Institut für Informatik
Prof. Dr. J. Rothe

Sommersemester 2024
Übungsblatt 12

Lösungsvorschläge

Kryptokomplexität II

Bearbeitungszeit: 25. Juni bis 5. Juli
Verantwortlich: Roman Zorn

Aufgabe 1: Abschluss von PP unter $\leq_{\mathrm{m}}^{\mathrm{p}}$

▶ Zeigen Sie, dass PP unter $\leq_{\mathrm{m}}^{\mathrm{p}}$ abgeschlossen ist.

Lösungsvorschlag: Wir setzen voraus, dass $A \leq_{\mathrm{m}}^{\mathrm{p}} B$ via $f \in \mathrm{FP}$, wobei $B \in \mathrm{PP}$ mit NPTM M. Wir müssen zeigen, dass $A \in \mathrm{PP}$ gilt.

Wir konstruieren eine NPTM M' für A. Die NPTM M' arbeitet bei Eingabe x wie folgt: Führe $f(x)$ aus und simuliere M auf $f(x)$. Akzeptiere und lehne ab, genau wie M es tut.

Da f in deterministischer Polynomialzeit berechnet werden kann, verändern sich die Wahrscheinlichkeiten bei Berechnung von M nicht (Falls eine Normaliserung erwünscht ist, wird am Ende eines jeden Pfades von f die Maschine M simuliert. Die Wahrscheinlichkeiten ändern sich nicht). Somit

$$\begin{aligned} x \in A &\iff \Pr\left(\{\alpha \mid M' \text{ akzeptiert } x \text{ auf } \alpha\}\right) \geq \frac{1}{2} \\ &\iff \Pr\left(\{\alpha \mid M \text{ akzeptiert } f(x) \text{ auf } \alpha\}\right) \geq \frac{1}{2} \\ &\iff f(x) \in B. \end{aligned}$$

Aufgabe 2: Abschluss von RP unter $\leq_{\mathrm{m}}^{\mathrm{p}}$

▶ Zeigen Sie, dass RP unter $\leq_{\mathrm{m}}^{\mathrm{p}}$-Reduktion abgeschlossen ist.

Lösungsvorschlag: Wir setzen voraus, dass $A \leq_{\mathrm{m}}^{\mathrm{p}} B$ via $f \in \mathrm{FP}$. Wir müssen zeigen, dass $B \in \mathrm{RP} \Rightarrow A \in \mathrm{RP}$.

Sei M eine NPTM für B, d.h.

$$y \in B \Rightarrow \Pr\left(\{\alpha \mid M \text{ akzeptiert } y \text{ auf } \alpha\}\right) \geq \frac{1}{2}$$

und

$$y \notin B \Rightarrow \Pr\left(\{\alpha \mid M \text{ akzeptiert } y \text{ auf } \alpha\}\right) = 0.$$

Sei f die Polynomialzeitreduktion von A auf B. Wir konstruieren eine NPTM M' für A: für eine Eingabe x berechnet M' zunächst $f(x)$ und simuliert dann M, d.h. M' akzeptiert x genau dann, wenn M $f(x)$ akzeptieren würde (Da f deterministisch ist, ändert sich nichts an den Wahrscheinlichkeiten für die Akzeptanz, wie bei Aufgabe 1). Das bedeutet insbesondere

- $f(x) \in B \Rightarrow x \in A$, und deswegen

$$\Pr\left(\{\alpha \mid M \text{ akzeptiert } f(x) \text{ auf } \alpha\}\right) \geq \frac{1}{2}$$

$$\Rightarrow \Pr\left(\{\alpha \mid M' \text{ akzeptiert } x \text{ auf } \alpha\}\right) \geq \frac{1}{2},$$

- $f(x) \notin B \Rightarrow x \notin A$, und deswegen

$$\Pr\left(\{\alpha \mid M \text{ akzeptiert } f(x) \text{ auf } \alpha\}\right) = 0$$

$$\Rightarrow \Pr\left(\{\alpha \mid M' \text{ akzeptiert } x \text{ auf } \alpha\}\right) = 0.$$

Aufgabe 3: Abschluss von PP unter Komplementbildung

▶ Zeigen Sie (formal), dass PP = coPP gilt.

