Prof. Martin Hofmann
Steffen Jost

Ludwig-Maximilians-Universität München
Institut für Informatik

Wintersemester 2002/03
30. Januar 2003

Übung 12

Komplexitätstheorie

Aufgabe G40 (Die Klasse PP): ¶

> "In some very real sense, computation is inherently randomized. It can be argued that the probability that a computer will be destroyed by a meteorite during any given microsecond of its operation is at least 2^{-100}." *C.H.Papadimitriou*

a) Beweise, dass PP unter Komplementbildung abgeschlossen ist.

b) Beweise: NP $\subseteq$ PP.

c) Eine Sprache gehöhre zu der Klasse PP_ϵ, falls es eine probabilistische Turing Maschine gibt, die Wörter dieser Sprache mit Wahrscheinlichkeit größer als ϵ akzeptiert und alle anderen Wörter nur mit Wahrscheinlichkeit kleiner oder gleich ϵ akzeptiert. Es gilt also $\mathrm{PP}_{\frac{1}{2}} = \mathrm{PP}$.

   Zeige, dass $\mathrm{PP}_{\frac{1}{4}} = \mathrm{PP}_{\frac{1}{2}} = \mathrm{PP}_{\frac{3}{4}}$ gilt.

d) Beweise: BPP $\subseteq$ PP.

   Hinweis: Falls eine Sprache von einer BPP-Turing Maschine erkannt wird, so kann man diese auch als PP-Turing Maschine interpretieren.

   Diskutiere nocheinmal den Unterschied der beiden Klassen!

¶Zur Erinnerung:

- PP steht für "probabilistic polynomial time"
- BPP steht für "bounded-error probabilistic polynomial time"

Aufgabe G41 (Interactive Proof Systems):

a) Beweise, dass IP unter polynomiellen Reduktionen abgeschlossen ist.

b) Beweise die Inklusion NP $\subseteq$ IP.

c) Skizziere den Beweis, dass IP $\subseteq$ PSPACE gilt.

   Bemerkung: IP = PSPACE wurde 1992 von A. Shamir bewiesen.

d) Ein *Arthur-Merlin interaktives Beweissystem* ist ein interaktives Beweissystem, bei dem der Verifier lediglich Auskunft über das Ergebnis seiner Zufallsexperimente (Münzwürfe) erteilt.

   Zeige, dass das in der Vorlesung vorgestellte Graphenisomorphieproblem mit einem Arthur-Merlin System gelöst werden kann!

   Bemerkung: Man kann sogar allgemein zeigen, das beide Systeme die gleiche Stärke besitzen.

Aufgabe G42: Eine Sprache A heiße *per Orakel beweisbar*, falls es eine polynomial zeitbeschränkte, probabilistische Orakel Turing Maschine M gibt, so dass für alle x gilt:

$$x \in A \implies \exists B.\ M^B(x) \text{ akzeptiert mit Wahrscheinlichkeit} > \tfrac{2}{3}$$
$$x \notin A \implies \forall B.\ M^B(x) \text{ akzeptiert mit Wahrscheinlichkeit} < \tfrac{1}{3}$$

a) Zeige: $A \in$ IP impliziert, dass A per Orakel beweisbar ist!

b) Diskutiere weiterhin warum die Umkehrung möglicherweise nicht gilt!