Theoretische Informatik II

Prof. Dr. Christoph Kreitz / Holger Arnold
Universität Potsdam, Theoretische Informatik, Sommersemester 2006

Übung 14 (Version 1)

Quiz 14

Markieren Sie die folgenden Aussagen als wahr (w) oder falsch (f).

[ ] Die Fehlerwahrscheinlichkeit eines RP-Algorithmus kann durch k-fache Wiederholung exponentiell in k verkleinert werden.

[ ] Sei M_k eine TM, die eine probabilistische TM M, deren Sprache in BPP liegt, k-mal simuliert (für ungerade k) und ein Wort w genau dann akzeptiert, wenn w von mehr als der Hälfte der Simulationen akzeptiert wird. Dann liegt die Sprache von M_k ebenfalls in BPP.

[ ] Eine Sprache L ist genau dann in RP, wenn es eine nichtdeterministische TM M gibt, so dass w von M nicht akzeptiert wird, wenn w nicht in L liegt und mindestens die Hälfte aller möglichen Berechnungspfade von M das Wort w akzeptieren, wenn w in L liegt.

Aufgabe 14.1

Beweisen Sie folgende Aussagen:

1. Eine Sprache L ist genau dann in RP, wenn es eine polynomielle probabilistische TM M und ein $c > 0$ gibt, so dass $P(M \text{ akzeptiert } w) = 0$ für alle $w \notin L$ und $P(M \text{ akzeptiert } w) \geq c$ für alle $w \in L$.
2. Eine Sprache $L \subseteq \Sigma^*$ ist genau dann in ZPP, wenn es eine polynomielle probabilistische TM M gibt, die eine Funktion f_M berechnet, so dass gilt: Wenn $x \in L$, dann ist $f_M(x) \in \{1, ?\}$ und $P(f_M(x) = 1) \geq 1/2$. Wenn $x \notin L$, dann ist $f_M(x) \in \{0, ?\}$ und $P(f_M(x) = 0) \geq 1/2$.

Aufgabe 14.2

1. Sei q ein Polynom in einer Variablen vom Grad d. Beweisen Sie durch Induktion über den Grad des Polynoms, dass q entweder das Nullpolynom ist oder q höchstens d Nullstellen besitzt.
2. Sei F ein endlicher Körper mit n Elementen (z.B. die Menge der Restklassen von $\mathbb{Z}$ modulo n für eine Primzahl n). Sei $(F^k, \mathcal{P}(F^k), P)$ ein Wahrscheinlichkeitsraum mit dem Wahrscheinlichkeitsmaß $P : \mathcal{P}(F^k) \to [0, 1]$ mit $P\{(x_1, \ldots, x_k)\} = n^{-k}$. Sei q ein Polynom in k Variablen, das nicht das Nullpolynom ist und das in jeder Variablen höchstens den Grad d besitzt. Sei $N_{k,q} : F^k \to \{0, 1\}$ eine Zufallsvariable mit

$$N_{k,q}(x_1, \ldots, x_k) = \begin{cases} 1 & \text{falls } q(x_1, \ldots, x_k) = 0, \\ 0 & \text{sonst .} \end{cases}$$

   Beschreiben Sie in Worten die Bedeutung des Ereignisses

$$(N_{k,q} = 1) = \bigcup_{x \in F^k, N_{k,q}(x)=1} \{x\}.$$

Beweisen Sie durch Induktion über die Anzahl der Variablen des Polynoms, dass $P(N_{k,q} = 1) \leq kd/n$ gilt. Wie groß muss n in Abhängigkeit von k und d mindestens gewählt werden, damit die Wahrscheinlichkeit, durch gleichverteilt zufällige Wahl eines Punktes aus F^k eine Nullstelle von q zu finden, höchstens $1/4$ beträgt?

3. Zeigen Sie, dass die Sprache

$$\{\langle q_1, q_2 \rangle \mid q_1 \text{ und } q_2 \text{ beschreiben äquivalente Polynome über } \mathbb{Z}\}$$

in coRP enthalten ist. Sie können dabei annehmen, dass ein Polynom über einem endlichen Körper in polynomieller Zeit ausgewertet werden kann.