Übungsblatt 11

Abgabe der schriftlichen Lösungen bis 29. Januar 2013

Aufgabe 54 — *mündlich*

Eine Funktion f heißt *unbeschränkte und-Funktion* (kurz $\wedge$-*Funktion*) für eine Sprache $A \subseteq \Sigma^*$, falls für alle $x_1, \dots, x_k \in \Sigma^*$ gilt:

$$f(x_1\# \cdots \# x_k) \in A \quad \Leftrightarrow \quad \forall i = 1, \dots, k : x_i \in A.$$

Der Begriff der *unbeschränkten oder-Funktion* (kurz $\vee$-*Funktion*) ist analog definiert. f heißt *linear*, falls $|f(w)| = \mathcal{O}(|w|)$ ist. Zeigen Sie:

(a) Falls A eine lineare $\wedge_2$-Funktion (bzw. $\vee_2$-Funktion) in FP hat, so hat A auch eine $\wedge$-Funktion (bzw. $\vee$-Funktion) in FP.

(b) Sat, $\oplus$Sat und GI haben $\wedge$- und $\vee$-Funktionen in FP.

Aufgabe 55 — *mündlich*

Für zwei gegebene Graphen $G_i = (V, E_i)$, $i = 1, 2$, bezeichne UGI das Problem, zu entscheiden, ob zwischen G_1 und G_2 genau ein Isomorphismus existiert. Zeigen Sie:

(a) $\overline{\text{GA}} \leq_m^{log}$ UGI.

(b) UGI $\in \mathsf{P}_{\|}^{\text{GA}[3]}$. (*Bemerkung:* Es ist nicht bekannt, ob GI $\in \mathsf{P}^{\text{GA}}$ ist.)

(c) GI $\in \mathsf{SCW}$, d.h. GI hat selfcomputable witnesses.

(d) Für jedes Graphenpaar $(G_1, G_2) \in$ UGI lässt sich mit nichtadaptiven Orakelfragen an GA ein Isomorphismus in Polynomialzeit berechnen.

(e) GA $\leq_{dis}^{log}$ GI und GA $\leq_{dis}^{log}$ UGI.

(f) GA $\leq_m^{P}$ GI.

Aufgabe 56 — *mündlich*

Eine nichtdeterministische Orakel-Turingmaschine (NOTM) N heißt *strong* unter Orakel B, falls N^B bei jeder Eingabe x entweder mindestens eine akzeptierende oder mindestens eine verwerfende Rechnung ausführt, aber nicht beides. Eine NPOTM ist eine polynomiell zeitbeschränkte NOTM. Zeigen Sie:

$$\mathsf{NP}^B \cap \mathsf{co\text{-}NP}^B = \{L(N^B) \mid N \text{ ist eine NPOTM, die strong unter } B \text{ ist}\}.$$

Aufgabe 57 — Zeigen Sie: — *mündlich*

(a) Das Promise-Problem (1Sat, Sat) hat genau dann eine Lösung in BPP, wenn $\mathsf{NP} = \mathsf{RP}$ ist.

(b) USat ist in der Klasse $\mathsf{D}^p = \{A \setminus B \mid A, B \in \mathsf{NP}\}$ enthalten und hart für $\mathsf{UP} \cup \mathsf{co\text{-}NP}$.

(c) $\#\mathsf{P}^A = \#\mathsf{P} \Leftrightarrow A \in \mathsf{UP} \cap \mathsf{co\text{-}UP}$.

Aufgabe 58 — Zeigen Sie: — *mündlich*

(a) $\mathsf{BP} \cdot \mathsf{co\text{-}NP} \subseteq \mathsf{R} \cdot \mathsf{co\text{-}NP}$,

Hinweis: Modifizieren Sie den Beweis von $\mathsf{BP} \cdot \mathsf{co\text{-}NP} \subseteq \exists \cdot \mathsf{co\text{-}NP}$ (vgl. Satz von Lautemann).

(b) $\mathsf{BPP} \subseteq \mathsf{R} \cdot \mathsf{co\text{-}NP} \cap \mathsf{co\text{-}}(\mathsf{R} \cdot \mathsf{co\text{-}NP}) \subseteq \mathsf{ZPP}^{\mathsf{NP}}$.

Bemerkung: Es gilt sogar $\mathsf{NP}^{\mathsf{BPP}} \subseteq \mathsf{ZPP}^{\mathsf{NP}}$ (d.h. $\mathsf{NP} \subseteq \mathsf{BPP}$ impliziert $\mathsf{PH} = \mathsf{BPP}$).

Aufgabe 59 — *10 Punkte*

Eine Sprache $S \subseteq \Sigma^*$ heißt *sparse* (kurz $S \in \mathsf{SPARSE}$), falls für ein Polynom p und alle n gilt: $\|S \cap \Sigma^n\| \leq p(n)$. Sprachen $T \subseteq \{1\}^*$ heißen *tally* (kurz $T \in \mathsf{TALLY}$). Zeigen Sie:

$$\mathsf{P}/\text{poly} = \mathsf{P}(\mathsf{SPARSE}) = \mathsf{P}(\mathsf{TALLY}).$$