Homework 6
Due 2017-Feb-20, 11:59pm

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 7 points.*

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!*

On this homework, "circuits" are allowed to have unbounded fan-in. The complexity class AC^0 consists of Boolean functions that can be computed by constant depth polynomial size circuits with AND, OR and NOT gates. Here are two natural Boolean function families, each of the form $f = \{f_n\}_{n\in\mathbb{N}}$, where $f_n : \{0,1\}^n \to \{0,1\}$.

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

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

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:

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

    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 $\mathscr{R}_{pn-s} \times \mathrm{Sel}_{k,s} \times \{0,1\}^s$, where

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

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

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

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