CS 239
Fall 2011
Computation Complexity

Homework 3
Due Mon Nov 28, 5:00pm

Prof. Amit Chakrabarti
Department of Computer Science
Dartmouth College

General Instructions. Each problem has a fairly short solution. Feel free to reference things we have proved in class, to keep your own solutions short. **Each problem is worth 10 points, except for the last problem, which is worth 20 points.** I have indicated a partial score breakdown for the last problem as a guideline only.

Honor Prinicple. You are allowed to discuss the problems and exchange solution ideas with your classmates. But when you write up any solutions for submission, you must work alone. You may refer to any textbook you like, including online ones. However, you may not refer to published or online solutions to the specific problems on the homework. *If in doubt, ask the professor for clarification!*

General Instructions:

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 $f_n : \{0,1\}^n \to \{0,1\}$.

$$\begin{array}{llll}
\textsc{par}: & \textsc{par}_n(x) = 1 \iff \sum_{i=1}^n x_i \equiv 1 \pmod 2\,, & & \forall\, x \in \{0,1\}^n\,. \\
\textsc{mod}_m: & \textsc{mod}_{m,n}(x) = 1 \iff \sum_{i=1}^n x_i \not\equiv 0 \pmod m\,, & & \forall\, x \in \{0,1\}^n, m \in \mathbb{N}, m \geq 2\,. \\
\textsc{mod}'_{m,k}: & \textsc{mod}'_{m,k,n}(x) = 1 \iff \sum_{i=1}^n x_i \equiv k \pmod m\,, & & \forall\, x \in \{0,1\}^n, m,k \in \mathbb{N}, m \geq 2\,. \\
\textsc{maj}: & \textsc{maj}_n(x) = 1 \iff \sum_{i=1}^n x_i \geq n/2\,, & & \forall\, x \in \{0,1\}^n\,.
\end{array}$$

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 $\textsc{mod}_m$ gates, where $m \geq 2$ is a constant integer.

12. Complete the proof of Håstad's Switching Lemma, by filling in the steps we skipped in class. As a reminder, here is an outline of the proof, along with what we did not show in class.

    Let f be a k-DNF on n variables. Let $\mathscr{R}_m$ denote the set of restrictions (i.e., partial assignments) of these variables that have exactly m stars, i.e., $\mathscr{R}_m = \{\alpha \in \{0,1,\star\}^n : \mathrm{Ex}(\alpha) = n - m\}$. Let $p \in (0, \frac{1}{2})$ be a small fraction. The switching lemma says that hitting f with a random restriction from $\mathscr{R}_{pn}$ will very likely result in a function of low deterministic query complexity. To be precise:

    $$\Pr_{\rho \in_R \mathscr{R}_{pn}} [\mathrm{D}(f|_\rho) \geq s] \;\leq\; (7pk)^s\,. \tag{1}$$

    To prove this, we considered the set of "bad" restrictions $\mathscr{B} = \{\rho \in \mathscr{R}_{pn} : \mathrm{D}(f|_\rho) \geq s\}$. We gave an injective map from $\mathscr{B}$ to $\mathscr{R}_{pn-s} \times \{0,1\}^s \times \mathrm{stars}(k,s)$, where

    $$\mathrm{stars}(k,s) \;:=\; \{(w_1,\ldots,w_\ell) :\; \ell \geq 1,\text{ each } w_i \in \{0,1\}^k \setminus \{0\}^k, \text{ and } |w_1| + \cdots + |w_\ell| = s\}\,,$$

    where $|w|$ denotes the number of 1s in the binary string w.

    12.1. Prove that $|\mathrm{stars}(k,s)| \leq (k/\ln 2)^s$.

    Hint: Use induction on s to prove that $|\mathrm{stars}(k,s)| \leq \alpha^s$, where $(1 + 1/\alpha)^k = 2$. Then show that this inequality implies the above. For the base case, put the empty string in $\mathrm{stars}(k,0)$ for convenience.

    12.2. Use the above result to upper bound $|\mathscr{B}|$, and complete the calculations required to derive Eq. (1).

13. 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 $\textsc{par} \notin \mathsf{AC}^0$, we showed that if such a circuit computes $\textsc{par}_n$, it must have size at least 2^{n-1}. But what if we're only interested in a circuit that computes $\textsc{par}_n$ correctly on *some* subset of a little more than half of the 2^n different inputs?

    13.1. Why is it not interesting to compute $\textsc{par}_n$ correctly on just 2^{n-1} inputs?

    13.2. Show that there is a depth-2 circuit of size $2^{O(\sqrt{n})}$ that computes $\textsc{par}_n$ correctly on at least $2^{n-1} + 2^{\sqrt{n}}$ inputs.

14. Prove that $\textsc{maj} \notin \mathsf{AC}^0$.

    Hint: This can be solved using either of the two techniques we used in class to show $\textsc{par} \notin \mathsf{AC}^0$. However, you can give a shorter proof by exhibiting an AC^0 circuit that reduces $\textsc{par}$ to $\textsc{maj}$. For this approach, it might help to use $\textsc{false} = +1$, $\textsc{true} = -1$ 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.

15. Let $n = 2m \log m$, and assume m is a power of 2. The Element Distinctness function $\textsc{ed}_n : \{0,1\}^n \to \{0,1\}$ is defined by viewing the input as (the concatenation of) the binary representations of m integers $s_1, \ldots, s_m$, each of which is represented by $2 \log m$ bits. It tells us whether or not these integers are distinct. Formally,

$$\textsc{ed}_n(s_1, \ldots, s_m) = 1 \iff \forall\, i \neq j \in [m] : s_i \neq s_j .$$

    Using Neciporuk's method, prove that $\mathrm{L}_B(\textsc{ed}_n) = \Omega(n^2/\log n)$.

16. 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 $\textsc{mod}_q \notin \mathsf{AC}^0[p]$. 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 $\textsc{mod}_q$. As in class, we can assume, thanks to de Morgan's Laws, that C contains no $\textsc{and}$ gates. We topologically sort C and proceed to approximate each of its gates, in order, by polynomials over $\mathbb{F}_p$.

    16.1. By generalizing the random subsums construction from class in a suitable manner, prove that there exists a polynomial $h(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ such that

    - $\deg h \le (p-1)\ell$,
    - $\forall\, \vec{x} \in \{0,1\}^n : h(\vec{x}) \in \{0,1\}$, and
    - $\Pr[h(\vec{x}) \neq \textsc{or}_n(\vec{x})] \le 1/p^{\ell}$, with $\vec{x} \in_R \{0,1\}^n$. [3 points]

    16.2. 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

    - $\deg f \le \sqrt{n}$.
    - $\forall\, \vec{x} \in \{0,1\}^n : f(\vec{x}) \in \{0,1\}$, and
    - $\Pr[f(\vec{x}) \neq C(\vec{x}) = \textsc{mod}_q(\vec{x})] \le s \cdot p^{-n^{1/(2d)}/(p-1)}$, where $\vec{x} \in_R \{0,1\}^n$.

    To get these bounds you will need to set ℓ appropriately in the previous construction. [2 points]

    16.3. The above gave us a "low degree approximation" to the single Boolean function $\textsc{mod}_q$. 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 $\textsc{mod}'_{q,k}$ (with $0 \le k \le q-1$) 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. [4 points]

16.4. 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'. [5 points]

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

16.6. 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. [5 points]