McGill University COMP531 Winter 2010 **Instructor: Phuong Nguyen**

Assignment 4

Due April 7 in lecture

The work you submit must be your own. You may discuss problems with each others; however, you should prepare written solutions alone. Copying assignments is a serious academic offense, and will be dealt with accordingly.

(It is helpful to give a high level description of a proof or an algorithm before giving the details.)

Question 1 (10pt) Find the smallest size of a DNF (disjunctive normal form) formula $F(x_1, x_2, \ldots, x_n)$ that computes $Parity(x_1, x_2, \ldots, x_n)$ (i.e., $F(x_1, x_2, \ldots, x_n)$ is true if and only if there are an odd number of x_i that are 1). Here the size of a formula is defined to be the total number of *literals* appearing in the formula. Prove your result, and give explicitly a DNF formula of the smallest size you find that computes Parity.

Similarly, find the smallest size of a CNF (conjunctive normal form) formula that computes the Parity function. Prove your result and give explicitly a CNF formula of the size you find that computes Parity.

Question 2 (10pt) In this question we consider circuits that have only $\wedge$- and $\vee$-gates and that take inputs from $x_1, x_2, \ldots, x_n, \neg x_1, \neg x_2, \ldots, \neg x_n$. In other words, we disregard the $\neg$-gates by pushing them to the input layers. The depth of such a circuit is the total number of its layers. For example, CNF and DNF formulas are depth 2 circuits.

Show that there is a depth 3 circuits of size $\mathcal{O}(\sqrt{n}2^{\sqrt{n}})$ that computes Parity. (Note the lower bound we get from Håstad's Switching Lemma is $\Omega(n^{\Omega(n^{1/3})})$.)

Question 3 (10pt) This question is to test your understanding of the proof of Razborov–Smolensky Theorem. Prove (directly) that Parity is not in $\mathbf{AC}^0(5)$. Justify every step.

Question 4 (10pt) For this question you can use the following facts:

- The Law of Quadratic Reciprocity states that for odd number m, n such that $gcd(m, n) = 1$:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}$$

- For odd n, the equation

$$x^2 = 2 \mod n$$

  has solution if and only if $n \mod 8 = \pm 1$.

Show that the Jacobi symbol $\left(\frac{m}{n}\right)$ can be computed in time polynomial in the size of the inputs (i.e., polynomial in $\log(n)\log(m)$).

Question 5 (10pt) This question refers to the Polynomial Identity Testing problem in Section 7.2.3 in the text book.

An *algebraic circuit* is defined similarly to a Boolean circuit, but instead of the gates $\neg$, $\wedge$, $\vee$ we use the gate $+$, $-$, $\times$. For example the output of gate $\times(x_1, x_2, \ldots, x_k)$ is the product $x_1 x_2 \ldots x_k$. So an algebraic circuit computes a polynomial in the inputs. Note that a small (i.e., size $p(n)$ for some polynomial p) circuit over $x_1, x_2, \ldots, x_n$ can compute a polynomial that contains exponentially many monomials. For example, consider the circuit with a $\times$-gate output that takes input from m $+$-gates

$$(x_1 + x_2), \quad (x_3 + x_4), \quad (x_5 + x_6), \quad \ldots, (x_{2m-1} + x_{2m})$$

(where $m = \lfloor n/2 \rfloor$). The polynomial computed by this circuit is

$$\prod_{i=1}^{m} (x_{2i-1} + x_{2i})$$

and it has 2^m monomials.

Given an algebraic circuit, we want to test whether it computes the 0 polynomial. Formally, the language ZEROP consists of all encoding of algebraic circuits that compute the identically zero polynomial. It follows from the results in Section 7.2.3. that this language belongs to *co*-**RP**.

Prove that there is a family of polynomial size Boolean circuits $\{C_1, C_2, \ldots\}$ that computes ZEROP. (You can use the fact mentioned above, but give full details for any other arguments.)