Karlsruher Institut für Technologie

Maximilian Katzmann
Hans-Peter Lehmann
Stefan Walzer

Übungsblatt 08

Randomisierte Algorithmik – Wintersemester 2023/2024

Aufgaben zur Vorlesung vom 14.12.2023
Abgabe im ILIAS bis 21.12.2023, 11:30 Uhr
Besprechung am 16.01.2024, 08:00 Uhr
Achte insbesondere bei handschriftlichen Abgaben auf Lesbarkeit. Die Abgabe erfolgt über das Übungsmodul im ILIAS. Gib Deine Ausarbeitungen in *einer* PDF-Datei ab.

Aufgabe 1 – Beziehungen zwischen Komplexitätsklassen

Begründe folgende Inklusionen:

(i) **ZPP** $\subseteq$ **RP** und **ZPP** $\subseteq$ co–**RP**

(ii) **P** $\subseteq$ **ZPP**

(iii) **RP** $\subseteq$ **NP** und co–**RP** $\subseteq$ co–**NP**

(iv) **RP** $\subseteq$ **BPP** und co–**RP** $\subseteq$ **BPP**

(v) **BPP** $\subseteq$ **PP**

Aufgabe 2 – Las Vegas Algorithmus für L impliziert $L \in$ ZPP

Sei **LV** (für Las Vegas) die Klasse aller Sprachen L, für die eine probabilistische Turingmaschine T mit folgenden Eigenschaften existiert:

- T entscheidet L. (Das heißt L liefert für alle $x \in L$ stets die Ausgabe 1 und für alle $x \notin L$ stets die Ausgabe 0.)
- Es gibt ein Polynom $p(n)$, sodass die *erwartete* Laufzeit von T bei Eingabe x durch $p(|x|)$ beschränkt ist.

In der Vorlesung haben wir bewiesen, dass **ZPP** $\subseteq$ **LV** gilt. Zeige nun, dass auch **LV** $\subseteq$ **ZPP** gilt. die beiden Klassen sind also identisch.
Nützliche Zutaten: Definition von **ZPP**, Markov-Ungleichung.

Aufgabe 3 – Bonus: Probability Amplification für BPP

Sei T eine **BPP**-PTM für eine Sprache $L \subseteq \{0,1\}^*$. Betrachte die folgende PTM T':

```
1  Algorithm T'(w, k):
2      a ← 0
3      for i ← 1 to k do
4          r ← T(w)
5          if r = YES then
6              a ← a + 1
7      if a > k/2 then
8          return YES
9      else
10         return NO
```

(i) Zeige (z.B. mit Chernoff Schranken), dass die Wahrscheinlichkeit, dass T' inkorrekt antwortet, höchstens $\exp(-\Omega(k))$ ist.

(ii) Nehmen wir an, wir betrachten nur Eingaben einer festen Länge $n \in \mathbb{N}$. Wie muss man k in Abhängigkeit von n wählen, sodass die Wahrscheinlichkeit, dass T' für eine gegebene Eingabe inkorrekt antwortet, weniger als 2^{-n} beträgt? Argumentiere, dass es eine Wahl für die Zufallsbits von T' gibt, sodass T' auf *allen* Eingaben der Länge n korrekt antwortet.

(iii) Recherchiere auf Wikipedia, was es mit der Komplexitätsklasse **P/poly** auf sich hat. Zeige, dass **BPP** $\subseteq$ **P/poly** gilt. Diese Einsicht heißt auch Adlemans Satz.