

Übungen zur Vorlesung
Komplexitätstheorie
Sommer 2015
Übungsblatt 11

Hinweis: Dies ist das letzte Übungsblatt. Für die Aufgaben zu probabilistischer Komplexität sind keine weiteren Vorkenntnisse notwendig als die, die in der Übung am 01.07. besprochen werden. Prüfungsrelevant ist jedoch das *ganze* Kapitel 21.

Aufgabe 11.1

In der Vorlesung (s. Konversion von Software zu Hardware) wurde gezeigt, dass jedes Element von P sich durch eine polynomielle Schaltkreisfamilie $C = (C_n)_{n \geq 0}$ berechnen lässt. Zeigen Sie, dass sich $desc(C_n)$ in $(\log n)$ -beschränkten Speicherplatz berechnen lässt. (D.h. die Familie $(C_n)_n$ ist uniform)

Aufgabe 11.2

Zeigen Sie, dass jede spärliche Sprache ein Element von $P_{/poly}$ ist.
Zeigen Sie dies direkt, d.h. ohne dabei Satz 20.11 anzuwenden.

Aufgabe 11.3

Zeigen Sie, dass sich ein Zufallszahlengenerator auf der Menge $\{1, \dots, N, ?\}$ durch eine PTM simulieren lässt, die folgendes erfüllt:

- Die PTM gibt stets ein Element aus $1, \dots, N, ?$ aus.
- Die Ausgabe des Zeichens $?$ erfolgt mit Wahrscheinlichkeit $\leq 1/2$.
- Sofern die Ausgabe nicht $?$ ist, gibt die PTM gleichverteilt ein Element aus $\{1, \dots, N\}$ aus.
- Die Laufzeit der PTM ist $O(\log N)$.

Aufgabe 11.4

Zeigen Sie, dass man einen Münzwurf mit $\Pr[\text{Kopf}] = p$ in erwarteter Zeit $O(1)$ von einer PTM berechnen lassen kann, vorausgesetzt, dass das i -te Bit von p in $poly(i)$ Zeit berechnet werden kann.