Übungsblatt 9

Abgabe der schriftlichen Lösungen bis 19. Januar 2017

Aufgabe 41 ***mündlich***

Sei $\rho \in [0,1]$ eine reelle Zahl. Eine ρ-PM ist eine PM mit maximalem Verzweigungsgrad 2, die eine ρ-Münze benutzt: Hat eine Konfiguration K zwei Folgekonfigurationen K' und K'', so gilt $\Pr[K \to_M K'] = \rho$ und $\Pr[K \to_M K''] = 1 - \rho$. Ersetzen wir in der Definition von PP, BPP, RP und ZPP PMs durch ρ-PMs, so führt dies auf die Klassen PP_ρ, BPP_ρ, RP_ρ und ZPP_ρ. Zeigen Sie:

(a) Für $\rho \in \{0,1\}$ gilt $\mathsf{PP}_\rho = \mathsf{BPP}_\rho = \mathsf{RP}_\rho = \mathsf{ZPP}_\rho = \mathsf{P}$.
(b) Für $\rho \in (0,1)$ kann jede PM M durch eine ρ-PM M' mit derselben Akzeptanzwahrscheinlichkeit in erwarteter Laufzeit $\mathcal{O}(\mathrm{time}_M(x))$ simuliert werden.
(c) Jede ρ-PM M kann durch eine PM M' mit derselben Akzeptanzwahrscheinlichkeit in erwarteter Laufzeit $\mathcal{O}(\mathrm{time}_M(x))$ simuliert werden, falls ρ P-berechenbar ist (d.h. das n-te Bit b_n der Binärrepresentation $0.b_1b_2\ldots$ von ρ ist in Zeit $n^{\mathcal{O}(1)}$ berechenbar).
(d) Für jedes P-berechenbare $\rho \in (0,1)$ gilt $\mathsf{BPP} = \mathsf{BPP}_\rho$ (entsprechend für RP und ZPP).
(e) Es gibt Zahlen $\rho \in (0,1)$ mit $\mathsf{PP} \neq \mathsf{PP}_\rho$ (sogar $\mathsf{PP}_\rho \not\subseteq \mathsf{RE}$).

Aufgabe 42 ***mündlich***

Zeigen Sie, dass aus $\mathsf{NP} \subseteq \mathsf{BPP}$ die Gleichheit $\mathsf{NP} = \mathsf{RP}$ folgt. (*Hinweis:* Benutzen Sie einen BPP-Algorithmus für Sat, um für eine gegebene Formel $F \in$ Sat mit hoher Wahrscheinlichkeit eine erfüllende Belegung zu finden.)

Aufgabe 43 ***10 Punkte***

Sei C unter $\leq_m^{log}$-Reduktionen abgeschlossen. Zeigen Sie:

(a) $\oplus \cdot \mathsf{C}$ ist unter $\leq_m^{log}$-Reduktionen abgeschlossen.
(b) $\oplus \cdot \mathsf{C}$ ist unter dem $\oplus$-Operator abgeschlossen, d.h. $\oplus \cdot \oplus \cdot \mathsf{C} = \oplus \cdot \mathsf{C}$.
(c) $\exists \cdot \mathsf{C}$ ist unter dem $\exists$-Operator abgeschlossen, d.h. $\exists \cdot \exists \cdot \mathsf{C} = \exists \cdot \mathsf{C}$.
(d) $\forall \cdot \mathsf{C}$ ist unter dem $\forall$-Operator abgeschlossen, d.h. $\forall \cdot \forall \cdot \mathsf{C} = \forall \cdot \mathsf{C}$.