Homework 3
Due Mon May 19, 5:00pm

Prof. Amit Chakrabarti
Department of Computer Science
Dartmouth College

General Instructions: Feel free to reference things we have proved in class. That will help a lot in this homework, and will keep your own solutions short.

Notation: We consider certain natural Boolean function families in this homework, which we now define. Each of these function families is of the form $f = \{f_n\}_{n\in\mathbb{N}}$, where $f_n : \{0,1\}^n \to \{0,1\}$.

$$\text{PAR}: \quad \text{PAR}_n(x) = 1 \iff \sum_{i=1}^{n} x_i \equiv 1 \pmod 2, \quad \forall\, x \in \{0,1\}^n.$$

$$\text{MOD}_m: \quad \text{MOD}_{m,n}(x) = 1 \iff \sum_{i=1}^{n} x_i \not\equiv 0 \pmod m, \quad \forall\, x \in \{0,1\}^n, m \in \mathbb{N}, m \geq 2.$$

$$\text{MOD}'_{m,k}: \quad \text{MOD}'_{m,k,n}(x) = 1 \iff \sum_{i=1}^{n} x_i \equiv k \pmod m, \quad \forall\, x \in \{0,1\}^n, m, k \in \mathbb{N}, m \geq 2.$$

$$\text{MAJ}: \quad \text{MAJ}_n(x) = 1 \iff \sum_{i=1}^{n} x_i \geq n/2, \quad \forall\, x \in \{0,1\}^n.$$

Throughout this homework, "circuits" are allowed to have unbounded fan-in. The class AC^0 consists of Boolean functions (equivalently, languages over the alphabet $\{0,1\}$) that can be computed by constant depth polynomial size circuits with AND, OR and NOT gates. The class $\mathsf{AC}^0[m]$ is similar, except that it additionally allows MOD_m gates, where $m \geq 2$ is a constant integer.

1. As we remarked in class, it is clear that monotone circuits can only compute monotone functions. Prove the converse, i.e., prove that any n-bit monotone Boolean function can be computed by an n-input monotone circuit. [5 points]

2. Consider depth-2 circuits with access to each input bit x_i and its negation $\neg x_i$, where $\vec{x} \in \{0,1\}^n$ is the input vector. As part of our proof that $\text{PAR} \notin \mathsf{AC}^0$, we showed that if such a circuit computes PAR_n, it must have size at least 2^{n-1}. But what if we're only interested in a circuit that computes PAR_n correctly on *some* subset of a little more than half of the 2^n different inputs?

   2.1. Why is it not interesting to compute PAR_n correctly on just 2^{n-1} inputs? [1 points]

   2.2. Show that there is a depth-2 circuit of size $2^{O(\sqrt{n})}$ that computes PAR_n correctly on at least $2^{n-1} + 2^{\sqrt{n}}$ inputs. [9 points]

3. We proved in class that $\text{PAR} \notin \mathsf{AC}^0$, and later seemingly strengthened this by showing $\text{PAR} \notin \mathsf{AC}^0[3]$. Prove that this latter result *is* in fact stronger by showing that $\mathsf{AC}^0 \subset \mathsf{AC}^0[3]$ (i.e., a proper subset). For this problem, use only the random restrictions technique, and not the approximation-by-polynomials technique. [5 points]

4. Prove that $\text{MAJ} \notin \mathsf{AC}^0$.

   Hint: This can be solved using either of the two techniques we used in class to show $\text{PAR} \notin \mathsf{AC}^0$. However, you can give a shorter proof by exhibiting an AC^0 circuit that reduces PAR to MAJ. For this approach, it might help to use $\text{FALSE} = +1$, $\text{TRUE} = -1$ and consider sums of the form $x_1 + \cdots + x_{n/2} - x_{n/2+1} - \cdots - x_n$. Be careful about separating the two cases: (a) n is odd (b) n is even. [10 points]

5. Revisit the random restrictions proof that $\text{PAR} \notin \mathsf{AC}^0$ and perform the necessary calculations to obtain a specific quantitative lower bound, in terms of n and d, on the size of depth-d circuit that computes PAR_n. Your bound should be something super-polynomial in n (for constant d). Do not worry if you don't quite get the optimal bound of $2^{n^{1/(d-1)}}$ — just derive what you can. [10 points]

6. Let p and q be primes with $p \neq q$. We claimed in class that the approximation-by-polynomials technique can be extended to show that $\text{MOD}_q \notin \mathsf{AC}^0[p]$. This problem walks you through the proof.

