

Theoretische Informatik HS24

Nicolas Wehrli

Übungsstunde 10

26. November 2024

ETH Zürich

nwehrli@ethz.ch

- ① Feedback zur Serie
- ② Komplexitätstheorie
- ③ Nichtdeterministische Komplexitätstheorie

Feedback zur Serie

1. Unterschied EE-Reduktion und R-Reduktion
2. Reduktion alleine reicht nicht.

Ihr müsst noch die Konsequenz davon aufzeigen, um die gewünschte Aussage zu beweisen.

3. zusätzliche $\frac{n}{12}$ kommen vom zurückbewegen des Kopfes an den Start, nicht vom Schreiben!

Implikationsbeweis für Reduktion

Wenn eine Reduktion verlangt wird, dann dürft ihr die Implikation nicht trivial per Implikationsaussage zeigen.

Gemeint damit ist folgender Ansatz.

$L_1 \leq_R L_2$ soll gezeigt werden.

Da per Definition

$$L_1 \leq_R L_2 \iff (L_2 \in \mathcal{L}_R \implies L_1 \in \mathcal{L}_R)$$

folgt die gewünschte Aussage per $L_2 \notin \mathcal{L}_R$ (oder $L_1 \in \mathcal{L}_R$).

Dieser Ansatz gibt an der Prüfung 0 Punkte.

Komplexitätstheorie

Sei M eine MTM oder TM, die immer hält. Sei Σ das Eingabealphabet von M . Sei $x \in \Sigma^*$ und $D = C_1, C_2, \dots, C_k$ die Berechnung von M auf x .

Die **Zeitkomplexität** $\text{Time}_M(x)$ der Berechnung von M auf x ist definiert durch

$$\text{Time}_M(x) = k - 1.$$

Die **Zeitkomplexität von M** ist die Funktion $\text{Time}_M : \mathbb{N} \rightarrow \mathbb{N}$, definiert durch

$$\text{Time}_M(n) = \max \{ \text{Time}_M(x) \mid x \in \Sigma^n \}.$$

Sei $k \in \mathbb{N} \setminus \{0\}$. Sei M eine k -Band-TM, die immer hält.

Sei

$$C = (q, x, i, \alpha_1, i_1, \alpha_2, i_2, \dots, \alpha_k, i_k)$$

mit $0 \leq i \leq |x| + 1$ und $0 \leq i_j \leq |\alpha_j|$ für $j = 1, \dots, k$

eine Konfiguration von M .

Die **Speicherplatzkomplexität von C** ist

$$\text{Space}_M(C) = \max\{|\alpha_i| \mid i = 1, \dots, k\}.$$

Sei C_1, C_2, \dots, C_l die Berechnung von M auf x . Die **Speicherplatzkomplexität von M auf x** ist

$$\mathbf{Space}_M(x) = \max \{ \mathbf{Space}_M(C_i) \mid i = 1, \dots, l \}.$$

Die **Speicherplatzkomplexität von M** ist die Funktion $\mathbf{Space}_M : \mathbb{N} \rightarrow \mathbb{N}$, definiert durch

$$\mathbf{Space}_M(n) = \max \{ \mathbf{Space}_M(x) \mid x \in \Sigma^n \}.$$

Bemerkungen

1. Länge des Eingabewortes, hat keinen Einfluss auf die Speicherplatzkomplexität.
2. Mächtigkeit des Alphabets hat keinen Einfluss auf die Speicherplatzkomplexität.

Lemma 6.1

Sei $k \in \mathbb{N} \setminus \{0\}$. Für jede k -Band-TM A , die immer hält, existiert eine äquivalente 1-Band-TM B , so dass

$$\text{Space}_B(n) \leq \text{Space}_A(n)$$

Beweisskizze:

Gleiche Konstruktion wie in Lemma 4.2.

Lemma 4.2 = "Für jede MTM A existiert eine äquivalente TM B ".

Wir sehen, dass B genau so viele Felder braucht, wie A .

Lemma 6.2

Zu jeder MTM A existiert eine äquivalente MTM B mit

$$\text{Space}_B(n) \leq \frac{\text{Space}_A(n)}{2} + 2$$

Beweisskizze:

Wir fassen jeweils 2 Felder von A zu einem Feld in B zusammen. $\Gamma_B = \Gamma_A \times \Gamma_A$.
Wir addieren 1 für das \wp am linken Rand und 1 für das Aufrunden im Fall von ungerader Länge.

