsilon, \triangleright x, \varepsilon, \triangleright) \xrightarrow{M'} (q'_1, \triangleright, x, \triangleright, \sqcup) \xrightarrow{M'} (q'_2, \varepsilon, \triangleright x, \triangleright, \begin{pmatrix} \hat{\triangleright} \\ \vdots \\ \hat{\triangleright} \end{pmatrix})$$

Simulation: M' simuliert einen Rechenschritt von M , indem sie den Kopf auf dem Arbeitsband soweit nach rechts bewegt, bis sie alle $(k-1)$ markierten Zeichen $a_2, \dots, a_k$ gefunden hat. Diese speichert sie neben dem aktuellen Zustand q von M in ihrem Zustand. Während M' den Kopf wieder nach links bewegt, führt M' folgende Aktionen durch: Ist a_1 das von M' (und von M) gelesene Eingabezeichen und ist $\delta(q, a_1, a_2, \dots, a_k) = (q', a_1, D_1, a'_2, D_2, \dots, a'_k, D_k)$, so bewegt M' den Eingabekopf gemäß D_1 , ersetzt auf dem Arbeitsband die markierten Zeichen a_i durch a'_i und verschiebt deren Marken gemäß D_i , $i = 2, \dots, k$.

Akzeptanzverhalten: M' akzeptiert genau dann, wenn M akzeptiert.

Offenbar gilt nun $L(M') = L(M)$ und $\text{space}_{M'}(x) \leq \text{space}_M(x)$. $\square$

In den Übungen wird gezeigt, dass die Sprache der Palindrome durch eine 2-DTM zwar in Linearzeit entscheidbar ist, eine 1-DTM hierzu jedoch Zeit $\Omega(n^2)$ benötigt. Tatsächlich lässt sich jede $t(n)$ -zeitbeschränkte k -DTM M von einer 1-DTM M' in Zeit $O(t(n)^2)$ simulieren. Bei Verwendung einer 2-DTM ist die Simulation sogar in Zeit $O(t(n) \log t(n))$ durchführbar (siehe Übungen). Als nächstes wenden wir uns wichtigen Robustheitseigenschaften von Platz- und Zeitkomplexitätsklassen zu.

Satz 16 (Lineare Platzkompression und Beschleunigung).

Für alle $c > 0$ gilt

- i) $\text{DSPACE}(s(n)) \subseteq \text{DSPACE}(2 + cs(n))$, (lin. space compression)
- ii) $\text{DTIME}(t(n)) \subseteq \text{DTIME}(2 + n + c \cdot t(n))$. (linear speedup)

Beweis. i) Sei $L \in \text{DSPACE}(s(n))$ und sei $M = (Q, \Sigma, \Gamma, \delta, q_0)$ eine $s(n)$ -platzbeschränkte Offline- k -DTM mit $L(M) = L$. Nach vorigem Lemma können wir $k = 2$ annehmen. O.B.d.A. sei $c < 1$. Wähle $m = \lceil 1/c \rceil$ und betrachte die Offline-2-DTM

$$M' = (Q \times \{1, \dots, m\}, \Sigma, \Gamma \cup \Gamma^m, \delta', (q_0, m))$$

mit

$$\delta'((q, i), a, b) = \begin{cases} ((q', 1), a, D_1, \triangleright, R), & \text{falls } b = \triangleright \text{ und } \delta(q, a, \triangleright) = (q', a, D_1, \triangleright, R), \\ ((q', j), a, D_1, (b_1, \dots, b_{i-1}, b'_i, b_{i+1}, \dots, b_m), D'_2), & \text{falls } [b = (b_1, \dots, b_m) \text{ oder } b = \sqcup = b_1 = \dots = b_m] \text{ und } \delta(q, a, b_i) = (q', a, D_1, b'_i, D_2), \end{cases}$$

wobei

$$j = \begin{cases} i, & D_2 = N \\ i + 1, & D_2 = R, i < m \\ 1, & D_2 = R, i = m \\ m, & D_2 = L, i = 1 \\ i - 1, & D_2 = L, i > 1 \end{cases} \quad \text{und} \quad D'_2 = \begin{cases} L, & D_2 = L, i = 1 \\ R, & D_2 = R, i = m \\ N, & \text{sonst} \end{cases}$$

