

Vorlesungsskript
Einführung in die
Komplexitätstheorie

Wintersemester 2016/17

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

17. November 2016

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
3.2	Deterministische Simulationen von nichtdeterministischen Berechnungen	9
3.3	Der Satz von Savitch	10
3.4	Der Satz von Immerman und Szelepcsényi	11
4	Hierarchiesätze	16
4.1	Unentscheidbarkeit mittels Diagonalisierung	16
4.2	Das Gap-Theorem	17

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)
- Kryptografie (Wieviel Rechenressourcen benötigt ein Gegner, um ein Kryptosystem zu brechen?)

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

Erreichbarkeitsproblem in Digraphen (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:

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

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. Dieser markiert nach und nach alle Knoten, die vom Knoten 1 aus erreichbar sind. Hierzu speichert er jeden markierten Knoten solange in einer Menge S bis er sämtliche Nachbarknoten markiert hat. 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 (und/oder die Anzahl m der Kanten) als Bezugsgröße dienen. Der Ressourcenverbrauch hängt auch davon ab, wie wir die Eingabe kodieren. So führt die Repräsentation eines Graphen als Adjazenzliste oftmals zu effizienteren Lösungsverfahren.

Komplexitätsbetrachtungen:

- REACH ist in Zeit $O(n^2)$ entscheidbar.

1 Einführung

- REACH ist nichtdeterministisch in Platz $O(\log n)$ entscheidbar (und daher deterministisch in Platz $O(\log^2 n)$; 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 $O(n^5)$ lösbar.
- MAXFLOW ist in Platz $O(n^2)$ 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 $G = (U, W, E)$ mit $U \cap W = \emptyset$ und $e \cap U \neq \emptyset \neq e \cap W$ für alle Kanten $e \in E$.

Gefragt: Besitzt G ein perfektes Matching?

Zur Erinnerung: Eine Kantenmenge $M \subseteq E$ heißt **Matching**, falls für alle Kanten $e, e' \in M$ mit $e \neq e'$ gilt: $e \cap e' = \emptyset$. Gilt zudem $\|M\| = n/2$, so heißt M **perfekt** (n ist die Knotenzahl von G).

Komplexitätsbetrachtungen:

- MATCHING ist in Zeit $O(n^3)$ entscheidbar.
- MATCHING ist in Platz $O(n^2)$ 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. Wie üblich bezeichnen wir die Gruppe aller Permutationen auf der Menge $\{1, \dots, n\}$ mit S_n .

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

*Hierzu 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 5-Tupel $M = (Q, \Sigma, \Gamma, \delta, q_0)$. 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

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

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 **halt** bei Eingabe $x \in \Sigma^*$ (kurz: $M(x)$ halt), falls 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 ,

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

Dabei ergibt sich y aus $u_k v_k$, indem das erste Symbol \triangleright und samtliche Blanks am Ende entfernt werden, d. h. $u_k v_k = \triangleright y \sqcup^i$ fur ein $i \geq 0$. Fur $M(x) = \text{ja}$ sagen wir auch „ $M(x)$ akzeptiert“ und fur $M(x) = \text{nein}$ „ $M(x)$ 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 heit L **semi-entscheidbar** (oder **rekursiv aufzahlbar**). 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 fur 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 heit L **entscheidbar** (oder **rekursiv**).

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

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

f heit dann **berechenbar** (oder **rekursiv**).

Aus dem Grundstudium wissen wir, dass eine nichtleere Sprache $L \subseteq \Sigma^*$ genau dann semi-entscheidbar ist, wenn eine berechenbare 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, fur die in jeder Konfiguration hochstens eine Anweisung ausfuhrbar 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

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

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

Die Begriffe **Konfiguration**, **Start-** und **Endkonfiguration** ubertragen sich unmittelbar von DTMs auf NTMs. Der Begriff der **Folgekonfiguration** lasst sich ubertragen, 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 Fallen schreiben wir auch $(q, a_1, \dots, a_k) \mapsto (q', a'_1, D_1, \dots, a'_k, D_k)$.

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

Definition 11. Sei M eine NTM.

- $M(x)$ **hält** (kurz $M(x) \downarrow$), falls $M(x)$ nur endlich lange Rechnungen ausführt. Andernfalls schreiben wir $M(x) \uparrow$.
- $M(x)$ **akzeptiert**, falls $M(x)$ hält und eine akzeptierende Endkonfiguration K existiert mit $K_x \rightarrow^* K$.
- $M(x)$ **verwirft**, falls $M(x)$ hält und $M(x)$ nicht akzeptiert.
- Die von M **akzeptierte Sprache** ist

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

- 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 von Rechenschritten, die M ausgehend von der Startkonfiguration K_x ausführen kann (bzw. undefiniert oder ∞ , falls unendlich lange Rechnungen existieren).

Definition 12.

- Sei M eine TM (d.h. eine DTM oder NTM) und sei $x \in \Sigma^*$ eine Eingabe. Dann ist

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

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

- 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

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

bzw.

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

zusammen. Ferner sei

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

Für eine Klasse F von Funktionen $t : \mathbb{N} \rightarrow \mathbb{N}$ sei $\text{DTIME}(F) = \bigcup_{t \in F} \text{DTIME}(t(n))$. $\text{NTIME}(F)$ und $\text{FTIME}(F)$ sind analog definiert. Die Klasse aller polynomiell beschränkten Funktionen bezeichnen wir mit $\text{poly}(n)$. Die wichtigsten Zeitkomplexitätsklassen sind

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

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 Bedingung

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

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 dieses kann nicht als Speicher benutzt 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 Anzahl aller während der Rechnung besuchten Bandfelder.

Definition 14.

