Prof. Martin Hofmann
Steffen Jost

Ludwig-Maximilians-Universität München
Institut für Informatik

Wintersemester 2002/03
6. Februar 2003

Übung 13

Komplexitätstheorie

Aufgabe G43 (coNP $\subseteq$ IP): Wir wollen nocheinmal den Beweis coNP $\subseteq$ IP aus der Vorlesung nachvollziehen. Dazu wollen wir uns zuerst nocheinmal die im Beweis verwendete Arithmetisierung Boolescher Formeln ins Gedächtnis rufen.

a) Arithmetisiere folgende Formeln, so wie in der Vorlesung angegeben:

$$(1)\quad x \wedge (\neg x \vee y) \wedge \neg y \qquad\qquad (2)\quad (x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z)$$

Der in der Vorlesung behandelte Beweis[†] bestand nun in der Angabe eines interaktiven Beweissystems für $\overline{\text{3SAT}}$. Da $\overline{\text{3SAT}}$ ein coNP-vollständiges Problem ist, folgt somit schon die Behauptung coNP $\subseteq$ IP.

b) Simuliere dieses interaktive Beweissystem für beide in a) angegebenen Formeln von Hand. Um die Berechnung von Hand zu vereinfachen nehmen wir dabei an, dass die Primzahl p groß genug gewählt wurde.

   Versuche bei der Simulation für Eingabeformel (2) einmal den Verifier durch geschickte Antworten des Provers auszutricksen, so dass dieser die Eingabe akzeptiert, obwohl Formel (2) erfüllbar, also nicht in $\overline{\text{3SAT}}$ ist.

c) Neben der polynomiellen Laufzeit des Verifiers mußte natürlich auch noch die Korrektheit dieses interaktiven Beweissystems gezeigt werden. Dazu benötigten wir folgende Aussage:

   > Wenn f eine erfüllbare Formel ist, der Algorithmus die i-te Runde erreicht hat und $b_{i-1} = g'_i(0) + g'_i(1)$ gilt, dann ist die Wahrscheinlichkeit, dass g'_i ungleich g_i ist, größer als $\left(1 - \frac{3m}{p}\right)^i$.

   wobei g'_i das i-te vom Prover gesendete Polynom, g_i das vom Verifier berechnete, teilweise ausgewertete Polynom, also $g_i(x) := A^i_f(r_1, \ldots, r_{i-1}, x)$, r_i die i-te vom Verifier ermittelte Zufallsvariable und b_i den Wert $g'_i(r_i)$ bezeichnet.

   Beweise diese Aussage mit Induktion über i.

   Bemerkung: Wenn $g'_i \neq g_i$ gilt, dann hat der Prover geschummelt. Der Verifier muß in der Lage sein, dies mit Wahrscheinlichkeit größer $\frac{2}{3}$ zu bemerken.

[†] Theorem 10.2