Wir erinnern uns:

Konfiguration einer k -Band-TM

Die Konfiguration einer k -Band-TM sieht wie folgt aus

$$(q, w, i, u_1, i_1, u_2, i_2, \dots, u_k, i_k) \in Q \times \Sigma^* \times \mathbb{N} \times (\Gamma^* \times \mathbb{N})^k$$

wobei

- ▶ q der Zustand der TM ist
- ▶ $\$w\$$ der Inhalt des Eingabebandes, Lesekopf Eingabeband auf dem i -ten Feld
- ▶ für $j \in \{1, \dots, k\}$ ist der Inhalt des j -ten Bandes $\$u_j\$$ und $i_j \leq |u_j|$ die Position des Kopfs auf dem j -ten Band.

► $\mathcal{O}(f(n))$:

Menge aller Funktionen, die asymptotisch nicht schneller wachsen als $f(n)$.

► $\Omega(g(n))$:

Menge aller Funktionen, die asymptotisch mind. so schnell wachsen wie $g(n)$.

► $\Theta(h(n))$:

Menge aller Funktionen, die asymptotisch gleich schnell wachsen wie $h(n)$.

Small o-notation

Seien f und g zwei Funktionen von \mathbb{N} nach \mathbb{R}^+ .

Falls $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$, dann sagen wir, dass g asymptotisch **schneller wächst** als f :

$$f(n) \in o(g(n))$$

Satz 6.1

Es **existiert** ein Entscheidungsproblem $(\Sigma_{\text{bool}}, L)$, so dass für jede MTM A , die $(\Sigma_{\text{bool}}, L)$ entscheidet, eine MTM B existiert, die auch $(\Sigma_{\text{bool}}, L)$ entscheidet, und für die gilt

$$\text{Time}_B(n) \leq \log_2(\text{Time}_A(n))$$

für unendlich viele $n \in \mathbb{N}$.

I.e. es existieren Entscheidungsprobleme, die keinen optimalen Algorithmus haben.

Deswegen fokussieren wir uns auf untere und obere Schranken der Komplexität eines Problems und nicht auf die genaue Bestimmung davon.

Komplexität eines Entscheidungsproblems (Σ, L)

Sei L eine Sprache. Sei $f, g : \mathbb{N} \rightarrow \mathbb{R}^+$.

- ▶ $\mathcal{O}(g(n))$ ist eine **obere Schranke für die Zeitkomplexität von L** , falls eine MTM A **existiert**, die L entscheidet und $\text{Time}_A(n) \in \mathcal{O}(g(n))$.
- ▶ $\Omega(f(n))$ ist eine **untere Schranke für die Zeitkomplexität von L** , falls für **jede** MTM B die L entscheidet und $\text{Time}_B(n) \in \Omega(f(n))$.
- ▶ Eine MTM C heisst **optimal für L** , falls $\text{Time}_C(n) \in \mathcal{O}(f(n))$ und $\Omega(f(n))$ eine untere Schranke für die Zeitkomplexität ist.

Untere Schranke finden und beweisen: **schwierig**.

Obere Schranke kann durch einen konkreten Algorithmus gezeigt werden.

Klassen

Für alle Funktionen $f, g : \mathbb{N} \rightarrow \mathbb{R}^+$ definieren wir

$$\mathbf{TIME}(f) = \{L(B) \mid B \text{ ist eine MTM mit } \text{Time}_B(n) \in \mathcal{O}(f(n))\}$$

$$\mathbf{SPACE}(g) = \{L(A) \mid A \text{ ist eine MTM mit } \text{Space}_A(n) \in \mathcal{O}(g(n))\}$$

$$\mathbf{DLOG} = \mathbf{SPACE}(\log_2 n)$$

$$\mathbf{P} = \bigcup_{c \in \mathbb{N}} \mathbf{TIME}(n^c)$$

$$\mathbf{PSPACE} = \bigcup_{c \in \mathbb{N}} \mathbf{SPACE}(n^c)$$

$$\mathbf{EXPTIME} = \bigcup_{d \in \mathbb{N}} \mathbf{TIME}(2^{nd})$$

Lemma 6.3

Für jede Funktion $t : \mathbb{N} \rightarrow \mathbb{R}^+$ gilt

$$\text{TIME}(t(n)) \subseteq \text{SPACE}(t(n))$$

Beweisskizze:

In $\mathcal{O}(t(n))$ Schritten sind höchstens $\mathcal{O}(t(n))$ Felder beschreibbar.