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

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

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

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

D.h., $space_M(x)$ ist undefiniert, falls $time_M(x) = \infty$ 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

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

Die wichtigsten Platzkomplexitätsklassen sind

$$\begin{aligned} L &= \text{LOGSPACE} = DSPACE(O(\log n)) \\ L^c &= DSPACE(O(\log^c n)) \\ \text{Linspace} &= DSPACE(O(n)) \\ \text{PSPACE} &= DSPACE(\text{poly}(n)) \\ \text{ESPACE} &= DSPACE(2^{O(n)}) \\ \text{EXSPACE} &= DSPACE(2^{\text{poly}(n)}) \end{aligned}$$

Die Klassen NL, NLINSPACE und NPSPACE, sowie FL, FLINSPACE 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).

Zu jeder $s(n)$ -platzbeschränkten Offline-DTM M ex. eine $s(n)$ -platzbeschränkte Offline-2-DTM M' mit $L(M') = L(M)$.

Beweis. Sei $M = (Q, \Sigma, \Gamma, \delta, q_0)$ eine Offline- k -DTM mit $k \geq 3$. 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 $space_{M'}(x) \leq space_M(x)$. ■

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

Beweis. i) Sei $L \in DSPACE(s(n))$ 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

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

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 k -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. ■

Korollar 17.

- i) $\text{DSPACE}(O(s(n))) = \text{DSPACE}(s(n))$, falls $s(n) \geq 2$.
- ii) $\text{DTIME}(O(t(n))) = \text{DTIME}(t(n))$, falls $t(n) \geq (1 + \varepsilon)n + 2$ für ein $\varepsilon > 0$ ist.
- iii) $\text{DTIME}(O(n)) = \bigcap_{\varepsilon > 0} \text{DTIME}((1 + \varepsilon)n + 2)$.

Beweis. i) Sei $L \in \text{DSPACE}(cs(n) + c)$ für eine Konstante $c \geq 0$. Ist $s(n) < 6$ für alle n , so folgt $L \in \text{DSPACE}(O(1)) = \text{DSPACE}(0)$. Gilt dagegen $s(n) \geq 6$ für alle $n \geq n_0$, so existiert für $c' = 1/2c$ eine Offline- k -DTM M , die L für fast alle Eingaben in Platz $2 + c'cs(n) + c'c \leq 3 + s(n)/2 \leq s(n)$ entscheidet. Wegen $s(n) \geq 2$ können wir M leicht so modifizieren, dass sie auch die endlich vielen Ausnahmen in Platz $s(n)$ entscheidet.

ii) Sei $L \in \text{DTIME}(ct(n) + c)$ für ein $c \geq 0$. Nach vorigem Satz existiert für $c' = \varepsilon/(2 + 2\varepsilon)c$ eine DTM M , die L in Zeit $\text{time}_M(x) \leq 2 + n + c'(ct(n) + c)$ entscheidet. Wegen $t(n) \geq (1 + \varepsilon)n$ und da für alle $n \geq (4 + 2c')/\varepsilon$ die Ungleichung $2 + c'c \leq \varepsilon n/2$ gilt, folgt

$$\text{time}_M(x) \leq 2 + n + c'ct(n) + c'c = \underbrace{c'ct(n)}_{=\frac{\varepsilon t(n)}{2+2\varepsilon}} + \underbrace{2 + c'c + n}_{\leq \frac{(\varepsilon+2)n}{2} \leq \frac{(\varepsilon+2)t(n)}{2+2\varepsilon}} \leq t(n)$$

für fast alle n . Zudem können wir M wegen $t(n) \geq n + 2$ leicht so modifizieren, dass sie auch die endlich vielen Ausnahmen in Zeit $t(n)$ entscheidet.

iii) Klar, da $\text{DTIME}(O(n)) = \text{DTIME}(O((1 + \varepsilon)n + 2))$ und diese Klasse nach ii) für jedes $\varepsilon > 0$ gleich $\text{DTIME}((1 + \varepsilon)n + 2)$ ist. ■

3.2 Deterministische Simulationen von nichtdeterministischen Berechnungen

In diesem Abschnitt betrachten wir möglichst platz- und zeiteffiziente deterministische Simulationen von nichtdeterministischen TMs.

Satz 18.

- i) $\text{NTIME}(t(n)) \subseteq \text{DSPACE}(O(t(n)))$,
- ii) $\text{NSPACE}(s(n)) \subseteq \text{DTIME}(2^{O(s(n)+\log n)})$.

Beweis. i) Sei $L \in \text{NTIME}(t(n))$ und sei $N = (Q, \Sigma, \Gamma, \Delta, q_0)$ eine k -NTM, die L in Zeit $t(n)$ entscheidet. Weiter sei

$$d = \max_{(q, \vec{a}) \in Q \times \Gamma^k} \|\delta(q, \vec{a})\|$$

der maximale Verzweigungsgrad von N . Dann ist jede Rechnung

$$K_x = K_0 \xrightarrow{N} K_1 \xrightarrow{N} \dots \xrightarrow{N} K_t$$

der Länge t von $N(x)$ eindeutig durch eine Folge $(i_1, \dots, i_t) \in \{1, \dots, d\}^t$ beschreibbar. Betrachte die Offline- $(k+2)$ -DTM M , die auf ihrem 2. Band für $t = 1, 2, \dots$ der Reihe nach alle Folgen $(i_1, \dots, i_t) \in \{1, \dots, d\}^t$ generiert. Für jede solche Folge kopiert M die Eingabe auf Band 3 und simuliert die zugehörige Rechnung von $N(x)$ auf den Bändern 3 bis $k+2$. M akzeptiert, sobald N bei einer dieser Simulationen in den Zustand q_{ja} gelangt. Wird dagegen ein t erreicht, für das alle d^t Simulationen von N im Zustand q_{nein} oder q_{h} enden, so verwirft M . Nun ist leicht zu sehen, dass $L(M) = L(N)$ und der Platzverbrauch von M durch

$$\text{space}_M(x) \leq \text{time}_N(x) + \text{space}_N(x) \leq (k+1)(\text{time}_N(x) + 1)$$

beschränkt ist.

ii) Sei $L \in \text{NSPACE}(s(n))$ und sei $N = (Q, \Sigma, \Gamma, \delta, q_0)$ eine Offline-2-NTM, die L in Platz $s(n)$ entscheidet. Bei einer Eingabe x der Länge n kann N

- die Köpfe des Eingabe- bzw. Arbeitsbandes auf höchstens $n + 2$ bzw. $s(n)$ verschiedenen Bandfeldern positionieren,
- das Arbeitsband mit höchstens $\|\Gamma\|^{s(n)}$ verschiedenen Beschriftungen versehen und

- höchstens $\|Q\|$ verschiedene Zustände annehmen.

