Grundzüge der Theoretischen Informatik

7.1.2022

Markus Bläser

Universität des Saarlandes

Kapitel 21: Zeit versus Platz, Determinismus versus Nichtdeterminismus

Der Konfigurationsgraph

- Sei M eine TM.
- Der Konfigurationsgraph ist $\mathrm{CG}_M = (\mathrm{Conf}_M, \vdash_M)$.
  $(\vdash_M \subseteq \mathrm{Conf}_M \times \mathrm{Conf}_M)$
- CG_M ist gerichtet und unendlich.
- M akzeptiert x, falls es einen Pfad von $\mathrm{SC}_M(x)$ zu einer akzeptierenden Konfiguration gibt.
- Im Allgemeinen ist das unentscheidbar.

Lemma (21.3)

Sei M eine s-platzbeschränkte TM mit $s(n) \geq \log n$ für alle n. Dann gibt es eine Konstante c (abhängig von M), so dass M auf Eingabe x höchsten $c^{s(|x|)}$ Konfigurationen von $\mathrm{SC}(x)$ erreichen kann.

Graph $G = (V, E)$ (gerichtet)

V Knoten, $E \subseteq V \times V$ Kanten (E ist binäre Relation auf V)

$(u,v) \in E$ „es gibt eine Kante von u nach v“

$\overset{u}{\bullet} \longrightarrow \overset{v}{\bullet}$

gerichteter Pfad

$u_1, \dots, u_\ell$ mit $\forall\, 1 \le i < \ell$: $(u_i, u_{i+1}) \in E$

$\underset{u_1}{\bullet} \to \underset{u_2}{\bullet} \to \underset{u_3}{\bullet} \dots \to \underset{u_\ell}{\bullet}$

u_ℓ ist von u_1 erreichbar

G heißt ungerichtet wenn $\forall u, v \in V$ gilt:

$(u, v) \in E \Leftrightarrow (v, u) \in E$

Der Konfigurationsgraph (2)

Korollar (21.4)

Sei $s(n) \geq \log n$ für alle n. Wenn eine s-platzbeschränkte DTM auf x hält, dann kann sie höchstens $c^{s(|x|)}$ Schritte auf x machen.

Korollar (21.5)

Sei $s(n) \geq \log n$ platzkonstruierbar. $\mathrm{DSpace}(s)$ ist abgeschlossen unter Komplement, d.h. falls $L \in \mathrm{DSpace}(s)$, dann auch $\bar{L}$.

Bemerkung (21.6)

- Korollar 21.5 gilt trivialer Weise für deterministische Zeitklassen.
- Offen für nichtdeterministische Zeitklassen.
- Gilt nicht-trivialer Weise für nichtdeterministische Platzklassen. (Immerman-Szelepcsényi-Theorem)

Erreichbarkeit

Länge eines Pfades
= Anzahl der Kanten

Beobachtung (21.7)

Sei G ein Graph. Falls es einen Pfad der Länge ℓ von u nach v gibt, dann gibt es einen Knoten w und Pfade von u nach w und w nach v der Längen $\lceil \ell/2 \rceil$ bzw. $\lfloor \ell/2 \rfloor$.

Lemma (21.8)

Sei M eine s-platzbeschränkte TM, wobei $s(n) \geq \log n$ platzkonstruierbar ist. Dann gibt es

- *eine $2^{O(s(|x|))}$-zeitbeschränkte DTM M_1 und*
- *eine $O(s^2(|x|))$-platzbeschränkte DTM M_2,*

die auf Eingabe x entscheiden, ob eine akzeptierende Konfiguration von $SC_M(x)$ aus in CG_M erreichbar ist.

Beweis 21.8.

M_1 (zeitbeschränkt) / $c^{s(|x|)} = 2^{O(s(|x|))}$

- Zählt alle Konfigurationen auf, die $s(|x|)$ platzbeschränkt $\left(2^{O(s(|x|))}\right)$

im Sinne der O-Notation

$\left(\left(2^{O(s(|x|))}\right)^2 \text{"="} 2^{O(s(|x|))}\right)$

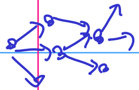
(C_1, C_2)

- Teste für alle Paare von Konfigurationen, ob $C_1 \vdash_M C_2$ $\Rightarrow$ alle Kanten des Konfigurationen $\left(2^{O(s(|x|))}\right)$

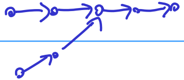
- Teste für jede akz. Konfiguration C, ob C von $SC(x)$ erreichbar ist.
z.B. Breitensuche $\left(2^{O(s(|x|))}\right)$ ✓

M_2

nichtdet



det.



$$R(C, C', \ell) = \begin{cases} 1 & \text{falls } C' \text{ von } C \text{ mit } \le \ell \text{ vielen Schritten erreicht werden kann} \\ 0 & \text{sonst} \end{cases}$$

Wir zeigen: Wir können $R(C, C', \ell)$ für alle $s(n)$-platzbeschr. C, C' und $\ell \le c^{s(n)}$ in Platz $O(s^2(n))$ ausrechnen

$R(C, C', \ell) = 1 \iff$
es gibt ein C'' mit $R(C, C'', \lceil \ell/2 \rceil) = 1$
und $R(C'', C', \lfloor \ell/2 \rfloor) = 1$ oder $C \vdash C'$.

Rekursiver Algorithmus

1. Falls $C \vdash C'$ gib 1 zurück
2. Sonst zähle alle Konfigurationen C'' auf und teste rekursiv, ob $R(C, C'', \lceil \ell/2 \rceil) = 1$ und $R(C'', C', \lfloor \ell/2 \rfloor) = 1$. Falls ja, gib 1 zurück
3. Sonst gib 0 zurück

Wie viel Platz braucht der Algorithmus?

