Approximationsalgorithmen

Prof. Dr. Klaus Meer, Ameen Naif

Aufgabenblatt 5
Version 29.01.2020

Aufgabe 1.

Zeigen Sie, dass die 3. Phase der Definition eines (r, q)-Verifeires in der Vorlesung zu der folgenden Version äquivalent ist: "V berechnet deterministisch aus x und den gewählten Komponenten aus y ein Ergebnis aus $\{0, 1\}$".

Aufgabe 2.

Seien $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}_2^n$. Zeigen Sie folgendes:

(a) Falls $a = b$, dann gilt $a^T \cdot r = b^T \cdot r$ für alle $r \in \mathbb{Z}_2^n$

(b) Falls $a \neq b$, dann ist $Pr_{r \in \mathbb{Z}_2^n}(a^T \cdot r = b^T \cdot r) = \frac{1}{2}$.

Aufgabe 3.

(aus Motwani, Raghavan: Randomized Algorithms)
Als Abstandsmaß zwischen Funktionen $f, g : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2$ definieren wir wie in der Vorlesung $\Delta(f, g) := \Pr_x(f(x) \neq g(x))$.

(a) Zeigen Sie, dass $\Delta(f, g)$ tatsächlich eine Metrik ist, d.h. sie ist positiv definit, symmetrisch und erfüllt die Dreiecksungleichung.

(b) Für eine Funktionsfamilie $\mathcal{F} \subseteq \{f : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2\}$ sei $\Delta_{\min}(\mathcal{F})$ der minimale paarweise Abstand zwischen den Funktionen aus $\mathcal{F}$. Zeigen Sie, dass für jede beliebige Funktion g (nicht notwendig aus $\mathcal{F}$) höchstens ein $f \in \mathcal{F}$ existiert mit Abstand $\Delta(g, f) \leq \Delta_{\min}(\mathcal{F})/2$.

(c) Sei nun $\mathcal{F}$ die Menge der linearen Funktionen $\mathbb{Z}_2^n \mapsto \mathbb{Z}_2$. Wie groß ist $\Delta_{\min}(\mathcal{F})$?

Aufgabe 4.

Gegeben seien $a, b \in \mathbb{Z}_2^n$ und $c \in \mathbb{Z}_2^{n^2}$. Wie kann ein Verifier $c = a \circ b$ überprüfen, d.h. die eventuelle Ungleichheit mit hoher Wahrscheinlichkeit feststellen? Dabei stehen nur Auswertungen wie $a \cdot x$ zur Verfügung.