

THEORETISCHE GRUNDLAGEN DER INFORMATIK

TUTORIUM 11

WINTERSEMESTER 2013/14

MORITZ KLAMMLER

21. JANUAR 2014



Tagesthemen

- Fixed-Parameter-Tractability
- Complexity-Zoo
 - Counting Classes
 - Probabilistische Komplexitätsklassen
- Informationstheorie
 - Komprimierbarkeit (KOLMOGOROW-Komplexität)
 - Entropie (→ nächstes Mal)

Erratum

Sei Σ ein Alphabet und $A, B \subset \Sigma^*$. Falls $A \leq B$, sprechen wir

„ A ist **reduzierbar auf B** “.

Die Unterlagen werden demnächst konsistent korrigiert. Vielen Dank für den Hinweis.

Fixed-Parameter-Tractability

Sei Σ ein Alphabet und $L \subset \Sigma^*$ eine Sprache, sodass jedem $w \in \Sigma^*$ ein Parameter $k \in \mathbb{N}_0$ zugeordnet werden kann. L ist **fixed-parameter tractable** in k , genau dann wenn L von einer Turingmaschine entschieden werden kann, die für jedes $w \in \Sigma^*$ nach höchstens

$$\mathcal{O}(f(k)|w|^{\mathcal{O}(1)})$$

Berechnungsschritten hält, für eine berechenbare Funktion $f : \mathbb{N}_0 \rightarrow \mathbb{N}_0$.

Die Menge aller fixed-parameter tractablen Sprachen heißt \mathcal{FPT} .

Es ist *nicht* bekannt, dass k -CLIQUE fixed-parameter tractable in k ist. Sicher ist, dass

$$k\text{-CLIQUE} \in \mathcal{W}[1] \supseteq \mathcal{W}[0] = \mathcal{FPT} .$$

Zählende Turingmaschine

Eine **zählende Turingmaschine** ist eine nichtdeterministische Turingmaschine, deren Ausgabe die Anzahl der akzeptierenden Berechnungspfade ist.

Die Klasse $\#\mathcal{P}$ enthält alle Funktionen, die von einer zählenden Turingmaschine in höchstens polynomiell vielen Schritten berechnet werden können.

Randomisierte Turingmaschine

Eine **randomisierte Turingmaschine** (RTM) ist eine Turingmaschine, bei der für jede Eingabe eine der beiden folgenden Aussagen gilt.

- Es existiert kein akzeptierender Berechnungspfad.
- Mehr als die Hälfte der Berechnungspfade akzeptieren.

Bei einer Berechnung wird *gleichverteilt* einer der möglichen Pfade zufällig gewählt.

Die Klasse \mathcal{R}

Die Klasse \mathcal{R} enthält jede Sprache $L \subset \Sigma^*$, die von einer randomisierten Turingmaschine M , die für jede Eingabe $w \in \Sigma^*$ nach höchstens $\mathcal{O}(|w|^k)$ vielen Schritten (für konstantes $k \in \mathbb{N}_0$) hält, „entschieden“ werden kann.

$$\Pr [M(w)] \begin{cases} = 0, & w \notin L \\ > \frac{1}{2}, & w \in L \end{cases}$$

Viele Autoren nennen \mathcal{R} auch \mathcal{RP} .

$$\mathcal{P} \subseteq \mathcal{RP} \subseteq \mathcal{NP}$$

Die Klasse $\text{co-}\mathcal{R}$

Die Klasse $\text{co-}\mathcal{R}$ enthält jede Sprache $L \subset \Sigma^*$, deren Komplement L^C von einer randomisierten Turingmaschine M , die für jede Eingabe $w \in \Sigma^*$ nach höchstens $O(|w|^k)$ vielen Schritten (für konstantes $k \in \mathbb{N}_0$) hält, „entschieden“ werden kann.

$$\Pr [M(w)] \begin{cases} < \frac{1}{2}, & w \notin L \\ = 1, & w \in L \end{cases}$$

Viele Autoren nennen $\text{co-}\mathcal{R}$ auch $\text{co-}\mathcal{RP}$.

$$\text{co-}\mathcal{P} \subseteq \text{co-}\mathcal{RP} \subseteq \text{co-}\mathcal{NP}$$

Die Klasse ZPP

Die Klasse ZPP enthält jede Sprache $L \subset \Sigma^*$, die von einer Turingmaschine M , die „Zufall benutzen darf“, sicher entschieden werden kann, wobei M für Eingabe $w \in \Sigma^*$ nach *erwartet* $O(|w|^k)$ vielen Schritten (für konstantes $k \in \mathbb{N}_0$) hält.

$$M(w) \quad \Leftrightarrow \quad w \in L$$

Wir erlauben, dass M für manche Eingaben mehr als polynomiell viele Berechnungsschritte ausführt.

$$ZPP = \mathcal{R} \cup \text{co-}\mathcal{R}$$

Casino-Algorithmen

Algorithmen, die als Entscheider für \mathcal{R} -Sprachen taugen (garantiert polynomielle Laufzeit, beschränkter einseitiger Fehler), heißen **Monte-Carlo-Algorithmen**.

