HOMEWORK 11

**Due: 10:00am, Thursday November 30**

---

1. **(Just mod 6 things.)**

   (a) Let $f : \{0,1\}^n \to \{0,1\}$ and let $p$ be a prime. As you showed in HW8.3(b), there is a multilinear polynomial $F(x_1, \ldots, x_n)$ over $\mathbb{F}_p$ such that $F(x) = f(x)$ for all $x \in \{0,1\}^n$. Show that such a multilinear representation is unique. (Hint: if $F_1(x) = F_2(x)$, key in on the least-degree nonzero monomial in $F_1(x) - F_2(x)$.) Deduce that any multilinear polynomial over $\mathbb{F}_p$ computing the AND function must have degree $n$.

   (b) Show that AND functions cannot be computed by constant-depth circuits (of *arbitrary* size) consisting only of input gates, the constant 1 gate, and $\text{mod}_p$ gates, where $p$ is a fixed prime. Recall that a $\text{mod}_m$ gate outputs 0 or 1 depending on whether the number of input 1's is zero or nonzero modulo $m$. (Hint: show that such a circuit computes a polynomial of constant degree.)

   (c) Show that AND functions *can* be computed by depth-2 circuits (albeit of exponential size) consisting only of input gates, the constant 1 gate, and $\text{mod}_6$ gates. (Hint: first show how to get $\text{mod}_3$ and $\text{mod}_2$ gates; then show that if you take the $\text{mod}_2$ of *every* subset of the inputs, then $\text{mod}_3$-together the $2^n$ results, you basically get the OR function.)

   Remark: It is open to show that AND is not computable by depth-3, poly-size circuits consisting only of $\text{mod}_6$ gates. It is also open to show this about SAT.

2. **(Circuit lower bounds for Permanent.)** Prove that the Permanent function (of integer matrices) is not computable by (uniform) $\mathsf{ACC}$ circuits, even with $2^{n^{o(1)}}$ size. You may take for granted the following facts: (i) the Time Hierarchy Theorem holds relative to any oracle; (ii) many reductions in classic complexity theorems (e.g., the Cook–Levin Theorem, Valiant's $\#\mathsf{P}$-completeness of Permanent for integer matrices, ...) can be carried out in (uniform) $\mathsf{AC}^0$.

   Remark: In fact, it has been shown that Permanent is not even in the larger circuit class of (uniform) $\mathsf{TC}^0$: namely, $O(1)$-depth poly-size circuits of Majority gates.

3. **(Fighting perebor for ACC-SAT.)** In this problem, your algorithms may be in the random-access Turing Machine model.

   (a) Show that there is a $2^m \cdot \text{poly}(m)$ time algorithm for deciding whether a given $m$-input, "size-$2^{\sqrt{m}}$ SYM+ circuit" is satisfiable. Recall that such a circuit is of the form $h(p(x_1, \ldots, x_m))$, where $p$ is a multilinear polynomial given by the sum of at most $2^{\sqrt{m}}$ monomials (each of degree at most $\sqrt{m}$) and $h$ is an explicitly given function $\{0, 1, 2, \ldots, 2^{\sqrt{m}}\} \to \{0,1\}$. (Hint: you may appeal to a problem from Homework 7.)

   (b) Fix a depth $d \in \mathbb{N}^+$ and a modulus $r$. Show that for a sufficiently small constant $\delta > 0$, there is a $2^m \cdot \text{poly}(m)$ time algorithm for deciding whether a given $m$-input, depth-$(d+1)$, size-$2^{O(m^\delta)}$ $\mathsf{AC}^0[r]$ circuit is satisfiable. (Hint: you may appeal to theorems from class.)

   (c) Show that there is a $2^{n-\Omega(n^\delta)}$ time algorithm for deciding whether a given $n$-input, depth-$d$, size-$2^{n^\delta}$ $\mathsf{AC}^0[r]$ circuit is satisfiable. (Hint: given $C$, consider $C'$ which is an OR over all possible settings to the first $n^\delta$ variables of $C$.)