# Problem Set 3

- Due Date: **16 Dec (Fri), 2011**
- If you submit handwritten solutions, start each problem on a fresh page.
- Collaboration is encouraged, but all writeups must be done individually and must include names of all collaborators.
- Referring sources other than the lectures is strongly discouraged. But if you do use an outside source (eg., other text books, lecture notes, any material available online), ACKNOWLEDGE it in your writeup.
- The points for each problem are indicated on the side.
- If you don't know the answer to a problem, then just don't answer it. Do not try to convince yourself or others into believing a false proof.
- Be clear in your writing.

---

1. **[universal relation]**

   The universal relation $U_n$ is defined as follows.

   $$U_n = \{(x, y, i) \in \{0,1\}^n \times \{0,1\}^n \times [n] : x_i \neq y_i\}.$$

   Alice is given $x \in \{0,1\}^n$ and Bob $y \in \{0,1\}^n$ such that $x \neq y$. They have to determine an $i$ such that $(x, y, i) \in U_n$.

   In this problem, we will show that there is a randomized public coins protocol, where

   - Alice sends one message of $O((\log n)^2)$ bits;
   - Bob determines an $i$ such that $(x, y, i) \in U_n$;
   - $Pr[x_i \neq y_i] \geq \frac{2}{3}$.

   Consider the following subproblems.

   (a) [Identify] Give an $O(\log n)$ bit protocol that makes error at most $1/3$ under the promise that $x$ and $y$ differ in only one position. (There is a deterministic protocol but a randomized protocol would suffice.)

   (b) [Isolate] Now for the general case, when $x$ and $y$ may differ in more than one position. Using shared randomness, devise a distribution for sets $S_1, S_2, ..., S_\ell \subseteq [n]$ ($\ell = O(\log n)$), such that with constant probability there is an $i$ such that $x|_{S_i}$ and $y|_{S_i}$ differ in only one position.

   (c) [Verify] Suppose Alice has $x$ and Bob has $(y, i)$. Give a constant protocol in which Alice sends $O(1)$ bits and Bob verifies with probability at least $2/3$ that $x$ and $y$ differ only at $i$.

   (d) Combine the above parts to obtain the one-round randomized protocol for the universal relation.

   In the second part of this problem, we will show that any public coins randomized protocol (error at most $\frac{1}{3}$) for the universal relation where Alice sends just one message, requires $\Omega((\log n)^2)$ bits of communication.

   Use the following augmented index function problem. Alice gets $u \in [L]^L$ and Bob gets $i$ and $u_1, ..., u_{i-1}$; Alice sends one message and Bob determines $u_i$. (Later we will set $L$ to be about $\log n$.)

(e) Any randomized (public coins) protocol for this augmented index function problem requires $\Omega(L^2)$ bits of communication.

(f) [Reduction] Suppose Alice needs to send a number $z \in [L]$ to Bob. Show how you will do this using a protocol for the universal relation on $L$ bit inputs. That is, Alice transforms her input $i$ to $f(i) \in \{0,1\}^L$ and Bob produces an input $v \in \{0,1\}^L$; they run the protocol for the universal relation, and from the output Bob determines $z$.

(g) Use the reduction in part (f) appropriately to $u_1, ..., u_L$, thereby producing inputs to the universal function problem of size $n = L^2$. In other words, give a reduction such that Alice transforms her input $u_{[1,L]} = (u_1, \ldots, u_L)$ to an input in $\{0,1\}^{L^2}$ and Bob transforms his input $(u_{[1,i-1]}, i)$ to an input in $\{0,1\}^{L^2}$ such that when they run the universal relation protocol on these transformed inputs, Bob recovers one of $u_i, u_{i+1}, ..., u_L$.

(h) Use public randomness and increase the input length to $2^{O(L)}$ to ensure that with high probability the protocol actually helps Bob recover $u_i$ itself.

