Übungsblatt 11

Abgabe der schriftlichen Lösungen bis 29. Januar 2009

Aufgabe 53 ***mündlich***

Zeigen Sie, dass die Varianz für paarweise stochastisch unabhängige Zufallsvariablen $X_1, \ldots, X_n$ additiv ist: $\mathrm{Var}(\sum_{i=1}^n X_i) = \sum_{i=1}^n \mathrm{Var}(X_i)$.

Aufgabe 54 ***mündlich***

Eine **k-Färbung** von $G = (V, E)$ ist eine Abbildung $c : V \to \{1, \ldots, k\}$. Ein Isomorphismus φ zwischen zwei gefärbten Graphen (G_1, c_1) und (G_2, c_2) darf einen Knoten u mit Farbe $c_1(u) = i$ nur auf Knoten v mit derselben Farbe $c_2(v) = i$ abbilden. Bezeichne ColGI das Graphenisomorphieproblem für gefärbte Graphen. Zeigen Sie:

(a) ColGI und GI sind logspace-äquivalent, d.h. es gilt ColGI $\equiv_m^{log}$ GI.
(b) Das Graphenisomorphieproblem für Bäume liegt in P.

Aufgabe 55 ***mündlich***

Eine NP-Sprache $A \subseteq \Sigma^*$ hat *selfcomputable witnesses* ($A \in \mathsf{SCW}$), falls ein Polynom p, eine p-balancierte Sprache $B \in \mathsf{P}$ und ein polynomiell zeitbeschränkter Orakeltransducer M existieren mit

- $A = \exists B$, d.h. $\forall x \in \Sigma^* : x \in A \Leftrightarrow \exists y \in \{0,1\}^{p(|x|)} : x\#y \in B$,
- für jede Eingabe $x \in A$ erzeugt M^A eine Ausgabe $M^A(x)$ der Länge $p(|x|)$ mit $x\#M^A(x) \in B$.

Wir sagen auch, M^A berechnet eine witness-Funktion für A (bzgl. B). Zeigen Sie:

(a) SAT $\in \mathsf{SCW}$.
(b) $\mathsf{NPC} \subseteq \mathsf{SCW}$, d.h. jede NP-vollständige Sprache besitzt *selfcomputable witnesses*.
(c) Jede Sprache $A \in \mathsf{PSK} \cap \mathsf{SCW}$ hat eine witness-Funktion in PSK, d.h. es existieren ein Polynom p, eine p-balancierte Sprache $B \in \mathsf{P}$ und eine Folge C_n von booleschen Schaltkreisen polynomieller Größe mit n Eingängen und $p(n)$ Ausgängen, so dass für alle n und alle $x \in A$ der Länge n gilt: $x\#C_n(x) \in B$.
(d) $\mathsf{NP}(\mathsf{NP}(\mathsf{PSK} \cap \mathsf{SCW})) = \mathsf{NP}(\mathsf{NP})$,
(e) SAT ist nicht in PSK enthalten, außer wenn PH auf Σ_2^p kollabiert.

Aufgabe 56 Zeigen Sie: ***mündlich***

(a) $\#\mathsf{P} \subseteq \mathsf{FP}(\mathsf{PP})$,
(b) $\oplus\mathsf{P} \subseteq \mathsf{P}(\mathsf{PP})$,
(c) $\oplus\mathsf{P}(\oplus\mathsf{P}) = \oplus \cdot \oplus \cdot \mathsf{P} = \oplus\mathsf{P}$,
(d) $\mathsf{BPP}(\mathsf{BPP}) = \mathsf{BP} \cdot \mathsf{BP} \cdot \mathsf{P} = \mathsf{BPP}$,
(e) $\mathsf{PP}(\mathsf{BPP}) = \mathsf{P} \cdot \mathsf{BP} \cdot \mathsf{P} = \mathsf{PP}$.

Aufgabe 57 ***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:

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