Technische Universität München
Institut für Informatik
Lehrstuhl für Effiziente Algorithmen
Prof. Dr. Ernst W. Mayr

WS 2001/02
Übungsblatt 11
11. Januar 2002

Komplexitätstheorie

Abgabetermin: Freitag, 18. Januar 2002, in der Vorlesung

Aufgabe 1

Zeigen Sie den folgenden Satz aus Abschnitt 5.8 der Vorlesung: Die Anzahl $Z(n, b)$ der Booleschen Funktionen, die von $\{0,1\}^n$ nach $\{0,1\}$ abbilden und von Schaltkreisen mit höchstens b Gattern (aus B_2) berechnet werden können, ist nach oben beschränkt durch

$$\frac{(b+n+1)^{2b} \times 16 \times b}{b!}.$$

Aufgabe 2

Die Funktion f_{Fac} sei wie folgt definiert:

$$\begin{aligned} f_{\mathrm{Fac}} : \mathbf{N} &\to \Sigma^* \\ x &\mapsto (x_1, e_1, \ldots, x_n, e_n), \text{ wobei } x = \textstyle\prod_{i=1,\ldots,n} x_i^{e_i},\ x_1, \ldots, x_n \text{ prim}, \\ &\qquad x_1 < \ldots < x_n,\ e_1, \ldots, e_n \in \mathbf{N}. \end{aligned}$$

f_{Fac} berechnet also die Primfaktorisierung einer gegebenen Zahl x.
Weiter definiert man die Sprache FACTORING wie folgt:

$$\text{FACTORING} = \{\langle x, y\rangle \mid \exists z : yz \text{ stellt einen Primfaktor von } x \text{ dar.}\}$$

Dabei bezeichnet yz die Zahl, die sich durch Aneinanderhängen der beiden Strings y und z ergibt. Zeigen Sie:

1. $f_{\mathrm{Fac}} \in$ PF(FACTORING).

2. FACTORING $\in \mathcal{NP} \cap \mathrm{co}-\mathcal{NP}$.

Hinweise:

1. PF(FACTORING) ist, wie in der Vorlesung definiert, die Menge aller Funktionen, die sich in polynomieller Zeit mit Hilfe der Sprache FACTORING als Orakel berechnen lassen.

2. Erinnern Sie sich an die in der Vorlesung gezeigte Tatsache, dass PRIMES in $\mathcal{NP}$ liegt, d.h. dass für jede Primzahl x ein polynomiell langes Zertifikat y existiert, das die Primalität von x nachweist.

Aufgabe 3

Zeigen Sie, dass für alle $\mathrm{L} \subseteq \Sigma^*$ folgende Aussagen äquivalent sind:

1. $\mathrm{L} \in \mathrm{BPP}$
2. Es existiert ein Polynom p mit $p(n) > 2$ für alle $n \in \mathbf{N}$ und eine probabilistische Turingmaschine M, so dass für alle $x \in \{0,1\}^*$ gilt:
   (a) $x \in L \Longrightarrow Pr(M \text{ akzeptiert } x) \geq \frac{1}{2} + \frac{1}{p(|x|)}$.
   (b) $x \notin L \Longrightarrow Pr(M \text{ verwirft } x) \geq \frac{1}{2} + \frac{1}{p(|x|)}$.

Hinweis: Verwenden Sie wie schon in der Vorlesung das 'Majority-Vote-Verfahren' (d.h., man lässt die probabilistische Turingmaschine mehrmals laufen und entscheidet am Ende so, wie die Mehrzahl der Antworten war) und schätzen Sie die Wahrscheinlichkeiten möglichst genau ab, z.B. mit der Ungleichung von Chernoff.

Aufgabe 4

Sei ϵ eine rationale Zahl mit $0 < \epsilon < 1$. Die Komplexitätsklasse PP_ϵ sei definiert als die Klasse aller Sprachen $L \subseteq \Sigma^*$, für die eine probabilistische Turingmaschine M existiert mit:

1. $x \in \mathrm{L} \Longrightarrow$ mehr als der Bruchteil ϵ aller Pfade von M akzeptieren x,
2. $x \notin \mathrm{L} \Longrightarrow$ weniger als der Bruchteil ϵ aller Pfade von M akzeptieren x.

Zeigen Sie, dass $\mathrm{PP}_\epsilon = \mathrm{PP}$.