ist. Identifizieren wir die Zustände (q_{ja}, i) mit q_{ja} und (q_{nein}, i) mit q_{nein} , so ist leicht zu sehen, dass $L(M') = L(M) = L$ gilt. Zudem gilt

$$\begin{aligned} space_{M'} &\leq 1 + \lceil (space_M(x) - 1)/m \rceil \\ &\leq 2 + space_M(x)/m \\ &\leq 2 + c \cdot space_M(x) \quad (\text{wegen } m = \lceil 1/c \rceil \geq 1/c). \end{aligned}$$

ii) Sei $L \in \text{DTIME}(t(n))$ und sei $M = (Q, \Sigma, \Gamma, \delta, q_0)$ eine $t(n)$ -zeitbeschränkte k -DTM mit $L(M) = L$, wobei wir $k \geq 2$ annehmen. Wir konstruieren eine DTM M' mit $L(M') = L$ und $time_{M'}(x) \leq 2 + |x| + c \cdot time_M(x)$. M' verwendet das Alphabet $\Gamma' = \Gamma \cup \Gamma^m$ mit $m = \lceil 8/c \rceil$ und simuliert M wie folgt.

Initialisierung: M' kopiert die Eingabe $x = x_1 \dots x_n$ in Blockform auf das zweite Band. Hierzu fasst M' je m Zeichen von x zu einem Block $(x_{im+1}, \dots, x_{(i+1)m})$, $i = 0, \dots, l = \lceil n/m \rceil - 1$, zusammen, wobei der letzte Block $(x_{lm+1}, \dots, x_n, \sqcup, \dots, \sqcup)$ mit

$(l+1)m - n$ Blanks auf die Länge m gebracht wird. Sobald M' das erste Blank hinter der Eingabe x erreicht, ersetzt sie dieses durch das Zeichen $\triangleright$, d.h. das erste Band von M' ist nun mit $\triangleright x \triangleright$ und das zweite Band mit

$$\triangleright (x_1, \dots, x_m) \dots (x_{(l-1)m+1}, \dots, x_{lm}) (x_{lm+1}, \dots, x_n, \sqcup, \dots, \sqcup)$$

beschriftet. Hierzu benötigt M' genau $n+2$ Schritte. In weiteren $l+1 = \lceil n/m \rceil$ Schritten kehrt M' an den Beginn des 2. Bandes zurück. Von nun an benutzt M' das erste Band als Arbeitsband und das zweite als Eingabeband.

Simulation: M' simuliert jeweils eine Folge von m Schritten von M in 6 Schritten:

M' merkt sich in ihrem Zustand den Zustand q von M vor Ausführung dieser Folge und die aktuellen Kopfpositionen $i_j \in \{1, \dots, m\}$ von M innerhalb der gerade gelesenen Blöcke auf den Bändern $j = 1, \dots, k$. Die ersten 4 Schritte verwendet M' , um die beiden Nachbarblöcke auf jedem Band zu erfassen ($LRRL$). Mit dieser Information kann M' die nächsten m Schritte von M vorausberechnen und die entsprechende Konfiguration in 2 weiteren Schritten herstellen.

Akzeptanzverhalten: M' akzeptiert genau dann, wenn M dies tut.

Es ist klar, dass $L(M') = L$ ist. Zudem gilt für jede Eingabe x der Länge $|x| = n$

$$\begin{aligned} time_{M'}(x) &\leq n + 2 + \lceil n/m \rceil + 6 \lceil t(n)/m \rceil \\ &\leq n + 2 + 7 \lceil t(n)/m \rceil \\ &\leq n + 2 + 7ct(n)/8 + 7 \\ &\leq n + 2 + ct(n), \text{ falls } c \cdot t(n)/8 \geq 7. \end{aligned}$$

Da das Ergebnis der Rechnung von $M(x)$ im Fall $t(n) < 56/c$ nur von konstant vielen Eingabezeichen abhängt, kann M' diese Eingaben schon während der Initialisierungsphase (durch table-lookup) in Zeit $n+2$ entscheiden. $\square$