Prof. Martin Hofmann
Steffen Jost

Ludwig-Maximilians-Universität München
Institut für Informatik

Wintersemester 2002/03
7. Februar 2003

Lösungsvorschläge zur 13. Übung

# Komplexitätstheorie

**Lösung zu G43:**

a) Der Einfachheit wegen benennen wir die Variablen im Polynom genauso wie die korrespondierenden booleschen Variablen:

$$\text{(1)}\quad \big(1-(1-x)\big)\big(1-(x)(1-y)\big)\big(1-y\big) = x - x^2 - xy + 2x^2y + x^2y^2$$
$$\text{(2)}\quad \big(1-(1-x)(1-y)(1-z)\big)\big(1-xyz\big) = x + y + z - xy - xz - yz + xyz - x^2yz - xy^2z - xyz^2 + x^2y^2z + x^2yz^2 + xy^2z^2 - x^2y^2z^2$$

b) Wie in der Aufgabenstellung geschrieben, ignorieren wir momentan einmal das wir eigentlich modulo einer Primzahl $p$ rechnen:

(1) Die Eingabeformel ist offensichtlich unerfüllbar, d.h. wir wollen uns hier davon überzeugen, das der Prover den Verifier auch tatsächlich mit hoher Wahrscheinlichkeit überzeugen kann.
Betrachten wir nun die Kommunikation zwischen Verifier und Prover:

| **Prover** sendet | **Verifier** prüft | rät | sendet |
|---|---|---|---|
| $g'_0(x) = x - x^2$ | $g'_0(0) + g'_0(1) = 0$ | 14 | 14 |
| $g'_1(y) = -196y^2 + 378y - 182$ | $g'_1(0) + g'_1(1) = g'_0(14) = -182$ | 27 | |
| | $g'_1(27) = A_f(14, 27)$ | | |

wobei der Verifier bei einem negativen Prüfergebnis sofort mit Ablehnung der Eingabe abbricht.
Es bleibt zu bemerken, dass gültige Eingaben unter Verwendung eines vernünftigen Provers mit Wahrscheinlichkeit 1 akzeptiert werden.

(2) In diesem Fall versuchen wir einmal den Verifier hereinzulegen, den die Eingabeformel ist offensichtlich unerfüllbar und sollte daher vom Verifier mit hoher Wahrscheinlichkeit abgelehnt werden.

| **Prover** sendet | **Verifier** prüft | rät | sendet |
|---|---|---|---|
| $g'_0(x) = x - x^2$ | $g'_0(0) + g'_0(1) = 0$ | 3 | 3 |
| $g'_1(y) = -6y$ | $g'_1(0) + g'_1(1) = g'_0(3) = -6$ | 4 | 4 |
| $g'_2(z) = -24z$ | $g'_2(0) + g'_2(1) = g'_1(4) = -24$ | 5 | |
| | $g'_2(5) = A_f(3, 4, 5)$ | | |

was schließlich den schummelnden Prover entlarvt, denn

$$-1475 = A_f(3,4,5) \neq g_2'(5) = -120$$

Sämtliche vom Prover übermittelte Polynome waren 'falsch', z.B.:

$$-6y = g_1'(y) \neq A_f(3,y,0) + A_f(3,y,1) = 4 - y$$

c) Dies wird im Buch, Seite, 212, ausführlich behandelt. Es sei angemerkt, dass der Beweis natürlich sämtliche Prover berücksichtigen muß, die den Verifier hereinlegen könnten.

In jedem Fall kann der Prover im ersten Schritt nicht das richtige Polynom übermitteln, da im Falle einer erfüllbaren Formel ja gerade $g_0(0) + g_0(1) \neq 0$ gilt.

Desweiteren sind $g_i$ und $g_i'$ beides Polynome in einer Variablen vom Grad kleiner oder gleich $3m$. Wenn die Polynome verschieden sind, können diese also höchstens an $3m$ Stützstellen übereinstimmen, bzw. sind in einem Körper mit $p$ Elementen an $p - 3m$ Stellen verschieden. Somit liegt die Wahrscheinlichkeit, eine gemeinsame Stützstelle zu raten bei $\frac{p-3m}{p} = 1 - \frac{3m}{p}$.

Nach der Induktionshypothese sind mit Wahrscheinlichkeit $\left(1 - \frac{3m}{p}\right)^{i-1}$ die vorangegangenen Tests des Verifiers geglückt und $g_j \neq g_j'$ für $j < i$. Die Wahrscheinlichkeit, das der aktuelle Test glückt, liegt damit bei $\left(1 - \frac{3m}{p}\right)^{i}$, völlig unabhängig von der Strategie des schummelden Provers.