Sei $S(\ell)$ der maximale Platzbedarf um $R(c, c', \ell)$ zu berechnen

Platz wird wiederverwendet

$$S(\ell) = S(\lceil \ell/2 \rceil) + \cancel{S(\lfloor \ell/2 \rfloor)} + \underline{O(s(n))}$$

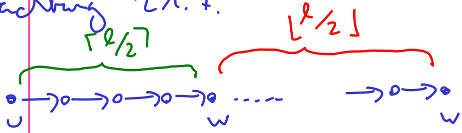
$$S(1) = O(s(n))$$

$$S(\ell) = O(s(n) \cdot \log \ell)$$

$$\ell \leq c^{s(n)} \Rightarrow \text{Platzbedarf } O(s^2(n))$$

✓

Beobachtung 21.7.



ℓ Kanten

$$\ell = \lceil \ell/2 \rceil + \lfloor \ell/2 \rfloor$$

"Auf jedem Pfad gibt es einen Knoten in der Mitte"

Platz versus Zeit, Nichtdeterminismus versus Determinismus

Theorem (21.10)

Sei $s(n) \geq \log(n)$ *platzkonstruierbar. Dann ist*

$$\mathrm{DSpace}(s) \subseteq \mathrm{NSpace}(s) \overset{M_1}{\subseteq} \mathrm{DTime}(2^{O(s)}).$$

Theorem (21.11)

Sei t *zeitkonstruierbar. Dann ist*

$$\mathrm{NTime}(t) \subseteq \mathrm{NSpace}(t) \overset{M_1}{\subseteq} \mathrm{DTime}(2^{O(t)}).$$

Theorem (Savitch, 21.12)

Sei $s(n) \geq \log n$ *platzkonstruierbar. Dann ist*

$$\mathrm{NSpace}(s) \overset{M_2}{\subseteq} \mathrm{DSpace}(O(s^2)).$$

Kapitel 22: P und NP

P und NP

„Probleme mit effizienten Algorithmus"

Definition (22.1)

$$P = \bigcup_{i \in \mathbb{N}} \mathrm{DTime}(O(n^i))$$

$$NP = \bigcup_{i \in \mathbb{N}} \mathrm{NTime}(O(n^i))$$

- P und NP sind robuste Klassen,
  d.h. unabhängig von konkreten Maschinenmodell.

$$NP = \bigcup_{i \in \mathbb{N}} \mathrm{NTime}(O(n^i)) \subseteq \bigcup_{i \in \mathbb{N}} \mathrm{DTime}(2^{O(n^i)}) =: EXP,$$

Probleme in P

$$s\text{-}t\text{-CONN} = \{(G, s, t) \mid \text{G ist ein gerichteter Graph der einen Pfad von } s \text{ nach } t \text{ hat}\}.$$

Theorem (22.2)

s-t-CONN $\in$ P.

Stärker gilt: s-t-CONN $\in$ NL := NSpace$(\log n)$

$$\text{NSpace}(O(\log n)) \subseteq \text{DTime}(2^{O(\log n)})$$
$$\subseteq \text{DTime}(p(n)), \; p \text{ Polynom}$$

NP und Zertifikate

Definition (22.3)

Eine polynomialzeit-beschränkte DTM M heißt *Polynomialzeit-Verifizierer* für $L \subseteq \{0,1\}^*$, falls es ein Polynom p gibt mit:

1. Für alle $x \in L$ gibt es ein $c \in \{0,1\}^*$ mit $|c| \leq p(|x|)$, so dass M das Paar $[x, c]$ akzeptiert.
2. Für alle $x \notin L$ und alle $c \in \{0,1\}^*$ liest M auf Eingabe $[x, c]$ höchstens $p(|x|)$ Bits von c und verwirft $[x, c]$ immer.

Die von M verifizierte Sprache L bezeichnen wir mit $V(M)$.

Theorem (22.4)

$L \in NP$ *genau dann wenn es einen Polynomialzeit-Verifizierer für* L *gibt.*

"$\Rightarrow$"

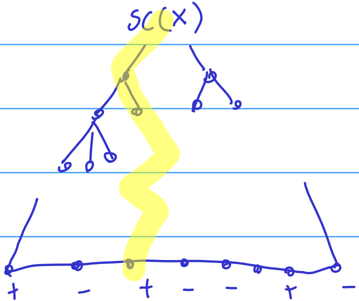
Sei $L \in NP$.

Es gibt eine NTM M mit $L(M) = L$

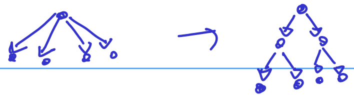
die $p(n)$-zeitbeschränkt ist für ein Polynom p.

Wir konstruieren einen Verifizierer V für L

Eingabe: $[x, c]$



O.E. hat M in jedem Schritt nur 2 nichtdet. Möglichkeiten.



V hat ein Band mehr als M

Auf dem Extraband markiert V $p(|x|)$ Zellen und kopiert die ersten $p(|x|)$ Bits von c dahin. V simuliert M schrittweise. Und in jedem Schritt benutzt V ein Bit vom Extraband, um den Schritt von M auszuwählen. V akz. gdw. M akz.

Wenn $x \in L$ ist, dann gibt es einen akz. Berechnungspfad von M auf x.
V akz. $[x, c]$, falls c einen akz. Berechnungspfad spezifiziert.

Wenn $x \notin L$, dann gibt es keinen akz. Berechnungspfad. Dann wird V niemals $[x, c]$ akz.

V ist polyzeit-beschränkt, weil nur ein Berechnungspfad von M simuliert wird.

✓