Computer Science 2401F
St. George Campus

December 6, 2002
University of Toronto

Homework Assignment #4
Due: January 7, 2003, by 5:00PM

Question 1. (10 marks) Show that Integer Addition can be done by uniform AC^0 circuits. That is, show that there is a (log-space uniform), polynomial size family of unbounded-fanin constant depth circuits $\{C_n\}$, such that C_n when given as input two n-bit integers, outputs their sum.

Question 2. (10 marks) Prove that there is no AC^0 family of circuits $\{C_n\}$ that compute integer multiplication, that is, such that C_n outputs the product of its two n-bit integer inputs.

You should use the fact that there is no AC^0 family of circuits for computing the exclusive-or (that is, the mod 2 sum) of the input bits. That is, show how you could use AC^0 circuits for multiplication to construct AC^0 circuits for exclusive-or.

Question 3. (20 marks) We say a function $f : \{0,1\}^* \to \{0,1\}^*$ is *average-case one-way* if

- f can be computed in (deterministic) polynomial time.
- For every probabilistic, polynomial time Turing machine ADV (ADV stands for "adversary") the following is true:

  Let p_n be the probability that if a random $x \in \{0,1\}^n$ is chosen and $\langle 1^n, f(x)\rangle$ is given to ADV, then ADV outputs a string $x' \in \{0,1\}^n$ such that $f(x') = f(x)$.

  Then for every c and sufficiently large n, $p_n < \frac{1}{n^c}$.

We say *there is a feasible collection of hard solved instances for satisfiability* if:

There is probabilistic, polynomial time Turing machine M which on input 1^n outputs a pair (F, τ) where F is a formula of the propositional calculus and τ is a truth assignment for the variables of F, such that:

- No matter how M tosses its coins, if M outputs (F, τ) then τ satisfies F.
- For every probabilistic, polynomial time Turing machine ADV the following is true:

  Let p_n be the probability that if M is given 1^n as input, and if M is then run (probabilistically) and outputs (F, τ), and if $\langle 1^n, F\rangle$ is then given to ADV, then ADV outputs a satisfying assignment for F.

  Then for every c and sufficiently large n, $p_n < \frac{1}{n^c}$.

1. Prove that there is an "average-case one-way function" if and only if "there is a feasible collection of hard solved instances for satisfiability".
2. It turns out that most cryptography depends for its security on the existence of average-case one-way functions. Prove that if **P=NP**, there are no such functions.