Komplexitätstheorie

Sommersemester 2013

Prof. Dr. Georg Schnitger,
Dipl. Inf. Bert Besser

Arbeitsgruppe Theoretische Informatik, Institut für Informatik

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Blatt 8

Ausgabe: 26.06.2012
Abgabe: 03.07.2012

8.1. Aufgabe (12)

Schaltkreise polynomieller Größe sind „mächtig“!

Definition BPP *ist die Klasse der Sprachen, die von einem randomisierten Algorithmus mit einem beidseitig durch* $\frac{1}{4}$ *beschränkten Fehler in polynomieller worst-case Zeit erkannt werden.*

Zeige BPP $\subseteq$ P/poly.

Hinweis: Sei B ein randomisierter Algorithmus mit einem beidseitig durch $\frac{1}{4}$ beschränkten Fehler und polynomieller worst-case Laufzeit. Wir fixieren eine beliebige Eingabelänge n. Existiert eine polynomiell in n große Menge von Bitstrings, die als “Zufallsquellen” von B für eine deterministische Mehrheitsentscheidung genutzt werden kann?

8.2. Aufgabe (12)

Sind Schaltkreise polynomieller Größe „schwach“?

Definition *Für* $k \geq 1$ *definiere*

$$\Sigma_k = \{L : w \in L \iff \exists^p x_1 \forall^p x_2 \ldots Q_k^p x_k \; f(w, x_1, x_2, \ldots, x_k)\} \text{ und}$$
$$\Pi_k = \{L : w \in L \iff \forall^p x_1 \exists^p x_2 \ldots Q_k^p x_k \; f(w, x_1, x_2, \ldots, x_k)\},$$

wobei $Q_k^p \in \{\exists^p, \forall^p\}$ *und die Quantoren sich abwechseln, alle Bitstrings* x_i *polynomielle Länge in* $|w|$ *haben und* f *eine in deterministischer Polynomialzeit berechenbare Funktion ist. Die* polynomielle Hierarchie *ist* $\text{PH} = \bigcup_{k \geq 1} \Sigma_k$.

Bemerkung Es gelten die Aussagen $\Sigma_1 = \text{NP}$, $\Pi_k = \text{co}\Sigma_k$, PH $\subseteq$ PSPACE und

$$\Pi_k \subseteq \Sigma_k \Rightarrow \Sigma_k \subseteq \Pi_k \Rightarrow \Pi_k = \Sigma_k \Rightarrow \Sigma_{k+1} \subseteq \Sigma_k \Rightarrow \Sigma_k = \Sigma_{k+1} = \Pi_{k+1} \Rightarrow \text{PH} = \Sigma_k,$$

zum Beispiel NP $\subseteq$ P $\Rightarrow$ NP = P $\Rightarrow$ coNP = coP = P = NP $\Rightarrow \Sigma_1 = \Pi_1 \Rightarrow$ PH = P.

Folklore Es wird angenommen, dass es kein k mit $\Sigma_k = \Pi_k$ gibt, dass also PH nicht *kollabiert.*

Zeige das Theorem von Karp-Lipton, d.h. die Implikation $\mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow \Pi_2 \subseteq \Sigma_2$.

Hinweis: Zeige zuerst, dass aus der Existenz eines P/poly-Schaltkreises für das SAT-Problem, also die Frage $\exists^p x\ \phi(x)$ für eine Formel ϕ, die Existenz eines P/poly-Schaltkreises S zur Konstruktion einer erfüllenden Belegung x von ϕ folgt.

Natürlich kann man S mit einem $\exists^p$-Quantor raten, aber wie verifiziert man, dass S tatsächlich das SAT-Problem löst? Zeige, dass das Verifikationsproblem in Π_1 liegt.