Hans U. Simon
Michael Kallweit

Bochum, den 01.07.2008
Abgabe bis 08.07.2008 um 10:00 Uhr

Übungen zur Vorlesung

Komplexitätstheorie

SS 2008

Blatt 11

Aufgabe 11.1

Zeige, dass ein $=(O(log(n)),2)$-beschränkter Verifizierer nicht mehr Rechenkraft besitzt als eine polynomialzeit-beschränkte deterministische Turingmaschine. D.h.

$$\mathrm{PCP}_{\mathrm{exact}}[O(log(n)),2] \subseteq \mathcal{P}$$

Aufgabe 11.2

Seien $N \in \mathbb{N}$ und X eine Menge mit $|X| = N$ beliebig. Zeige wie man mit polynomiell (in N) vielen Schritten eine Abbildung $T : X \to \{1, \ldots, N^5\}$ konstruieren kann, die folgendes leistet:

> Für zwei verschiedene Multiteilmengen von X der Größe 3, sagen wir $\{x_1, x_2, x_3\}$ und $\{y_1, y_2, y_3\}$ gilt:
>
> $$T(x_1) + T(x_2) + T(x_3) \neq T(y_1) + T(y_2) + T(y_3) \pmod{N^5}$$

Aufgabe 11.3

Vervollständige den Beweis der Nichtapproximierbarkeit von Min-Partition-Into-Cliques aus der Vorlesung: Zeige, dass alle Cliquen in G'_x nur Originalkanten verwenden. [Fall B bleibt noch zu zeigen]

Aufgabe 11.4

Beim Beweis von $\mathcal{NP} \subseteq \mathrm{PCP}_{n^{-\delta}}[log(n), log(n)]$ aus der Vorlesung wird vorausgesetzt, dass der Verifizierer einen fairen fünfseitigen Würfel und einen 5-regulären Expandergraphen der passenden Knotenanzahl zur Verfügung hat. Tatsächlich aber hat der Verifizier nur Random-bits (also eine Münze) zur Verfügung, und die gewünschten Expandergraphen gibt es nicht für jede mögliche Knotenanzahl.

Zeige, dass dies kein Problem darstellt, also der Verifizierer sich das Gewünschte beschaffen kann. [Hinweis: Verwende eine Chernoff-Schranke]

Anhang

Chernoff-Schranken (multiplikative Form)

Seien $X_1, \ldots, X_m$ eine Folge von m unabhängigen Bernoulli-Experimenten mit Erfolgswahrscheinlichkeit p. Dann gilt für jedes $0 \leq \gamma \leq 1$:

$$P\left[\sum_{i=1}^{m} X_i > (1+\gamma) \cdot p \cdot m\right] \leq e^{-m \cdot p \cdot \gamma^2/3}$$

und

$$P\left[\sum_{i=1}^{m} X_i < (1-\gamma) \cdot p \cdot m\right] \leq e^{-m \cdot p \cdot \gamma^2/2}$$