Lösungsvorschlag: Sei $L \in \text{PP}$ via einer NPTM M mit Laufzeit p, dessen Berechnungsbaum immer einen vollen Binärbaum bildet. Wir geben eine NPTM M' an, so dass für alle $x \in \Sigma^*$

$$x \notin L \iff \Pr\left(\{\alpha \mid M' \text{ akzeptiert } x \text{ auf } \alpha\}\right) \geq \frac{1}{2}.$$

Dazu spaltet sich am Anfang der Berechnung von M' der Berechnungsbaum in einen linken und einen rechten Teilbaum auf:

- Der linke Teilbaum simuliert die Berechnung von M mit der Eingabe.
  - Falls M auf einem Pfad akzeptiert, wird in den beiden Nachfolgern des Pfades abgelehnt (M' lehnt ab).
  - Falls M auf einem Pfad ablehnt, wird in den beiden Nachfolgern akzeptiert.

- Der rechte Teilbaum ist ein voller Binärbaum der Höhe $p(|x|)+1$. In der Hälfte der Blätter und einem zusätzlichen Blatt wird abgelehnt, in der anderen Hälfte abzüglich einem Blatt wird akzeptiert (z.B. abwechselnd akzeptieren und ablehnen und beim letzten Paar von Blättern ablehnen).

Da M einen vollen Binärbaum bildet, bildet auch M' einen vollen Binärbaum. Bezeichne mit

$$\mathrm{TOT}_M(x) = \{\alpha \mid \alpha \text{ ist ein Berechnungspfad in } M(x)\},$$

$$\mathrm{TOT}_{M'}(x) = \{\alpha \mid \alpha \text{ ist ein Berechnungspfad in } M'(x)\}$$

und mit

$$\mathrm{ACC}_M(x) = \{\alpha \mid M \text{ akzeptiert } x \text{ auf } \alpha\} \subseteq \mathrm{TOT}_M(x),$$
$$\mathrm{ACC}_{M'}(x) = \{\alpha \mid M' \text{ akzeptiert } x \text{ auf } \alpha\} \subseteq \mathrm{TOT}_{M'}(x).$$

Dann

$$|\mathrm{TOT}_{M'}(x)| = 4|\mathrm{TOT}_M(x)|$$

und M' akzeptiert, wenn M ablehnt, oder wenn es sich in einer der akzeptierenden Pfade des rechten Teilbaums befindet. Somit

$$|\mathrm{ACC}_{M'}(x)| = 2(|\mathrm{TOT}_M(x)| - |\mathrm{ACC}_M(x)|) + \frac{2|\mathrm{TOT}_M(x)|}{2} - 1.$$

$$\begin{aligned}\Pr\left(\mathrm{ACC}_{M'}(x)\right) &= \sum_{\alpha\in\mathrm{ACC}_{M'}(x)} \mu_T(\alpha) = \sum_{\alpha\in\mathrm{ACC}_{M'}(x)} 2^{-|\alpha|} = \frac{|\mathrm{ACC}_{M'}(x)|}{|\mathrm{TOT}_{M'}(x)|} \\ &= \frac{3|\mathrm{TOT}_M(x)| - 2|\mathrm{ACC}_M(x)| - 1}{4|\mathrm{TOT}_M(x)|} = \frac{3}{4} - \frac{1}{2}\frac{|\mathrm{ACC}_M(x)|}{|\mathrm{TOT}_M(x)|} - \frac{1}{4|\mathrm{TOT}_M(x)|}.\end{aligned}$$

Angenommen $x \notin L$. Zu zeigen ist, dass

$$\Pr\left(\mathrm{ACC}_{M'}(x)\right) \geq \frac{1}{2}$$

gilt. Nach Voraussetzung gilt dann

$$\Pr\left(\mathrm{ACC}_M(x)\right) < \frac{1}{2}.$$

Die Anzahl der akzeptierenden Pfade in $M(x)$ ist echt weniger als die Hälfte. Somit

$$\frac{|\mathrm{ACC}_M(x)|}{|\mathrm{TOT}_M(x)|} \leq \frac{2^{p(|x|)-1} - 1}{2^{p(|x|)}} = \frac{1}{2} - \frac{1}{2^{p(|x|)}}.$$

Insgesamt ergibt dies

$$\Pr\left(\mathrm{ACC}_{M'}(x)\right) \geq \frac{3}{4} - \frac{1}{2}\left(\frac{1}{2} - \frac{1}{2^{p(|x|)}}\right) - \frac{1}{2^{p(|x|)+2}} = \frac{1}{2} + \frac{1}{2^{p(|x|)+2}} \geq \frac{1}{2}.$$