2. [**disjointness of fixed size sets**]

Suppose Alice and Bob are given $k$-sized subsets of $[n]$ each and they have to determine if the sets are disjoint. Call this problem $\mathsf{DISJ}_{n,k}$. Show that the randomized public coins (error at most $\frac{1}{3}$) complexity of $\mathsf{DISJ}_{n,k}$ is $O(k)$. (Observe that an $O(k \log n)$ protocol is easy to obtain.) The following hints might help you in constructing the protocol

- [Small sets] Suppose $k$ is constant. Hash into some $O(k^2)$ bits using public randomness, and determine the answer with $O(k^2)$ bits of communication.
- [Shrinking the bigger set]. Proceed as in the protocol for product distributions. Suppose the sets have sizes $s, t$ ($s \leq t \leq k$). Alice picks a random superset of her input and sends it to Bob with $O(s)$ bits of communication (use shared randomness). Bob restricts his input to inside this set. If this does not result in significant decrease in the size of Bob's set, then the sets probably intersect heavily (by Chernoff). Repeat, keeping the total error in control until the sets become small and apply the base case above..

3. [**FORK**]

[Kushilevitz-Nisan, Exercise 5.21] Let $\mathsf{FORK}'$ be the relations consisting of triples $(x, y, i)$ such that $x, y \in \Sigma^\ell$, and is is such that $x_i = y_i$ and $x_{i+1} \neq y_{i+1}$ or $x_{i-1} \neq y_{i-1}$. Prove that $D(\mathsf{FORK}') = \Omega(\log \ell, \log w)$.

4. [$s$-$t$ **connectivity: asymmetry in KW result**]

Karchmer and Wigderson showed that any monotone circuits for $s$-$t$ connectivity on $n$-vertex graphs, where ANDs have fanin at most $2^{n^{1/5}}$ and ORs have fanin at most $n^{1/5}$, must have depth $\Omega(\log n)$. Observe that there exist shallow circuits in which that AND and OR fanins are reversed.

Now, consider the $s$-$t$ cut function, which is true on an $n$ vertex directed graph if its complement has no $s$-$t$ path. Like the $s$-$t$ connectivity problem, this is a monotone function defined on $n \times n$ adjacency matrices (no self-loops, parallel edges).

A monotone projection from $s$-$t$ connectivity (on $n$ vertex graphs) to $s$-$t$ cut (on $N$ vertex graphs) is a function from $f : [N] \times [N] \to [n] \times [n]$, such that the $n \times n$ adjacency matrix $A = (a_{i,j})$ is $s$-$t$ connected iff the $N \times N$ matrix $B = (b_{k,\ell})$ where $b_{k,l} = a_{f(k,l)}$ is $s$-$t$ cut. Show that no such projection exists if $N$ is polynomially bounded in $n$.

5. [**Discrepancy of depth 2** $AC^0$ **circuits**]

(a) Let $f(x_1, \ldots, x_{2k+1}) = \mathsf{maj}(x_1, \ldots, x_{2k+1})$. Let Alice be given the first $k+1$ bits, i.e., $x_1, \ldots, x_{2k+1}$ and Bob the next $k$ bits. Show that there exists an $O(1)$-randomized protocol with error at most

$\frac{1}{2} - O\left(\frac{1}{k}\right)$ that computes $f$. Conclude that $\mathsf{maj}$ has discrepancy at least $\Omega(1/k)$ with respect to every distribution.

(b) Now, consider a function $f$ on $2k$ variables defined as a depth 2 $AC^0$ circuit as follows: $f(x_1, \ldots, x_{2k}) = T_1 \vee T_2 \vee \cdots \vee T_l$ where the $T_i$'s are conjunction of literals. Let Alice be given the first $k$ bits of $x_1, \ldots, x_{2k}$ and Bob the next $k$ bits. Show that there exists an $O(1)$-randomized protocol with error at most $\frac{1}{2} - O\left(\frac{1}{l}\right)$ that computes $f$. Conclude that any depth 2 $AC^0$ circuit with top fan-in $s$ has discrepancy at least $\Omega(1/s)$ with respect to every distribution.

6. [**communication complexity of $\mathsf{GT}$ and $\mathsf{LTF}$**]

(a) Given two $n$ bit integers $0 \leq x, y < 2^n$, "greater than" function $\mathsf{GT}(x, y) = 1$ iff $x > y$.
Using one of the theorems proved/stated in lecture, show that $\mathrm{R}_\varepsilon(\mathsf{GT}) = O\left(\log n + \log\left(\frac{1}{\varepsilon}\right)\right)$.