   The proof requires a bit of finite field theory, but that shouldn't daunt you. Here is the crucial fact we need: the finite field $K := \mathbb{F}_{p^{q-1}}$ contains $\mathbb{F}_p$ (the familiar field consisting of integers mod p) as a subfield, and also contains a *primitive q-th root of unity*, i.e., an element $\omega \in K \setminus \{0,1\}$ such that $\omega^q = 1$.

   Suppose C is an n-input $\mathsf{AC}^0[p]$ circuit with depth d and size s that computes the function MOD_q. As in class, we can assume, thanks to de Morgan's Laws, that C contains no AND gates. We topologically sort C and proceed to approximate each of its gates, in order, by polynomials over $\mathbb{F}_p$.

   6.1. By generalizing the random subsums construction from class suitably, prove that there exists a polynomial $h(x_1,\ldots,x_n) \in \mathbb{F}_p[x_1,\ldots,x_n]$ such that
   - $\deg h \leq (p-1)\ell$,
   - $\forall\, \vec{x} \in \{0,1\}^n :\ h(\vec{x}) \in \{0,1\}$, and
   - $\Pr[h(\vec{x}) \neq \text{OR}_n(\vec{x})] \leq 1/p^\ell$, with $\vec{x} \in_R \{0,1\}^n$. [5 points]

   6.2. Based on your construction above, prove that there exists a polynomial $f(x_1,\ldots,x_n) \in \mathbb{F}_p[x_1,\ldots,x_n]$ such that
   - $\deg f \leq \sqrt{n}$.
   - $\forall\, \vec{x} \in \{0,1\}^n :\ f(\vec{x}) \in \{0,1\}$, and
   - $\Pr[f(\vec{x}) \neq C(\vec{x}) = \text{MOD}_q(\vec{x})] \leq s \cdot p^{-n^{1/(2d)}/(p-1)}$, where $\vec{x} \in_R \{0,1\}^n$.

   To get these bounds you will need to set ℓ appropriately in the previous construction. [3 points]

   6.3. The above gave us a "low degree approximation" to the single Boolean function MOD_q. By suitably modifying the circuit C, prove that there exists a "large" *good set* $A \subseteq \{0,1\}^n$ on which each of the Boolean functions $\text{MOD}'_{q,k}$ (with $0 \leq k \leq q-1$) can be represented by a low degree polynomial. State your results precisely. In particular, state a precise lower bound on $|A|$ and an upper bound on the degree. [5 points]

   6.4. Consider the affine map $\alpha : K \to K$ given by $\alpha(x) = 1 + (\omega - 1)x$. This map gives us a "notation shift" for functions with Boolean input: $0/1$ notation becomes $1/\omega$ notation. Applying α coordinatewise maps the set A to some set $A' \subseteq \{1,\omega\}^n$. Based on your earlier observations, prove that the polynomial $y_1 y_2 \cdots y_n$ agrees with some "low" degree *multilinear* polynomial $g(y_1,\ldots,y_n) \in K[y_1,\ldots,y_n]$ on the set A'. [7 points]

   6.5. Argue that the equations $y_i^{-1} = 1 + (\omega^{-1} - 1)(\omega - 1)^{-1}(y_i - 1)$ hold for $(y_1,\ldots,y_n) \in A'$. [2 points]

   6.6. Proceeding as we did in class, prove that every function from A' to K can be represented (on A') by a multilinear polynomial in $K[y_1,\ldots,y_n]$ of degree $\leq n/2 + \sqrt{n}$. Using this, count the number of functions from A' to K in two ways to obtain the desired super-polynomial lower bound on s. [8 points]