Korollar 6.1

$$P \subseteq PSPACE$$

Eine Funktion: $s : \mathbb{N} \rightarrow \mathbb{N}$ heisst **platzkonstruierbar**, falls eine 1-Band-TM M existiert, so dass

- (i) $\text{Space}_M(n) \leq s(n)$ für alle $n \in \mathbb{N}$ und
- (ii) für jede Eingabe 0^n , generiert M das Wort $0^{s(n)}$ auf ihrem Arbeitsband und hält in q_{accept} .

Eine Funktion: $t : \mathbb{N} \rightarrow \mathbb{N}$ heisst **zeitkonstruierbar**, falls eine MTM A existiert, so dass

- (i) $\text{Time}_A(n) \leq \mathcal{O}(t(n))$ für alle $n \in \mathbb{N}$ und
- (ii) für jede Eingabe 0^n , generiert A das Wort $0^{t(n)}$ auf dem ersten Arbeitsband und hält in q_{accept} .

Lemma 6.4 (verständlicher formuliert)

Sei $s : \mathbb{N} \rightarrow \mathbb{N}$ platzkonstruierbar.

Für jede MTM M , für welche $\text{Space}_M(w) \leq s(|w|)$ nur für alle $w \in L(M)$ erfüllt, existiert eine äquivalente MTM A , welche dies für alle $w \in \Sigma^*$ erfüllt.

Beweisskizze:

Erzeuge für jede Eingabe $x \in \Sigma^*$ zuerst $0^{s(|x|)}$ auf einem zusätzlichen Band und nutze das als Platzüberwachung.

Wenn A diesen Platz überschreiten will, wird die Simulation unterbrochen und die Eingabe verworfen.

Lemma 6.5 (verständlicher formuliert)

Sei $t : \mathbb{N} \rightarrow \mathbb{N}$ zeitkonstruierbar.

Zu jeder MTM M , welche $\text{Time}_M(w) \leq t(|w|)$ nur für alle $w \in L(M)$ erfüllt, existiert eine äquivalente MTM A mit

$$\text{Time}_A(n) \in \mathcal{O}(t(n))$$

Beweisskizze

1. Schreibe für jede Eingabe $w \in \Sigma^*$ $0^{t(|w|)}$ auf ein zusätzliches Arbeitsband und nutze dies zur Zeitählung.
2. Wenn A mehr Schritte machen will, wird die Simulation abgebrochen und die Eingabe verworfen.
3. Erster Schritt in $\mathcal{O}(t(n))$ und die Simulation auf w dauert $\mathcal{O}(t(n))$

Satz 6.2

Für jede Funktion s mit $s(n) \geq \log_2(n)$ gilt:

$$\mathbf{SPACE}(s(n)) \subseteq \bigcup_{c \in \mathbb{N}} \mathbf{TIME}(c^{s(n)})$$

Beweis

Sei $L \in \mathbf{SPACE}(s(n))$. Nach Lemma 6.1 existiert eine 1-Band-TM $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{accept}, q_{reject})$, die **immer hält**, so dass $L = L(M)$ und $\text{Space}_M(n) \leq d \cdot s(n)$ für $d \in \mathbb{N}$ gelten.

Für jede Konfiguration $C = (q, w, i, x, j)$ von M definieren wir die **innere Konfiguration von C** als

$$\text{In}(C) = (q, i, x, j).$$

Die innere Konfiguration enthält das Eingabewort w nicht, da dies sich während einer Berechnung nicht ändert.

Sei $\text{InKonf}_M(n)$ die Menge aller möglichen inneren Konfigurationen auf Eingabewörtern der Länge n .

Sei $X = |\text{InKonf}_M(n)|$ dessen Kardinalität.

Sei $D = C_1 C_2 \dots C_k$ eine endliche Berechnung von M auf einem Wort w , $|w| = n$.

Wir zeigen per Widerspruch, dass D maximal X verschiedene Konfigurationen haben kann, i.e. $k \leq X$.

Speicherplatzkomplexität zu Zeitkomplexität

Nehmen wir zum Widerspruch an $k > X$.

Dann muss es in $D = C_1C_2...C_i...C_j...C_k$, zwei identische innere Konfigurationen $In(C_i)$ und $In(C_j)$ geben (für $i < j$).

