

Übungsblatt 5 – Randomised Complexity Classes

Randomisierte Algorithmik

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.

Hinweis: Definition von ZPP , Markov-Ungleichung.

Aufgabe 3 – Bonus: Probability Amplification für BPP

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.

Hinweis: Mache die Fehlerwahrscheinlichkeit kleiner als 2^{-n} . „Caste“ die PTM dann in eine DTM und zeige, dass es einen Zufallsstrings gibt, der für alle Eingaben zum richtigen Ergebnis führt.