CMSC 39600 Nov 20, 2007

Problem Set 2

- Due Date: **Dec 6 (Thurs), 2007**
- It is recommended that you try to solve all problems, but it is sufficient if you submit the writeup for any 5 problems.
- Collaboration is encouraged, but all writeups must be done individually.
- Indicate names of all collaborators.

Notation:

- $\mathbb{F}$ is a field of size q
- $\mathcal{S}_k^m$ is the set of affine subspaces of dimension k in $\mathbb{F}^m$.
- $P_{m,d}$ is the set of m-variate degree d polynomials

1. **[Affine subspaces sample well]**

   Let $A \subset \mathbb{F}^m$ of density μ (i.e., $|A| = \mu q^m$).

   $$\mathrm{Var}_{s \in \mathcal{S}_k^m}\left[\frac{|s \cap A|}{|s|}\right] \leq \frac{\mu}{q}.$$

   Hence, conclude that

   $$\Pr_{s \in \mathcal{S}_k^m}\left[\left|\frac{|s \cap A|}{|s|} - \mu\right| \geq \epsilon\right] \leq \frac{\mu}{\epsilon^2 q}.$$

2. **[Strategies for 2-Prover 1-Round Games]**

   Recall from lecture the definition of 2-prover 1-games. A game G is defined as follows: There are two all powerful provers P_1 and P_2 and question sets Q_1, Q_2 and answer sets A_1, A_2. A verifier draws inputs (q_1, q_2) from $Q_1 \times Q_2$ according to some underlying distribution $\mathcal{Q}$ known to both the provers. The verifiers sends query q_1 to prover P_1 and query q_2 to Prover P_2. The provers then return with answers a_1 and a_2. The verifier then accepts iff $V(q_1, q_2, a_1, a_2) = 1$ where V is some Boolean predicate. There are various strategies for the provers.

   - Local Strategy: The provers strategies is given by two functions $\pi_1 : Q_1 \to A_1$ and $\pi_2 : Q_2 \to A_2$. The value of the game $w(G)$ is then defined as follows:

     $$w(G) = \max_{\pi_1, \pi_2}\left\{\Pr_{(q_1,q_2) \sim_{\mathcal{Q}} Q_1 \times Q_2}\left[V(q_1, q_2, \pi_1(q_1), \pi_2(q_2)) = 1\right]\right\},$$

     where the maximum is taken over all local strategies (π_1, π_2).

- Local Strategy with shared randomness: In this case the provers share a random string r distributed according to some distribution $\mathcal{R}$ over some finite sized R. The prover strategies are then $\pi_1 : Q_1 \times R \to A_1$ and $\pi_2 : Q_2 \times R \to A_2$. The value of the game in this setting is given by

$$w^{\text{random}}(G) = \max_{\pi_1, \pi_2} \left\{ \Pr_{(q_1,q_2) \sim_{\mathcal{Q}} Q_1 \times Q_2, r \sim_{\mathcal{R}} R} [V(q_1, q_2, \pi_1(q_1, r), \pi_2(q_2, r)) = 1] \right\},$$

where the maximum is over all local strategies with shared randomness (π_1, π_2).

(a) Prove that randomness does not help the provers. In other words, the value of the game in both settings is identical ($w(G) = w^{\text{random}}(G)$ for all games G.

- Another type of prover strategies that is commonly studied is what is called the "no-signaling strategies". No-signaling strategies are not as stringent as the above local strategies which require the prover's computations to be dependent only on their input and not on the other prover's input. No-signally strategies only imply that is there is no communication between two the two provers. More formally, a pair of strategies $\pi : Q_1 \times Q_2 \times R \to A_1$ and $\pi_2 : Q_1 \times Q_2 \times R \to A_2$ is called no-signaling if for all q_1, q_2, q_1', q_2', the following distributions are identical

$$\begin{array}{lll} \pi_1(q_1, q_2, \mathcal{R}) & \text{is identical to} & \pi_1(q_1, q_2', \mathcal{R}) \\ \pi_2(q_1, q_2, \mathcal{R}) & \text{is identical to} & \pi_1(q_1', q_2, \mathcal{R}) \end{array}$$