Algorithmen, die als Entscheider für \mathcal{ZPP} -Sprachen taugen (erwartet polynomielle Laufzeit, garantiert kein Fehler), heißen **Las-Vegas-Algorithmen**.

Probabilistische Turingmaschine

Eine **probabilistische Turingmaschine** (PTM) ist eine nichtdeterministische Turingmaschine, die eine Eingabe genau dann akzeptiert, wenn die Mehrheit der Berechnungspfade akzeptierend ist.

(Diese Definition ist meines Erachtens mit Bauchschmerz behaftet.)

Die Klasse \mathcal{PP}

Die Klasse \mathcal{PP} enthält jede Sprache $L \subset \Sigma^*$, die von einer probabilistischen Turingmaschine M , die für jede Eingabe $w \in \Sigma^*$ nach höchstens $O(|w|^k)$ vielen Schritten (für konstantes $k \in \mathbb{N}_0$) hält, mit Wahrscheinlichkeit größer $\frac{1}{2}$ erkannt werden kann.

$$\Pr [M(w)] \begin{cases} \leq \frac{1}{2}, & w \notin L \\ > \frac{1}{2}, & w \in L \end{cases}$$

Die Klasse \mathcal{BPP}

Die Klasse \mathcal{BPP} enthält jede Sprache $L \subset \Sigma^*$, die von einer probabilistischen Turingmaschine M , die für jede Eingabe $w \in \Sigma^*$ nach höchstens $O(|w|^k)$ vielen Schritten (für konstantes $k \in \mathbb{N}_0$) hält, mit Wahrscheinlichkeit größer $\frac{1}{2} + \epsilon$ (für konstantes $\epsilon > 0$) erkannt werden kann.

$$\Pr [M(w)] \begin{cases} \leq \frac{1}{2} - \epsilon, & w \notin L \\ > \frac{1}{2} + \epsilon, & w \in L \end{cases}$$

Zusammenfassung

```
hexdump -C /dev/urandom
```

```
00000000 f3 79 2e 86 25 f6 a6 ce 40 41 92 50 91 8c e8 b5 |.y..%...@A.P....|
00000010 30 b9 81 b3 7c 47 da 16 41 47 d1 45 f3 d7 cf d9 |0...|G..AG.E....|
00000020 8f 57 32 16 27 bb de 3a d9 6a e8 13 3f 28 6b b2 |.W2.'...:j..?(k.|
00000030 a4 64 a0 f8 28 9c 76 ef 24 5a 87 3a b5 49 36 71 |.d..(.v.$Z...I6q|
00000040 29 02 7a ac 76 3a 4d 83 54 3a 93 a9 5d d9 d4 c9 |).z.v:M.T:...]|
00000050 bc 59 68 e9 df c8 a9 f1 8e 1d 12 09 32 da 34 18 |.Yh.....2.4.|
00000060 b5 38 2e 9c 85 61 2f fb af 03 c7 ae 0d 42 1d 5e |.8...a/.....B.^|
00000070 43 f1 04 ea ca 19 54 d7 26 72 ec a0 bf 23 cb 40 |C....T.&r...#.@|
00000080 9b 54 ad d6 d2 f9 26 39 3e c2 b7 ec 44 5a 6e 80 |.T....&9>...DZn.|
00000090 73 94 98 1c ee d9 f9 dd 8f 65 7d 08 cc be df b6 |s.....e}.....|
000000a0 76 cd 73 a4 41 e2 55 c5 11 bb 0c 47 b0 6c 1c 38 |v.s.A.U....G.l.8|
000000b0 51 7c b1 fb 2b 43 1e bf 31 cb 2c 34 90 a8 8b 89 |Q|..+C..1.,4....|
000000c0 72 4d 61 d4 c4 8a 30 0a d1 3d 58 cf 68 64 21 a2 |rMa...0...=X.hd!.|
000000d0 64 0f db 1d ea 3c 60 4d 57 3b 95 61 d7 59 f7 71 |d....<'MW;.a.Y.q|
000000e0 a8 f5 44 52 16 4c fb 57 88 e3 29 72 40 c5 6a d5 |..DR.L.W..)r@.j.|
000000f0 44 6a af 69 0a b2 20 c7 8c be d0 f0 99 9b 4d b2 |Dj.i.. .....M.|
```