Angenommen $x \in L$. Da M einen vollen Binärbaum bildet,

$$\Pr\left(\mathrm{ACC}_M(x)\right) = \frac{|\mathrm{ACC}_M(x)|}{|\mathrm{TOT}_M(x)|} \geq \frac{1}{2}.$$

Somit

$$\Pr\left(\mathrm{ACC}_{M'}(x)\right) = \frac{3}{4} - \frac{1}{2}\frac{|\mathrm{ACC}_M(x)|}{|\mathrm{TOT}_M(x)|} - \frac{1}{4|\mathrm{TOT}_M(x)|} \leq \frac{3}{4} - \frac{1}{4} - \frac{1}{4|\mathrm{TOT}_M(x)|} < \frac{1}{2}.$$

$\implies \overline{L} \in \mathrm{PP}$.

Also

$$L \in \mathrm{PP} \implies \overline{L} \in \mathrm{PP} \implies L \in \mathrm{coPP}$$

und

$$L \in \mathrm{coPP} \implies \overline{L} \in \mathrm{PP} \implies L \in \mathrm{PP}.$$

Aufgabe 4: Schwellwert-Klasse $\mathrm{RP}_{\mathrm{path}}$

► Wir nehmen an, dass der Verzweigungsgrad in einer NPTM maximal 2 ist. Für eine gegebene (nicht notwendigerweise normalisierte) NPTM M definieren wir

$$\mathrm{TOT}_M(x) = \{\alpha \mid \alpha \text{ ist ein Berechnungspfad in } M(x)\}$$

und

$$\mathrm{ACC}_M(x) = \{\alpha \mid M \text{ akzeptiert } x \text{ auf } \alpha\}.$$

Betrachten Sie die Klasse

$$\mathrm{RP}_{\mathrm{path}} = \left\{ A \;\middle|\; \begin{array}{l} \text{es gibt eine NPTM } M, \text{ so dass für jede Eingabe } x \text{ gilt:} \\ x \in A \implies |\mathrm{ACC}_M(x)| \geq 1/2 \cdot |\mathrm{TOT}_M(x)|; \\ x \notin A \implies |\mathrm{ACC}_M(x)| = 0 \end{array} \right\}.$$

Zeigen Sie

$$\mathrm{RP}_{\mathrm{path}} = \mathrm{NP}.$$

Lösungsvorschlag:

- $\mathrm{RP}_{\mathrm{path}} \subseteq \mathrm{NP}$:

  Sei $L \in \mathrm{RP}_{\mathrm{path}}$ via M. Wenn $x \in L$, dann

  $$|\mathrm{ACC}_M(x)| \geq 1/2 \cdot |\mathrm{TOT}_M(x)| \geq 1.$$

  Somit akzeptiert M im Sinne von NP. Wenn $x \notin L$, dann $|\mathrm{ACC}_M(x)| = 0$. Somit lehnt M auch im Sinne von NP ab.

- $\mathrm{NP} \subseteq \mathrm{RP}_{\mathrm{path}}$:

  Sei $L \in \mathrm{NP}$ via M mit Laufzeit p. M' simuliert M und fügt an akzeptierende Pfade jeweils einen rein akzeptierenden Teilbaum der Höhe $p(|x|) + 1$.

  Wenn $x \in L$, gilt

  $$|\mathrm{ACC}_{M'}(x)| = |\mathrm{ACC}_M(x)| \cdot 2^{p(|x|)+1}$$

  und

  $$\begin{aligned} |\mathrm{TOT}_{M'}(x)| &= |\mathrm{TOT}_M(x)| - |\mathrm{ACC}_M(x)| + |\mathrm{ACC}_M(x)|2^{p(|x|)+1} \leq \\ &\leq 2^{p(|x|)} - |\mathrm{ACC}_M(x)| + |\mathrm{ACC}_M(x)| \cdot 2^{p(|x|)+1} \leq \\ &\leq |\mathrm{ACC}_M(x)| \cdot 2^{p(|x|)+1} + |\mathrm{ACC}_M(x)| \cdot 2^{p(|x|)+1} = |\mathrm{ACC}_M(x)| \cdot 2^{p(|x|)+2}, \end{aligned}$$

  also insgesamt

  $$\frac{|\mathrm{ACC}_{M'}(x)|}{|\mathrm{TOT}_{M'}(x)|} \geq \frac{1}{2}.$$

  Wenn $x \notin L$, dann gibt es in M und somit in M' keine akzeptierenden Pfade.