HW6, CPSC 468/568, Due April 26, 2016

Throughout this assignment, if a proof or step of a proof follows directly from a definition given or a theorem proven in class or in a reading assignment, then you may simply say that, i.e., you need not reproduce proofs given in class or in the reading.

**Problem 1 (20 points):**
Prove that, for any \( f \) in \( \#P \) and any constant \( \epsilon > 0 \), the function \( f \) can be \( \epsilon \)-approximated in \( FP^{\Sigma^p_2} \). That is, prove that there is a function \( g \) that is an \( \epsilon \)-approximation of \( f \) and a deterministic polynomial-time oracle machine \( M \) such that \( M^O \) computes \( g \), where \( O \) is a \( \Sigma^p_2 \)-complete set.

(Hint: Use the ideas introduced in the proof that \( BPP \subseteq \Sigma^p_2 \cap \Pi^p_2 \).)

**Problem 2 (20 points):**
Consider the set \( C \) of circuits over the basis consisting of \( \neg \) and unbounded fan-in \( \land \) and \( \lor \). The non-uniform complexity class \( AC^0 \) consists of all languages accepted by families of polynomial-size, constant-depth circuits in \( C \); that is, \( L \in AC^0 \) if and only if it is accepted by a circuit family \( \{C_n\}_{n\geq 0} \) such that \( \{C_n\} \subseteq C \), \( \text{size}(C_n) \) is \( n^{O(1)} \), and \( \text{depth}(C_n) \) is \( O(1) \). A Boolean function \( f \) on \( \{0,1\}^n \) is symmetric if and only if, for any permutation \( \sigma \in S_n \),

\[
f(x_1,\ldots,x_n) = f(x_{\sigma(1)},\ldots,x_{\sigma(n)}).
\]

Prove that, for any \( L \in AC^0 \), there is a constant \( k \) such that \( L \) is accepted by a circuit family \( \{C'_n\}_{n\geq 0} \) in which the output gate of every \( C'_n \) is a symmetric function of fan-in \( n^{O(\log^k n)} = 2^{O(\log^{k+1} n)} \), each of whose inputs is an \( \land \) of \( O(\log^k n) \) input variables or their negations.

(Hint: Consider “scaling down” the proof of Toda’s Theorem.)

**Problem 3 (30 points):**
The language \( L \) is in the complexity class \( \text{Few} \) if there is a nondeterministic polynomial-time machine \( M \), a polynomial-time predicate \( Q \), and a polynomial \( p \) such that, for every \( x \in \{0,1\}^* \),

\[
\text{acc}_M(x) \leq p(|x|), \quad x \in L \text{ if and only if } Q(x, \text{acc}_M(x)), \quad \text{where } \text{acc}_M(x) \text{ is the number of accepting paths of } M \text{ on input } x.
\]

Show that \( \text{Few} \subseteq \text{D}^{\text{FewP}} \), where \( \text{FewP} \) is defined as in HW5, problem 6.

**Problem 4 (10 points):**
The language \( L \) is in the complexity class \( \text{C=P} \) if there is a nondeterministic polynomial-time machine \( M \) and a polynomial-time computable function \( f \) such that, for every \( x \in \{0,1\}^* \), \( x \in L \) if and only if \( \text{acc}_M(x) = f(x) \). Prove that \( \text{C=P} \subseteq \text{PP} \).

**Problem 5 (20 points):**
For any positive integer \( k \), the language \( L \) is in the complexity class \( \text{MOD}_k \text{P} \) if there is a nondeterministic polynomial-time \( M \) such that, for any \( x \in \{0,1\}^* \), \( x \) is in \( L \) if and only if \( \text{acc}_M(x) \not\equiv 0 \pmod{k} \). So \( \oplus \text{P} \) is \( \text{MOD}_2 \text{P} \). For any subsets \( A \) and \( B \) of \( \{0,1\}^* \), we define the join \( A \oplus B \) as the union of \( \{0x \mid x \in A\} \) and \( \{1y \mid y \in B\} \). For five points each, prove that, if \( k \) is prime, then \( \text{MOD}_k \text{P} \) is closed under union, intersection, complement, and join.