Effiziente Algorithmen

Sommersemester 2019

Prof. Dr. Martin Hoefer
Dr. Daniel Schmand
Martin Ludwig, Conrad Schecker

GOETHE UNIVERSITÄT
FRANKFURT AM MAIN

Institut für Informatik
Algorithmen & Komplexität

Übung 12

Ausgabe: 09.07.2019
Abgabe: 16.07.2019, 10:15

Aufgabe 12.1. (3 Punkte)

Im ConsecutiveOne Problem ist ein Bitstring $x \in \{0,1\}^n$ gegeben. Die Frage ist, ob x zwei aufeinander folgende 1-er enthält.

Betrachte einen randomisierten Las-Vegas-Algorithmus A, der immer das korrekte Ergebnis liefert. Beweise mit Hilfe von Yao's Prinzip: A betrachtet im Erwartungswert mindestens $\Omega(n)$ Bits.

Aufgabe 12.2. (3 + 3 + 3 Punkte)

a) Wir haben in der Vorlesung folgenden (nicht polynomiellen) Test T benutzt: Sei G ein Generator mit Streckung $p(n)$. Sei

$$T = \begin{cases} 1 & x \text{ ist eine Ausgabe von } G \\ 0 & \text{sonst .} \end{cases}$$

Dann gilt, dass T Ausgaben von G mit Wahrscheinlichkeit 1 akzeptiert, d.h.

$$\Pr[T \text{ akzeptiert } G(x) \mid |x| = n] = 1 \, .$$

Zeige, dass

$$\Pr[T \text{ akzeptiert } y \mid |y| = p(n)] \leq 1/2 \, .$$

b) Sei $G : \{0,1\}^n \to \{0,1\}^{2n}$ ein Pseudo-Random Generator. Betrachte $G' : \{0,1\}^n \to \{0,1\}^{2n}$ mit $G'(x) \coloneqq \overline{G(x)}$, d.h., G' gibt die bitweise Negation von $G(x)$ aus. Zeige, dass G' auch ein Pseudo-Random Generator ist.

c) Seien $G_1, G_2 : \{0,1\}^n \to \{0,1\}^{2n}$ zwei Pseudo-Random Generatoren mit $G_1 \neq G_2$. Wir bezeichnen mit $G_1(x)|G_2(x)$ den Bitstring, der aus den hineinandergehängten Bitstrings $G_1(x)$ und $G_2(x)$ besteht.

Beweise oder widerlege: $G : \{0,1\}^n \to \{0,1\}^{4n}$ mit $G(x) \coloneqq G_1(x)|G_2(x)$ ist ein Pseudo-Random Generator.

Bitte wenden!

Aufgabe 12.3. (3 Punkte)

Betrachte $\mathbb{Z}_p^*$ mit p prim und $p = 2q + 1$, q prim. Zeige, dass ein zufälliges Element aus $\mathbb{Z}_p^*$ mit Wahrscheinlichkeit höchstens $\frac{q+1}{2q}$ kein Generator ist.

E-Mail: {mhoefer,schmand}@em.uni-frankfurt.de