Eidgenössische Technische Hochschule Zürich
Ecole polytechnique fédérale de Zurich
Politecnico federale di Zurigo
Swiss Federal Institute of Technology Zurich

*Institut für Theoretische Informatik*
*Emo Welzl, Jiří Matoušek*

23.06.2005

# *Theoretische Informatik (Kernfach)* *SS 2005*
## *Exercise Set 11*

### Exercise 1

First recall the definition of the class NP as described in the lecture notes on page 47.

Prove the following two statements:

(a) $\mathrm{PCP}(0, \mathrm{poly}(n)) = \mathrm{NP}$, and

(b) $\mathrm{PCP}(\log(n), \mathrm{poly}(n)) = \mathrm{NP}$.

### Exercise 2

A quadratic polynomial $p$ in $n$ variables over $\mathrm{GF}(2)$ can be written as $p(x_1, \ldots, x_n) = a_0 + \sum_{i,j=1}^{n} a_{ij} x_i x_j$, with $a_0$ and $a_{ij} \in \mathrm{GF}(2)$. The problem QP-SAT (satisfiability of quadratic polynomials) is defined as follows:

Given a collection $p_1(x_1, \ldots, x_n), p_2(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)$ of $n$-variate quadratic polynomials over $\mathrm{GF}(2)$, do there exist $x_1, x_2, \ldots, x_n \in \mathrm{GF}(2)$ with $p_i(x_1, \ldots, x_n) = 0$ for all $i \in \{1, \ldots, m\}$? (That is, do these polynomials have a common root?)

Show that the problem QP-SAT is NP-complete (this is Fact 6.5.1 in the lecture notes). In a possible proof you reduce 3SAT to QP-SAT. Thus, you have to show that for any 3CNF formula $\psi$ you can in polynomial time generate a collection of quadratic polynomials that have a common root if and only if $\psi$ is satisfiable. Exercises (a)-(c) provide a short guideline.

(a) For the clause $C = x_1 \vee \bar{x}_2 \vee x_3$ find a polynomial $p_C(x_1, x_2, x_3)$ (not necessarely of degree two) such that for $x_1, x_2$ and $x_3$, $p_C(x_1, x_2, x_3)$ evaluates to zero if and only if $C$ is satisfied.

(b) Replace $p_C(x_1, x_2, x_3)$ by two polynomials $q_C(x_1, x_2, x_3, y)$ and $r_C(x_1, x_2, x_3, y)$ of degree at most two and with one additional variable $y$.

(c) Generalize this idea for any clause of length three and finally construct, for a given 3CNF formula $\psi$, a collection of quadratic polynomials such that they have a common root if and only if $\psi$ is satisfiable.

**Due-date:** 30.06.05 in the lecture