(b) Let $a_1, \ldots, a_n, b_1, \ldots, b_n, \theta \in \mathbb{R}$. Then, the linear threshold function corresponding to $(a, b, \theta)$ where $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ is defined as follows

$$\mathsf{LTF}_{a,b,\theta}(x, y) = \begin{cases} 1, & \text{if } \sum_{i=1}^{n} (a_i x_i + b_i y_i) \geq \theta, \\ 0, & \text{otherwise.} \end{cases}$$

Show using part (a) or otherwise that $\mathrm{R}_\varepsilon(\mathsf{LTF}_{a,b,\theta}) = O\left(\log n + \log\left(\frac{1}{\varepsilon}\right)\right)$ for all $a, b$ and $\theta$.
[Hint: Try to bound the size of the "possible" numbers $a_i, b_i, \theta$.]

7. [**Simultaneous messages**]

In a simultaneous message protocol (SMP), Alice and Bob send a message each (based on their respective inputs) to a referee, who must then announce the result.

(a) Show that there is a private coins simultaneous messages protocol for $\mathsf{EQ}_n$ where Alice and Bob both send $O(\sqrt{n})$ bits.

(b) Suppose there is a simultaneous messages private coins randomized protocol for a function $f$, where Alice sends messages of length $a$ and Bob sends messages of length $b$. Show that then there is a deterministic one-way communication protocol for $f$ with communication $O(ab)$. Conclude that the private coins simultaneous message complexity of $\mathsf{EQ}_n$ is at least $\Omega(\sqrt{n})$.
[Hint: View the referee's actions as a matrix with rows indexed by messages of Alice ($\in \{0,1\}^a$) and columns by message of Bob ($\in \{0,1\}^b$). Show that for each input $x$, Alice can send Bob a (multi-)set $S_x \subseteq \{0,1\}^a$ of $O(b)$ row indices (use Chernoff bounds to show the existence of such $S_x$); Bob can then restrict himself to these rows, and based on the distribution of his messages in the simultaneous protocol, simulate the referee's actions faithfully.]

8. [**A direct sum result for simultaneous message protocols.**]

Consider the direct sum problem for $m$ copies of $\mathsf{EQ}_n$ in the SMP model: so, Alice gets $x_1, x_2, \ldots, x_m \in \{0,1\}^n$ and Bob gets $y_1, y_2, \ldots, y_m \in \{0,1\}^n$, and they need to determine the answers for all $m$ instances. Complete the following argument to show that the simultaneous messages randomized private coins communication complexity of this problem is $\Omega(m\sqrt{n})$.

(a) Consider a distribution on Alice's inputs, where each coordinate is chosen independently. Show that if Alice sends $a$ bits and Bob sends $b$ bits, then there is a coordinate for which they send only $O(a/m)$ bits and $O(b/m)$ bits of information to the referee.

(b) Show that Alice's message can be compressed to $O(a/m)$ bits for most of her inputs. Let $X$ be the input of Alice and let $M$ be her message. Suppose $I[X : M] \leq \alpha$. Let $P$ be the distribution of $M$. Let $P_x$ be the distribution of $M$ conditioned on $X = x$.

i. Recall $I[X : M] = \sum_x \Pr[X = x] S(P_x \| P)$. Observe that for *most* (define 'most' appropriately) values $x$, $S(P_x \| P) = O(\alpha)$; call such $x$ *good.*

ii. Prove the following. There are constants $A$ and $B$, such if $S(P_x\|P) \leq s$, then for all $\varepsilon > 0$,

$$\sum_{m:P_x(m)\geq 2^{(As+B)/\varepsilon}P(m)} P_x(m) \leq \varepsilon.$$

iii. Assume that Alice and the referee share independent samples of $M$ (generated according to $P$). Show that Alice, on receiving a good $x$ may then send $O(S(P_x\|P)/\varepsilon)$ bits to the referee and help him select a sample whose distribution is close (how close?) to $P_x$.

(c) Prove the result ($\Omega(m\sqrt{n})$ bound) using the previous two exercises. Note that there the coins were private. What distributions will you choose for the inputs?