D.h. ausgehend von der Startkonfiguration K_x kann N in Platz $s(n)$ höchstens

$$t(n) = (n + 2)s(n)\|\Gamma\|^{s(n)}\|Q\| \leq c^{s(n)+\log n}$$

verschiedene Konfigurationen erreichen, wobei c eine von N abhängige Konstante ist. Um N zu simulieren, testet M für $s = 1, 2, \dots$, ob $N(x)$ eine akzeptierende Endkonfiguration $K = (q_{ja}, u_1, v_1, u_2, v_2)$ der Größe $|u_2v_2| = s$ erreichen kann. Ist dies der Fall, akzeptiert M . Erreicht dagegen s einen Wert, so dass $N(x)$ keine Konfiguration der Größe s erreichen kann, verwirft M . Hierzu muss M für $s = 1, 2, \dots, s(n)$ jeweils alle von der Startkonfiguration K_x erreichbaren Konfigurationen der Größe s bestimmen, was in Zeit $(c^{s(n)+\log n})^{O(1)} = 2^{O(s(n)+\log n)}$ möglich ist. ■

Korollar 19. $s(n) \geq \log n \Rightarrow \text{NSPACE}(s(n)) \subseteq \text{DTIME}(2^{O(s(n))})$.

Es gilt somit für jede Funktion $s(n) \geq \log n$,

$$\text{DSPACE}(s) \subseteq \text{NSPACE}(s) \subseteq \text{DTIME}(2^{O(s)})$$

und für jede Funktion $t(n) \geq n + 2$,

$$\text{DTIME}(t) \subseteq \text{NTIME}(t) \subseteq \text{DSPACE}(t).$$

Insbesondere erhalten wir somit die Inklusionskette

$$\begin{aligned} \text{L} \subseteq \text{NL} \subseteq \text{P} \subseteq \text{NP} \subseteq \text{PSPACE} \subseteq \text{NPSpace} \\ \subseteq \text{EXP} \subseteq \text{NEXP} \subseteq \text{EXPSPACE} \subseteq \dots \end{aligned}$$

Des weiteren impliziert Satz 16 für $t(n) \geq n + 2$ und $s(n) \geq \log n$ die beiden Inklusionen

$$\text{NTIME}(t) \subseteq \text{DTIME}(2^{O(t)}) \text{ und } \text{NSPACE}(s) \subseteq \text{DSPACE}(2^{O(s)}),$$

wovon sich letztere noch erheblich verbessern lässt, wie wir im nächsten Abschnitt sehen werden.

3.3 Der Satz von Savitch

Praktisch relevante Komplexitätsklassen werden durch Zeit- und Platzschränken $t(n)$ und $s(n)$ definiert, die sich mit relativ geringem Aufwand berechnen lassen.

Definition 20. Eine monotone Funktion $f : \mathbb{N} \rightarrow \mathbb{N}$ heißt **echte** (engl. proper) **Komplexitätsfunktion**, falls es einen Transducer M gibt mit

- $M(x) = 1^{f(|x|)}$,
- $\text{space}_M(x) = O(f(|x|))$ und
- $\text{time}_M(x) = O(f(|x|) + |x|)$.

Beispiele für echte Komplexitätsfunktionen sind k , $\lceil \log n \rceil$, $\lceil \log^k n \rceil$, $\lceil n \cdot \log n \rceil$, $n^k + k$, 2^n , $n! \cdot \lfloor \sqrt{n} \rfloor$ (siehe Übungen).

Satz 21 (Savitch, 1970).

Für jede echte Komplexitätsfunktion $s(n) \geq \log n$ gilt

$$\text{NSPACE}(s) \subseteq \text{DSPACE}(s^2).$$

Beweis. Sei $L \in \text{NSPACE}(s)$ und sei N eine Offline-2-NTM, die L in Platz $s(n)$ entscheidet. Wie im Beweis von Satz 18 gezeigt, kann N bei einer Eingabe x der Länge n höchstens $c^{s(n)}$ verschiedene Konfigurationen einnehmen. Daher muss im Fall $x \in L$ eine akzeptierende Rechnung der Länge $\leq c^{s(n)}$ existieren. Zudem können wir annehmen, dass $N(x)$ höchstens eine akzeptierende Endkonfiguration \hat{K}_x erreichen kann.

Sei $K_1, \dots, K_{c^{s(n)}}$ eine Aufzählung aller Konfigurationen von $N(x)$ die Platz höchstens $s(n)$ benötigen. Dann ist leicht zu sehen, dass für je zwei solche Konfigurationen K, K' und jede Zahl i folgende Äquivalenz gilt:

$$K \xrightarrow{N}^{\leq 2^i} K' \Leftrightarrow \exists K_j : K \xrightarrow{N}^{\leq 2^{i-1}} K_j \wedge K_j \xrightarrow{N}^{\leq 2^{i-1}} K'.$$

Diese Beobachtung führt sofort auf folgende Prozedur $\text{reach}(K, K', i)$, um die Gültigkeit von $K \xrightarrow[N]{\leq 2^i} K'$ zu testen.