Note that the provers are allowed to share a random string r as before distributed according to some distribution $\mathcal{R}$. The main difference is that the prover's answers could depend on the both queries. The value of the no-signaling game $w^{ns}(G)$ is defined similarly as follows:

$$w^{ns}(G) = \max_{\pi_1, \pi_2} \left\{ \Pr_{(q_1,q_2) \sim_{\mathcal{Q}} Q_1 \times Q_2, r \sim_{\mathcal{R}} R} [V(q_1, q_2, \pi_1(q_1, q_2, r), \pi_2(q_1, q_2, r)) = 1] \right\},$$

where the maximum is over all no-signaling strategies (π_1, π_2).

(b) (trivial) Prove that $w(G) \leq w^{ns}(G)$

(c) Consider the game in which the verifier draws a pair of random bits b_1 and b_2. The verifier sends b_1 to prover P_1 and b_2 to prover P_2. The provers respond with bits a_1 and a_2. The verifier accepts iff $b_1 \oplus b_2 = a_1 \wedge a_2$. Calculate $w(G)$ and $w^{ns}(G)$. Show that $w(G) < 1$ while $w^{ns}(G) = 1$.

It is known that the parallel repetition theorem is true for the no-signalling case too, i.e., if $w^{ns}(G) < 1$, there exists a constant $\delta \in (0, 1)$ such that $w^{ns}(G^{(k)}) \leq \delta^k$.

3. **[Fourier interpretations]**

Let $f : \{0,1\}^n \to \mathbb{R}$ and write the Fourier expansion of f, $f = \sum_{S \subseteq [n]} \hat{f}(S) \chi_S$ where $\chi_S : \{0,1\}^n \to \{-1, 1\}$ is defined as

$$\chi_S(x) = (-1)^{\sum_{i \in S} x_i},$$

and $\hat{f} : 2^{[n]} \to \mathbb{R}$ is defined as follows:

$$\hat{f}(S) = \langle f, \chi_S \rangle = \mathbb{E}\left[f(x)(-1)^{\sum_{i \in S} x_i}\right].$$

All probabilities and expectations in this question are with respect to the uniform product probability distribution on $\{0,1\}^n$.

(a) Given a set $S \subseteq [n]$, define $f^{\leq S} : \{0,1\}^n \to \mathbb{R}$ by

$$f^{\leq S} = \sum_{T : T \subseteq S} \hat{f}(T)\chi_T.$$

Note that $f^{\leq S}(x)$ actually only depends on the bits of x in S; call these bits x_S. Show that $f^{\leq S}(x_S)$ is equal to the expected value of f conditioned on the bits x_S (i.e., $f^{\leq S}(x_S) = \mathbb{E}_{y \in \{0,1\}^n}[f(y)|y_S = x_S]$ (The expectation is thus over the bits of x not in S.

(b) Suppose f's range is $\{-1,1\}$; i.e., f is a Boolean-valued function. We define the influence of the ith coordinate on f to be $\mathrm{Inf}_i(f) = \Pr_x[f(x) \neq f(x^{(i)})]$, where $x^{(i)}$ denotes the string x with the ith bit flipped. This measures how sensitive f is to flipping the ith coordinate. Show that

$$\mathrm{Inf}_i(f) = \sum_{S : i \in S} \hat{f}(S)^2.$$

(c) Again, suppose f is a Boolean-valued function. f is said to be monotone if $f(x) \leq f(y)$ whenever $x \geq y$. (By $x \geq y$ we mean $x_i \geq y_i$ for all i.) For example, the AND function which is given $\mathrm{AND}(x,y) = 1 - 2xy$ is monotone. Similarly, OR, and Majority are also monotone functions; Parity is not monotone.
Show that if f is monotone then $\mathrm{Inf}_i(f) = \hat{f}(\{i\})$ for each $i \in [n]$.