Da M deterministisch ist, sollte aber von $C_i = C_j$ aus immer die gleichen Berechnungsschritte ausgeführt werden.

Dann wäre aber D eine unendliche Berechnung mit der Endlosschleife $C_iC_{i+1}...C_j$.
Widerspruch, da M immer hält.

Speicherplatzkomplexität zu Zeitkomplexität

Eine beliebige endliche Berechnung D von M auf w , $|w| = n$, kann höchstens X viele Zeitschritte (i.e. Konfigurationen) haben.

Jetzt müssen wir noch $X = |\text{InKonf}_M(n)|$ abschätzen.

Wir wissen folgendes

- ▶ Es gibt $|Q|$ verschieden mögliche Zustände.
- ▶ Index des Eingabekopfes ist $0 \leq i \leq n + 1$ (Eingabeband $\$w\$$ mit $|w| = n$)
- ▶ Inhalt des Arbeitsbandes x hat Länge: $|x| \leq \text{Space}_M(n) \leq d \cdot s(n)$
- ▶ Index vom Kopf auf dem Arbeitsband: $0 \leq j \leq \text{Space}_M(n) \leq d \cdot s(n)$
- ▶ $x \in \Gamma^{|x|}$
- ▶ $n + 2 \leq 4^{\log_2 n} \leq 4^{s(n)}$ für $n \geq 2$

Setzen wir alles zusammen:

$$\begin{aligned} |\text{InKonf}_M(n)| &\leq |Q| \cdot (n + 2) \cdot |\Gamma|^{\text{Space}_M(n)} \cdot \text{Space}_M(n) \\ &\leq (\max\{4, |Q|, |\Gamma|\})^{4d \cdot s(n)} \\ &\leq c^{s(n)} \end{aligned}$$



Nichtdeterministische Komplexitätstheorie

Sei M eine NTM oder nichtdet. MTM. Sei $x \in L(M)$.

- $\text{Time}_M(x)$ ist die Länge der kürzesten akzeptierenden Berechnung von M auf x .
- $\text{Time}_M(n) = \max(\{\text{Time}_M(x) \mid x \in L(M) \wedge |x| = n\} \cup \{0\})$
- $\text{Space}_M(C) = \max\{\text{Space}_M(C_i) \mid i = 1, \dots, m\}$ für eine Berechnung $C = C_1, \dots, C_m$ von M .
- $\text{Space}_M(x) = \min\{\text{Space}_M(C) \mid C \text{ ist eine Berechnung von } M \text{ auf } x\}$
- $\text{Space}_M(n) = \max(\{\text{Space}_M(x) \mid x \in L(M) \wedge |x| = n\} \cup \{0\})$

Lemma 6.6

Für alle t, s mit $s(n) \geq \log_2(n)$ gilt:

- (i) $\text{NTIME}(t) \subseteq \text{NSPACE}(t)$
- (ii) $\text{NSPACE}(s) \subseteq \bigcup_{c \in \mathbb{N}} \text{NTIME}(c^{s(n)})$

Beweisskizze

- (i) Kürzeste akzeptierende Berechnung betrachten. Kann in höchstens t Zeitschritten höchstens t Felder beschreiben.
- (ii) Kürzeste akzeptierende Berechnung betrachten. Innere Konfigurationen zählen. Eine Konfiguration kann nicht zweimal vorkommen sonst ist es nicht die kürzeste Berechnung.

Satz 6.5

Sei $s : \mathbb{N} \rightarrow \mathbb{N}, t : \mathbb{N} \rightarrow \mathbb{R}^+$ platzkonstruierbar. Dann gilt:

- (i) $\text{TIME}(t) \subseteq \text{NTIME}(t)$
- (ii) $\text{SPACE}(t) \subseteq \text{NSPACE}(t)$
- (iii) $\text{NTIME}(s(n)) \subseteq \text{SPACE}(s(n)) \subseteq \bigcup_{c \in \mathbb{N}} \text{TIME}(c^{s(n)})$

Beweisskizze

Anzahl Transitionsmöglichkeiten beschränkt durch ein r . In t Schritten gibt es höchstens r^t mögliche Berechnungen.

Man kann auf einem zusätzlichen Band alle Entscheidungsketten durchiterieren. Für jede Entscheidungskette deterministisch simulieren.