Prozedur $\text{reach}(K, K', i)$

```

1  if  $i = 0$  then return( $K = K'$  or  $K \xrightarrow[N]{>} K'$ )
2  for each Konfiguration  $K_j$  do
3    if  $\text{reach}(K, K_j, i - 1)$  and  $\text{reach}(K_j, K', i - 1)$  then
4      return(true)
5  return(false)

```

Nun können wir N durch folgende Offline- β -DTM M simulieren. M benutzt ihr 2. Band als Laufzeitkeller zur Verwaltung der Inkarnationen der rekursiven Aufrufe von reach . Hierzu speichert M auf ihrem 2. Band eine Folge von Tripeln der Form (K, K', i) . Das 3. Band wird zum Kopieren von Tripeln auf dem 2. Band und zur Berechnung von K_{j+1} aus K_j benutzt wird.

Initialisierung: $M(x)$ schreibt das Tripel $(K_x, \hat{K}_x, \lceil s(|n|) \log c \rceil)$ auf das 2. Band, wobei für das Eingabeband nur die Kopfposition, nicht jedoch die Beschriftung notiert wird (also z.B. $K_x = (q_0, 1, \varepsilon, \triangleright)$).

Simulation: Sei (K, K', i) das am weitesten rechts auf dem 2. Band stehende Tripel (also das oberste Kellerelement).

Im Fall $i = 0$ testet M direkt, ob $K \xrightarrow[N]{\leq 1} K'$ gilt und gibt die Antwort zurück.

Andernfalls fügt M beginnend mit $j = 1$ das Tripel $(K, K_j, i - 1)$ hinzu und berechnet (rekursiv) die Antwort für dieses Tripel.

Ist diese negativ, so wird das Tripel $(K, K_j, i - 1)$ durch das nächste Tripel $(K, K_{j+1}, i - 1)$ ersetzt (solange $j < c^{s(n)}$ ist, andernfalls erfährt das Tripel (K, K', i) eine negative Antwort).

Erhält $(K, K_j, i - 1)$ eine positive Antwort, so ersetzt M das Tripel $(K, K_j, i - 1)$ durch das Tripel $(K_j, K', i - 1)$ und berechnet die zugehörige Antwort. Bei einer negativen Antwort

fährt M mit dem nächsten Tripel $(K, K_{j+1}, i - 1)$ fort. Bei einer positiven Antwort erhält auch (K, K', i) eine positive Antwort.

Akzeptanzverhalten: M akzeptiert, falls die Antwort auf das Starttripel $(K_x, \hat{K}_x, \lceil s(|n|) \log c \rceil)$ positiv ist.

Da sich auf dem 2. Band zu jedem Zeitpunkt höchstens $\lceil s(|n|) \log c \rceil$ Tripel befinden und jedes Tripel $O(s(|x|))$ Platz benötigt, besucht M nur $O(s^2(|x|))$ Felder. ■

Korollar 22.

- i) $\text{NL} \subseteq \text{L}^2$,
- ii) $\text{NPSpace} = \bigcup_{k>0} \text{NSpace}(n^k) \subseteq \bigcup_{k>0} \text{DSpace}(n^{2k}) = \text{PSPACE}$,
- iii) NPSpace ist unter Komplement abgeschlossen,
- iv) $\text{CSL} = \text{NSpace}(n) \subseteq \text{DSpace}(n^2) \cap \text{E}$.

Eine weitere Folgerung aus dem Satz von Savitch ist, dass das Komplement \bar{L} einer Sprache $L \in \text{NSpace}(s)$ in $\text{DSpace}(s^2)$ und somit auch in $\text{NSpace}(s^2)$ liegt. Wir werden gleich sehen, dass \bar{L} sogar in $\text{NSpace}(s)$ liegt, d.h. die nichtdeterministischen Platzklassen $\text{NSpace}(s)$ sind unter Komplementbildung abgeschlossen.

3.4 Der Satz von Immerman und Szelepcsényi

Wie wir gesehen haben, impliziert der Satz von Savitch den Abschluss von NPSpace unter Komplementbildung. Dagegen wurde die Frage ob auch die Klasse $\text{CSL} = \text{NSpace}(n)$ der kontextsensitiven Sprachen unter Komplementbildung abgeschlossen ist, erst in den 80ern von Neil Immerman und unabhängig davon von Robert Szelepcsényi gelöst.

Definition 23. Für eine Sprachklasse \mathcal{C} bezeichne $\text{co-}\mathcal{C} = \{\bar{L} \mid L \in \mathcal{C}\}$ die zu \mathcal{C} **komplementäre Sprachklasse**. Dabei bezeichnet $\bar{L} = \Sigma^* - L$ das **Komplement** einer Sprache $L \subseteq \Sigma^*$.

Die zu NP komplementäre Klasse ist $\text{co-NP} = \{L | \bar{L} \in \text{NP}\}$. Ein Beispiel für ein co-NP-Problem ist TAUT:

Gegeben: Eine boolsche Formel F über n Variablen x_1, \dots, x_n .

Gefragt: Ist F eine Tautologie, d. h. gilt $f(\vec{a}) = 1$ für alle Belegungen $\vec{a} \in \{0, 1\}^n$?

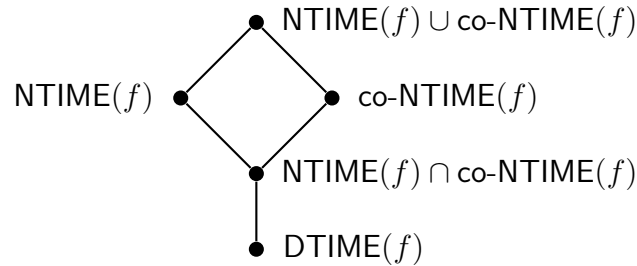
Die Frage ob NP unter Komplementbildung abgeschlossen ist (d. h., ob $\text{NP} = \text{co-NP}$ gilt), ist ähnlich wie das $\text{P} \stackrel{?}{=} \text{NP}$ -Problem ungelöst.

