Hans U. Simon
Malte Darnstädt

Bochum, den 7.07.2010
Abgabe bis zum 14.07. in der Übung

Übungen zur Vorlesung

Komplexitätstheorie

Sommer 2010

Übungsblatt 10

Aufgabe 10.1

Wir untersuchen Veränderungen in der Definition von IP:

a) Sei IP' so wie IP definiert, außer dass die Wahrscheinlichkeit in der Soundness-Bedingung auf 0 gesetzt wird. Also: $x \notin L \Rightarrow \forall P \ \Pr[\text{out}_V\langle V, P\rangle(x) = 1] = 0$

   Zeige: IP' = NP

b) Sei IP' so wie IP definiert, außer dass die Wahrscheinlichkeit in der Completeness-Bedingung auf 1 gesetzt wird. Also: $x \in L \Rightarrow \exists P \ \Pr[\text{out}_V\langle V, P\rangle(x) = 1] = 1$

   Zeige: IP' = IP

Aufgabe 10.2

In der Definition von IP wird dem Beweiser unbegrenzte Rechenkraft zugestanden. Dies ist jedoch nicht nötig:
Zeige, dass für jeden Verifizierer V ein *optimaler Beweiser* existiert, dessen Antworten die Akzeptanzwahrscheinlichkeit von V maximieren und sich in polynomiellem Platz berechnen lassen. Folgere daraus: IP $\subseteq$ PSPACE

Aufgabe 10.3

Sei $k \leq n$ und $\mathbb{F}_2 = \{0, 1\}$ der Körper mit zwei Elementen. Für jede Matrix $A \in \mathbb{F}_2^{k \times n}$ und jeden Vektor $b \in \mathbb{F}_2^k$ betrachte die Abbildung $h_{A,b} : \mathbb{F}_2^n \to \mathbb{F}_2^k$ mit $h_{A,b}(x) = Ax + b$. Sei $\mathcal{H}_{n,k}$ die Menge aller $h_{A,b}$.
Zeige, dass $\mathcal{H}_{n,k}$ eine Familie paarweise unabhängiger Hashfunktionen von $\{0,1\}^n$ auf $\{0,1\}^k$ ist.

Aufgabe 10.4

Zeige, dass GRAPH-ISOMORPHISM selbstreduzierend ist.

GRAPH-ISOMORPHISM

Eingabe: Zwei ungerichtete Graphen $G = (V, E), G' = (V', E')$.
Frage: Sind die Graphen bis auf Umbenennung der Knoten identisch, d.h. existiert eine bijektive Abbildung $\pi : V \to V'$, so dass $\{u, v\} \in E$ genau dann wenn $\{\pi(u), \pi(v)\} \in E'$ gilt?