(d) Once more, suppose f is Boolean-valued. Suppose we pick $x \in \{0,1\}^n$ at random and then form a string $y \in \{0,1\}^n$ as follows: for each $i = 1 \ldots n$ independently, we set $y_i = x_i$ with probability ρ and set y_i to be a uniformly random bit with probability $1 - \rho$. The noise stability of f at ρ is defined to be

$$\mathrm{Stab}_\rho(f) = 2\Pr[f(x) = f(y)] - 1,$$

a number in the range $[-1,1]$. This measures in some way how stable f is when you flip about $\frac{1}{2}(1-\rho)$ input bits. Show that

$$\mathrm{Stab}_\rho(f) = \sum_{S \subseteq [n]} \hat{f}(S)^2 \rho^{|S|}.$$

4. **[polynomial decoding]**

(a) **[Schwartz-Zippel Lemma]** Given a non-zero polynomial $p : \mathbb{F}^m \to \mathbb{F}$, prove that

$$\Pr_x[p(x) = 0] \leq \frac{d}{q}.$$

[Hint: Use the fact that a non-zero univariate polynomial has at most d zeros. Then, use induction to generalize to larger dimensions]

(b) **[short list of polynomials]** Let $A : \mathbb{F}^m \to \mathbb{F}$ be any function (not necessarily a low degree polynomial). Let $p_1, p_2, \dots, p_t : \mathbb{F}^m \to \mathbb{F}$ be the list of *all* degree d polynomials such that $\Pr_x[A(x) = p_i(x)] \geq \delta$. In other words, $p_1, \dots, p_t$ is the list of *all* polynomials that have each agreement at least δ with the function A. Assume $\delta \geq 2\sqrt{d/q}$. Prove that $t \leq 2/\delta$. Hence, there are not too many low-degree polynomials that have considerable agreement with two polynomials.

[Hint: Use the fact that two low degree polynomial agree on at most d/q fraction of points (Schwartz-Zippel Lemma)]

5. **[Interpolation from cliques of consistency graph]**

In lecture, we defined the notion of a consistency graph $G = (V, E)$, given a subspace oracle $A : \mathcal{S}_k^{k+1} \to P_{k,d}$ where $V = \mathcal{S}_k^m$ and $E = \{(s_1, s_2) | \forall x \in s_1 \cap s_2, A(s_1)(x) = A(s_2)(x)\}$. Suppose there exists a clique $W \subset V$ of size $\left(\frac{2d+1}{q}\right)|V|$, prove that there exists a polynomial $Q : F^m \to F$ of degree $2d$ such that for eah $w \in W$, we have $Q|_w \equiv A(w)$.

[Hint: Use the large size of W to show that there exists two sets of d parallel hyperplanes (i.e, affine spaces of dimension k) in W. Interpolate along these hyperplanes to obtain a degree $2d$ polynomial Q. Use Schwartz-Zippel repeatedly to argue that Q identifies with $A(s)$ for all hyperplanes $s \in W$]

6. **[Degree reduction]**

In lecture, we showed that if the plane-point low-degree test passes with with non-significant probability *gamma*, in other words

$$\Pr_{s \in \mathcal{S}_k^m, x \in s} [A(s)(x) = A(x)] \geq \gamma,$$

then there exists a polynomial $Q : \mathbb{F}^m \to \mathbb{F}$ of degree at most $2d$ such that

$$\Pr_x [Q(x) = A(x)] \geq \gamma^2 - \epsilon,$$

for some $\epsilon = m^\alpha (d/q)^\beta$. In this problem, we will show that the degree of the polynomial Q can be reduced from $2d$ to d.

Suppose there exists a polynomial $Q : \mathbb{F}^m \to \mathbb{F}$ of degree δq for some $0 < \delta < 1$ and furthermore,

$$\Pr_{s \in \mathcal{S}_k^m} [Q|_s \equiv A(s)] \geq \delta + \frac{1}{q},$$

show that the degree of Q is in fact, at most d.

[Hint: Suppose by contradiction this is not the case (i.e., degree$(Q) = D > d$. Consider any k dimensional affine subspace $s = z_0 + \text{span}\{z_1, z_2, \dots, z_k\}$ for linearly independent $z_1, \dots, z_k$. Any point in s is of the form $z_0 + \sum \alpha_i z_i$. Consider the coefficient of α_i^D in the polynomial $P(\alpha_1, \dots, \alpha_k) = Q(z_0 + \sum \alpha_i z_i)$. Show using Schwartz-Zippel Lemma that with high probability this coefficient is not zero. Hence, with high probability $Q|_s$ is a degree D polynomial. Contradiction]

7. **[low degree testing to list of polynomials]**

In lecture, we showed that if there is a list of low-degree polynomials that agrees with the space oracle then low-degree test theorem is true. In this problem, we will show the converse of this statement.