Da sich deterministische Rechnungen leicht komplementieren lassen (durch einfaches Vertauschen der Zustände q_{ja} und q_{nein}), sind deterministische Komplexitätsklassen unter Komplementbildung abgeschlossen.

Proposition 24.

- i) $\text{co-DSPACE}(s(n)) = \text{DSPACE}(s(n))$,
- ii) $\text{co-DTIME}(t(n)) = \text{DTIME}(t(n))$.

Damit ergibt sich folgende Inklusionsstruktur:



Dagegen lassen sich nichtdeterministische Berechnungen nicht ohne weiteres komplementieren; es sei denn, man fordert gewisse Zusatzeigenschaften.

Definition 25. Eine NTM N heißt **strong** bei Eingabe x , falls es entweder akzeptierende oder verwerfende Rechnungen bei Eingabe x gibt (aber nicht beides zugleich).

Proposition 26.

- i) $\text{NTIME}(t(n)) \cap \text{co-NTIME}(t(n)) = \{L(M) \mid M \text{ ist eine } t(n)\text{-zeitbeschränkte NTM, die bei allen Eingaben strong ist}\}$,
- ii) $\text{NSPACE}(s(n)) \cap \text{co-NSPACE}(s(n)) = \{L(M) \mid M \text{ ist eine } s(n)\text{-platzbeschr. Offline-NTM, die bei allen Eingaben strong ist}\}$.

Beweis. Siehe Übungen. ■

Satz 27 (Immerman und Szelepcsényi, 1987).

Für jede echte Komplexitätsfunktion $s(n) \geq \log n$ gilt

$$\text{NSPACE}(s) = \text{co-NSPACE}(s).$$

Beweis. Sei $L \in \text{NSPACE}(s)$ und sei N eine $s(n)$ -platzbeschränkte Offline-NTM mit $L(N) = L$. Wir konstruieren eine $O(s(n))$ -platzbeschränkte Offline-NTM N' mit $L(N') = L$, die bei allen Eingaben strong ist. Hierzu zeigen wir zuerst, dass die Frage, ob $N(x)$ eine Konfiguration K in höchstens t Schritten erreichen kann, durch eine $O(s(n))$ -platzbeschränkte Offline-NTM N_0 entscheidbar ist, die bei Kenntnis der Anzahl

$$r(x, t - 1) = \|\{K \mid K_x \xrightarrow{N}^{\leq t-1} K\}\|$$

aller in höchstens $t - 1$ Schritten erreichbaren Konfigurationen strong ist. Betrachte die Sprache

$$L_0 = \{\langle x, r, t, K \rangle \mid 1 \leq r, t \leq c^{s(n)} \text{ und } K_x \xrightarrow{N}^{\leq t} K\},$$

wobei $K_1, \dots, K_{c^{s(n)}}$ wie im Beweis des Satzes von Savitch eine Aufzählung aller Konfigurationen von $N(x)$ ist, die Platz höchstens $s(n)$ benötigen.

Behauptung 28. Es existiert eine Offline-NTM N_0 mit $L(N_0) = L_0$, die $O(s(|x|))$ Felder besucht und auf allen Eingaben der Form $\langle x, r(x, t - 1), t, K \rangle$ strong ist.

Beweis der Behauptung. $N_0(\langle x, r, t, K \rangle)$ benutzt einen mit dem Wert 0 initialisierten Zähler z und rät der Reihe nach für jede Konfiguration K_i eine Rechnung von $N(x)$ der Länge $\leq t - 1$, die in K_i endet. Falls dies gelingt, erhöht N_0 den Zähler z um 1 und testet, ob $K_i \xrightarrow{N}^{\leq 1} K$ gilt. Falls ja, so hält N_0 im Zustand q_{ja} . Nachdem N_0 alle Konfigurationen K_i durchlaufen hat, hält N_0 im Zustand q_{nein} , wenn z den Wert r hat, andernfalls im Zustand q_{h} .

Pseudocode für $N_0(\langle x, r, t, K \rangle)$

```

1  if  $t = 0$  then halte im Zustand  $q_{\text{nein}}$ 
2   $z := 0$ 
3  for each Konfiguration  $K_i$  do
4    rate eine Rechnung  $\alpha$  der Länge  $\leq t - 1$  von  $N(x)$ 
5    if  $\alpha$  endet in  $K_i$  then
6       $z := z + 1$ 
7      if  $K_i \xrightarrow{N} K$  then
8        halte im Zustand  $q_{\text{ja}}$ 
9  if  $z = r$  then
10   halte im Zustand  $q_{\text{nein}}$ 
11 else
12   halte im Zustand  $q_{\text{h}}$ 

```

Da N_0 genau dann eine akzeptierende Rechnung hat, wenn eine Konfiguration K_i mit $K_x \xrightarrow{N}^{\leq t-1} K_i$ und $K_i \xrightarrow{N}^{\leq 1} K$ existiert, ist klar, dass N_0 die Sprache L_0 entscheidet. Da N_0 zudem $O(s(n))$ -platzbeschränkt ist, bleibt nur noch zu zeigen, dass N_0 bei Eingaben der Form $x_0 = \langle x, r(x, t - 1), t, K \rangle$, $t \geq 1$, strong ist, also $N_0(x_0)$ genau im Fall $x_0 \notin L_0$ eine verwerfende Endkonfiguration erreichen kann.

