Homework 7
Due 2017-Mar-07, 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.*

Note that this homework is longer than usual and it is due on a Tuesday night, instead of the usual Monday night.

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

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

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

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

15. 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 $\mathbb{F}_p$.

    15.1. 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
    - $\deg h \leq (p-1)\ell$,
    - $\forall\, \vec{x} \in \{0,1\}^n : \; h(\vec{x}) \in \{0,1\}$, and
    - $\Pr[h(\vec{x}) \neq \text{OR}_n(\vec{x})] \leq 1/p^\ell$, with $\vec{x} \in_R \{0,1\}^n$.

    15.2. 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.

    15.3. 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.

16. Continuation of the previous problem (worth another 7 points).

    16.1. 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'.

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

16.3. 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.

17. Prove that, for every Boolean function $f : \{0,1\}^n \to \{0,1\}$, we have $\text{depth}(f) = \Theta(\log \mathrm{L}_D(f))$, where L_D denotes de Morgan formula length.

    Hint: One direction should be easy, using induction (say). For the other direction, first prove that, in a rooted binary tree with ℓ leaves, there exists a node v such that the number of leaves that are descendants of v lies in $[\ell/3, 2\ell/3]$. Then use this fact to "balance" a formula that is needlessly deep.

18. Recall the Karchmer-Wigderson game R_f corresponding to a nonconstant Boolean function $f : \{0,1\}^n \to \{0,1\}$. Alice gets an input $x \in \{0,1\}^n$ such that $f(x) = 1$ and Bob gets an input $y \in \{0,1\}^n$ such that $f(y) = 0$. Alice and Bob must agree on an index $i \in [n]$ such that $x_i \neq y_i$. Prove that $\mathrm{D}(R_f) = \text{depth}(f)$, where 'D' denotes deterministic communication complexity and 'depth' denotes circuit depth.

    Hint: We have already shown in class that $\mathrm{D}(R_f) \leq \text{depth}(f)$. For the other direction, use induction on the complexity of the best protocol for the game.

19. Let $\textsc{ustcon}_N : \{0,1\}^{\binom{N}{2}} \to \{0,1\}$ be the "undirected s–t connectivity" Boolean function. That is, the input is viewed as the description of an *undirected* labeled N-vertex graph, and the output is 1 iff there is a path in this graph between two designated vertices s and t (WLOG, we may take $s = 1, t = 2$).

    Prove the monotone circuit depth lower bound $\text{depth}_m(\textsc{ustcon}_N) = \Omega(\log^2 N)$. You may follow the same outline as our work in class for the function STCON, so you don't have to repeat long proofs from class. Just highlight the differences. Be explicit about what you need to change in the proof.

    Hint: Consider the relation $\textsc{fork}' \in [w]^\ell \times [w]^\ell \times \{0, 1, \ldots, \ell\}$ given by

    $$(x, y, i) \in \textsc{fork}' \iff \widetilde{x}_i = \widetilde{y}_i \wedge (\widetilde{x}_{i-1} \neq \widetilde{y}_{i-1} \vee \widetilde{x}_{i+1} \neq \widetilde{y}_{i+1}),$$

    where $\widetilde{x} = 1 \circ x \circ 1$ and $\widetilde{y} = 1 \circ y \circ 2$.