Suppose there exists a function $f : (0, 1) \to (0, 1)$ such that the following is true.

"[Low Degree Test Theorem] For every function $A : \mathbb{F}^m \to \mathbb{F}$ and $A : \mathcal{S}_k^m \to P_{m,d}$ that satisfies

$$\Pr_{s,x}\left[A(s)(x) = A(x)\right] \geq \gamma,$$

we have

$$\Pr_{x}\left[A(x) = Q(x)\right] \geq f(\gamma)$$

for some polynomial Q of degree at most d (end of Low Degree Test Theorem)"

(recall that we proved the above in lecture for the function $f(\gamma) = \gamma^2 - \epsilon$)

Let $\epsilon_0 = \sqrt{d/q}$ and $\delta \in (\epsilon_0, 1)$. Set $\delta' = f(\delta - \epsilon_0) - \epsilon_0 \geq 2\epsilon_0$. Prove that for any function $B : \mathbb{F}^m \to \mathbb{F}$, there exists a list of at most $t \leq 2/\delta'$ polynomials $Q_1, \ldots, Q_t : \mathbb{F}^m \to \mathbb{F}$ of degree at most d such that

$$\Pr_{s \in \mathcal{S}_k^m, x \in s}\left[B(s)(x) \neq B(x) \wedge (\exists i, Q_i|_s \equiv B(s))\right] \geq 1 - \delta.$$

You may assume the result of Problem 2(b). We will prove the above statement as follows. Suppose for contradiction that the statement if false.

Let $Q_1, Q_2, \ldots, Q_t$ be the list of polynomials that have at least δ' agreement with B. By Problem 2(b), $t \leq 2/\delta'$. Suppose the statement was false. Consider the following 3 events for a random $s \in \mathcal{S}_k^m$ and $x \in s$.

- $C : B(s)(x) = B(x)$
- $P : \exists i \in [t], B(x) = Q_i(x)$
- $Q : \exists i \in [t], B(s) \equiv Q_i|_s$

(a) Show that $\Pr[C \wedge \bar{S}] > \delta$. $\bar{S}$ denotes the event "not S"

(b) Argue using Schwartz-Zippel Lemma, $\Pr[C \wedge \bar{P} | \not{S}] \leq \epsilon_0$.

(c) Conclude that $\Pr[C \wedge \bar{P}] > \delta - \epsilon_0$.

(d) Construct a new oracle $B' : \mathbb{F}^m \to \mathbb{F}$ as follows: let Q' be an arbitrary polynomial of degree exactly $d + 1$. Set $B'(x)$ to be $Q'(x)$ on all points x that satisfy P and $B(x)$ otherwise. Let the space oracle of B' be the same as that of B. Show that

$$\Pr\left[B'(s)(x) = B'(x)\right] > \delta - \epsilon_0.$$

(e) Conclude from the low-degree test theorem that there exists a polynomial Q of degree at most d such that $\Pr[Q'(x) = Q(x)] \geq f(\delta - \epsilon_0)$. Argue that Q and Q' are distinct polynomials and hence,

$$\Pr[B'(x) = Q(x) \wedge B'(x) \neq B(x)] \leq \Pr[Q'(x) = Q(x)] \leq \frac{d+1}{q} \leq \epsilon_0.$$

(f) Argue that $\Pr[B(x) = Q(x) = B'(x)] \geq f(\delta - \epsilon_0) - \epsilon_0 = \delta'$.

(g) Conclude from above that there exists a $i \in [t]$ such that $Q \equiv Q_i$ (i.e., Q and Q_i are identical polynomials)

(h) Conclude that $\delta' \leq \Pr[B(x) = Q_i(x) = B'(x)] \leq \Pr[Q'(x) = Q(x)] \leq \epsilon_0$, which is a contradiction.