Um bei Eingabe x_0 eine verwerfende Endkonfiguration zu erreichen, muss N_0 $r = r(x, t - 1)$ Konfigurationen K_i finden, für die zwar $K_x \xrightarrow{N}^{\leq t-1} K_i$ aber nicht $K_i \xrightarrow{N}^{\leq 1} K$ gilt. Dies bedeutet jedoch, dass

K von keiner der $r(x, t - 1)$ in $t - 1$ Schritten erreichbaren Konfigurationen in einem Schritt erreichbar ist und somit x_0 tatsächlich nicht zu L_0 gehört. Die Umkehrung folgt analog. \square

Betrachte nun folgende NTM N' , die für $t = 1, 2, \dots$ die Anzahl $r(x, t)$ der in höchstens t Schritten erreichbaren Konfigurationen in der Variablen r berechnet (diese Technik wird induktives Zählen, engl. *inductive counting*, genannt) und mit Hilfe dieser Anzahlen im Fall $x \notin L$ verifiziert, dass keine der erreichbaren Konfigurationen akzeptierend ist.

Pseudocode für $N'(x)$

```

1   $t := 0$ 
2   $r := 1$ 
3  repeat
4     $t := t + 1$ 
5     $r^- := r$ 
6     $r := 0$ 
7    for each Konfiguration  $K_i$  do
8      simuliere  $N_0(\langle x, r^-, t, K_i \rangle)$ 
9      if  $N_0$  akzeptiert then
10        $r := r + 1$ 
11       if  $K_i$  ist akzeptierende Endkonfiguration then
12         halte im Zustand  $q_{\text{ja}}$ 
13       if  $N_0$  haelt im Zustand  $q_{\text{h}}$  then
14         halte im Zustand  $q_{\text{h}}$ 
15  until ( $r = r^-$ )
16  halte im Zustand  $q_{\text{nein}}$ 

```

Behauptung 29. *Im t -ten Durchlauf der repeat-Schleife wird r^- in Zeile 5 auf den Wert $r(x, t - 1)$ gesetzt. Folglich wird N_0 von N' in Zeile 8 nur mit Eingaben der Form $\langle x, r(x, t - 1), t, K_i \rangle$ aufgerufen.*

Beweis der Behauptung. Wir führen Induktion über t :

$t = 1$: Im ersten Durchlauf der repeat-Schleife erhält r^- den Wert $1 = r(x, 0)$.

$t \rightsquigarrow t + 1$: Da r^- zu Beginn des $(t + 1)$ -ten Durchlaufs auf den Wert von r gesetzt wird, müssen wir zeigen, dass r im t -ten Durchlauf auf $r(x, t)$ hochgezählt wird. Nach Induktionsvoraussetzung wird N_0 im t -ten Durchlauf nur mit Eingaben der Form $\langle x, r(x, t - 1), t, K_i \rangle$ aufgerufen. Da N_0 wegen Beh. 1 auf all diesen Eingaben strong ist und keine dieser Simulationen im Zustand q_h endet (andernfalls würde N' sofort stoppen), werden alle in $\leq t$ Schritten erreichbaren Konfigurationen K_i als solche erkannt und somit wird r tatsächlich auf den Wert $r(x, t)$ hochgezählt. ■

Behauptung 30. Bei Beendigung der repeat-Schleife in Zeile 15 gilt $r = r^- = \|\{K \mid K_x \xrightarrow{N^*} K\}\|$.

Beweis der Behauptung. Wir wissen bereits, dass im t -ten Durchlauf der repeat-Schleife r den Wert $r(x, t)$ und r^- den Wert $r(x, t - 1)$ erhält. Wird daher die repeat-Schleife nach t_e Durchläufen verlassen, so gilt $r = r^- = r(x, t_e) = r(x, t_e - 1)$.

Angenommen $r(x, t_e) < \|\{K \mid K_x \xrightarrow{N^*} K\}\|$. Dann gibt es eine Konfiguration K , die für ein $t' > t_e$ in t' Schritten, aber nicht in t_e Schritten erreichbar ist. Betrachte eine Rechnung $K_x = K_0 \xrightarrow{N} K_1 \xrightarrow{N} \dots \xrightarrow{N} K_{t'} = K$ minimaler Länge, die in K endet. Dann gilt $K_x \xrightarrow{N}^{t_e} K_{t_e}$, aber nicht $K_x \xrightarrow{N}^{\leq t_e - 1} K_{t_e}$ und daher folgt $r(x, t_e) > r(x, t_e - 1)$. Widerspruch! ■

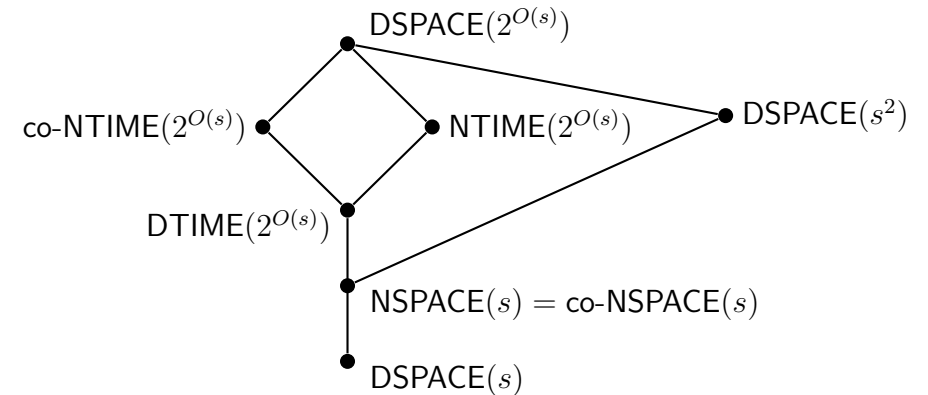
Da N' offenbar die Sprache L in Platz $O(s(n))$ entscheidet, bleibt nur noch zu zeigen, dass N' bei allen Eingaben strong ist. Wegen Behauptung 30 hat $N'(x)$ genau dann eine verwerfende Rechnung, wenn im letzten Durchlauf der repeat-Schleife alle erreichbaren Konfigurationen K als solche erkannt werden und darunter keine akzeptierende

Endkonfiguration ist. Dies impliziert $x \notin L$. Umgekehrt ist leicht zu sehen, dass $N'(x)$ im Fall $x \notin L$ eine verwerfende Rechnung hat. ■

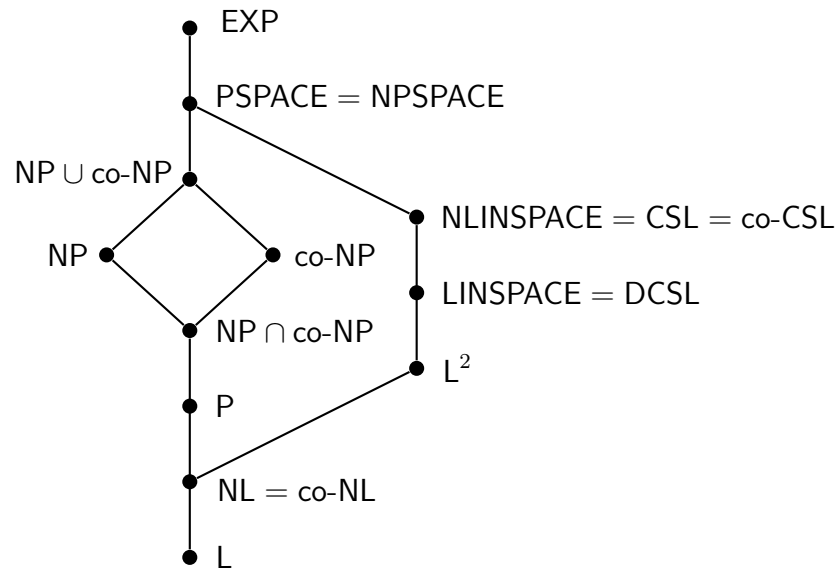
Korollar 31.

1. NL = co-NL,
2. CSL = NLINSPACE = co-CSL.

Damit ergibt sich folgende Inklusionsstruktur für (nicht)deterministische Platz- und Zeitklassen:



Angewandt auf die wichtigsten bisher betrachteten Komplexitätsklassen erhalten wir folgende Inklusionsstruktur:



Eine zentrale Fragestellung der Komplexitätstheorie ist, welche dieser Inklusionen echt sind. Dieser Frage gehen wir im nächsten Kapitel nach.

4 Hierarchiesätze

4.1 Unentscheidbarkeit mittels Diagonalisierung

Wir benutzen folgende Kodierung (Gödelisierung) von 1-DTMs $M = (Q, \Sigma, \Gamma, \delta, q_0)$. O.B.d.A. sei $Q = \{q_0, q_1, \dots, q_m\}$, $\{0, 1, \#\} \subseteq \Sigma$ und $\Gamma = \{a_1, \dots, a_l\}$ (also z.B. $a_1 = \sqcup$, $a_2 = \triangleright$, $a_3 = 0$, $a_4 = 1$ etc.). Dann kodieren wir jedes $\alpha \in Q \cup \Gamma \cup \{q_h, q_{ja}, q_{nein}, L, R, N\}$ wie folgt durch eine Binärzahl $c(\alpha)$ der Länge $b = \lceil \log_2(\|Q\| + \|\Gamma\| + 6) \rceil = \lceil \log_2(m + l + 7) \rceil$:

α	$c(\alpha)$
$q_i, i = 0, \dots, m$	$bin_b(i)$
$a_j, j = 1, \dots, l$	$bin_b(m + j)$
$q_h, q_{ja}, q_{nein}, L, R, N$	$bin_b(m + l + 1), \dots, bin_b(m + l + 6)$

M wird nun durch eine Folge von Binärzahlen, die durch $\#$ getrennt sind, kodiert:

$$\begin{aligned} &\#c(q_0) \#c(a_1) \#c(p_{0,1}) \#c(b_{0,1}) \#c(D_{0,1}) \# \\ &\#c(q_0) \#c(a_2) \#c(p_{0,2}) \#c(b_{0,2}) \#c(D_{0,2}) \# \\ &\quad \vdots \\ &\#c(q_m) \#c(a_l) \#c(p_{m,l}) \#c(b_{m,l}) \#c(D_{m,l}) \# \end{aligned}$$

wobei

$$\delta(q_i, a_j) = (p_{i,j}, b_{i,j}, D_{i,j})$$

für $i = 1, \dots, m$ und $j = 1, \dots, l$ ist. Kodieren wir die Zeichen $0, 1, \#$ binär (z.B. $0 \mapsto 00$, $1 \mapsto 11$, $\# \mapsto 10$), so gelangen wir zu einer

Binärkodierung von M . Diese Kodierung lässt sich auch auf k -DTM's und k -NTM's erweitern. Die Kodierung einer TM M bezeichnen wir mit $\langle M \rangle$. Umgekehrt können wir jedem Binärstring w eine TM M_w wie folgt zuordnen:

$$M_w = \begin{cases} M, & \langle M \rangle = w \\ M', & \text{sonst,} \end{cases}$$

wobei M' eine beliebig aber fest gewählte TM ist. Für M_w schreiben wir auch M_i , wobei i die Zahl mit der Binärdarstellung $1w$ ist. Ein Paar (M, x) bestehend aus einer TM M und einer Eingabe $x \in \{0, 1\}^*$ kodieren wir durch das Wort $\langle M, x \rangle = \langle M \rangle \# x$.

Satz 32. *Die Diagonalsprache*

$$D = \{\langle M_i \rangle \mid M_i \text{ ist eine DTM, die die Eingabe } x_i \text{ akzeptiert}\}.$$

ist semi-entscheidbar, aber nicht entscheidbar. Hierbei ist $x_1 = \varepsilon$, $x_2 = 0$, $x_3 = 1$, $x_4 = 00, \dots$ die Folge aller Binärstrings in lexikografischer Reihenfolge.

Beweis. Es ist klar, dass D semi-entscheidbar ist, da es eine DTM gibt, die bei Eingabe $\langle M_i \rangle$ die Berechnung von M_i bei Eingabe x_i simuliert und genau dann akzeptiert, wenn dies $M_i(x_i)$ tut.

Dass \bar{D} nicht semi-entscheidbar (und damit D nicht entscheidbar) ist, liegt daran, dass die charakteristische Funktion von \bar{D} „komplementär“ zur Diagonalen der Matrix ist, deren Zeilen die charakteristischen Funktionen aller semi-entscheidbaren Sprachen $L(M_i)$ auflisten. Wir zeigen durch einen einfachen Widerspruchsbeweis, dass keine Zeile der Matrix mit dem Komplement ihrer Diagonalen übereinstimmen kann. Wäre \bar{D} semi-entscheidbar, gäbe es also eine DTM M_d , die \bar{D} akzeptiert,

$$L(M_d) = \bar{D} \quad (**),$$

	x_1	x_2	x_3	x_4	\dots
M_1	1	0	0	0	\dots
M_2	0	1	0	0	\dots
M_3	1	0	0	0	\dots
M_4	0	0	0	1	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\ddots
M_d	0	0	1	0	\dots

so führt dies wegen

$$\begin{aligned} x_d \in D &\stackrel{(*)}{\Rightarrow} M_d(x_d) \text{ akzeptiert} \stackrel{(**)}{\Rightarrow} x_d \notin D \quad \text{!} \\ x_d \notin D &\stackrel{(*)}{\Rightarrow} M_d(x_d) \text{ akz. nicht} \stackrel{(**)}{\Rightarrow} x_d \in D \quad \text{!} \end{aligned}$$

zu einem Widerspruch. \blacksquare

Satz 33. Für jede berechenbare Funktion $g : \mathbb{N} \rightarrow \mathbb{N}$ existiert eine entscheidbare Sprache $D_g \notin \text{DTIME}(g(n))$.

Beweis. Betrachte die Diagonalsprache

$$D_g = \{ \langle M_i \rangle \mid M_i \text{ ist eine DTM, die die Eingabe } x_i \text{ in } \leq g(|x_i|) \text{ Schritten akzeptiert} \} \quad (*)$$

Offensichtlich ist D_g entscheidbar. Unter der Annahme, dass $D_g \in \text{DTIME}(g(n))$ ist, existiert eine $g(n)$ -zeitbeschränkte DTM M_d , die das Komplement von D_g entscheidet, d.h.

$$L(M_d) = \bar{D}_g \quad (**)$$

Dies führt jedoch auf einen Widerspruch:

$$\begin{aligned} x_d \in D_g &\stackrel{(*)}{\Rightarrow} M_d(x_d) \text{ akzeptiert} \stackrel{(**)}{\Rightarrow} x_d \notin D_g \quad \text{!} \\ x_d \notin D_g &\stackrel{(*)}{\Rightarrow} M_d(x_d) \text{ verwirft} \stackrel{(**)}{\Rightarrow} x_d \in D_g \quad \text{!} \end{aligned} \quad \blacksquare$$

Eine interessante Frage ist nun, wieviel Zeit eine DTM benötigt, um die Sprache D_g zu entscheiden. Im nächsten Abschnitt werden wir sehen, dass D_g i.a. sehr hohe Komplexität haben kann.

4.2 Das Gap-Theorem

Satz 34 (Gap-Theorem).

Es gibt eine berechenbare Funktion $g : \mathbb{N} \rightarrow \mathbb{N}$ mit

$$\text{DTIME}(2^{g(n)}) = \text{DTIME}(g(n)).$$

Beweis. Wir definieren $g(n) \geq n+2$ so, dass für jede $2^{g(n)}$ -zeitb. DTM M gilt:

$$\text{time}_M(x) \leq g(|x|) \text{ für fast alle Eingaben } x.$$

Betrachte hierzu das Prädikat

$$P(n, t) : t \geq n+2 \text{ und für } k = 1, \dots, n \text{ und alle } x \in \Sigma_k^n \text{ gilt: } \text{time}_{M_k}(x) \notin [t+1, 2^t].$$

Hierbei bezeichnet Σ_k das Eingabealphabet von M_k . Da für jedes n alle

$$t \geq \max\{\text{time}_{M_k}(x) \mid 1 \leq k \leq n, x \in \Sigma_k^n, M_k(x) \text{ hält}\}$$

das Prädikat $P(n, t)$ erfüllen, können wir $g(n)$ wie folgt induktiv definieren:

$$g(n) = \begin{cases} 2, & n = 0, \\ \min\{t \geq g(n-1) + n \mid P(n, t)\}, & n > 0. \end{cases}$$

Da P entscheidbar ist, ist g berechenbar.

Um zu zeigen, dass jede Sprache $L \in \text{DTIME}(2^{g(n)})$ bereits in $\text{DTIME}(g(n))$ enthalten ist, sei M_k eine beliebige $2^{g(n)}$ -zeitbeschränkte DTM mit $L(M_k) = L$. Dann muss M_k alle Eingaben x der Länge $n \geq k$ in Zeit $\text{time}_{M_k}(x) \leq g(n)$ entscheiden, da andernfalls $P(n, g(n))$ wegen $\text{time}_{M_k}(x) \in [g(n)+1, 2^{g(n)}]$ verletzt wäre. Folglich ist $L \in \text{DTIME}(g(n))$, da die endlich vielen Eingaben x der Länge $n < k$ durch table-lookup in Zeit $n+2 \leq g(n)$ entscheidbar sind. \blacksquare

Es ist leicht zu sehen, dass der Beweis des Gap-Theorems für jede berechenbare Funktion h eine berechenbare Zeitschranke g liefert, so dass $\text{DTIME}(h(g(n))) = \text{DTIME}(g(n))$ ist. Folglich ist die im Beweis von Satz 33 definierte Sprache D_g nicht in Zeit $h(g(n))$ entscheidbar.