Probabilistically Checkable Proofs	Spring 2008

Exercise no. 3

Due: April 16th, 2008

Let us remind a few definitions that were introduced in class: In all that follows $\mathbb{F}$ is a finite field and m and k are natural numbers.

- An *affine subspace* of dimension k in $\mathbb{F}^m$ is defined by a translation vector $\vec{z} \in \mathbb{F}^m$ and k linearly independent vectors $\vec{y}_1, \ldots, \vec{y}_k \in \mathbb{F}^m$ as $\left\{ \vec{z} + \sum_{i=1}^{k} t_i \cdot \vec{y}_i \;\middle|\; t_1, \ldots, t_k \in \mathbb{F} \right\}$. For instance, a *line* is an affine subspace of dimension 1.
- *Families of affine subspaces.* Let S_k^m be the set of all affine subspaces of dimension k in $\mathbb{F}^m$.
- *Canonical representation.* With every affine subspace $s \in S_k^m$ we associate (unique) representation vectors $\vec{z}, \vec{y}_1, \ldots, \vec{y}_k \in \mathbb{F}^m$. We use $s : \mathbb{F}^k \to \mathbb{F}$ to denote the function $s(t_1, \ldots, t_k) = \vec{z} + \sum_{i=1}^{k} t_i \cdot \vec{y}_i$.
- The *agreement* of a function $f : \mathbb{F}^m \to \mathbb{F}$ with another function $\tilde{f} : \mathbb{F}^m \to \mathbb{F}$ is $agr(f, \tilde{f}) \doteq \Pr_{\vec{x} \in \mathbb{F}^m} \left[f(\vec{x}) = \tilde{f}(\vec{x}) \right]$.
- For a natural number d, the *agreement with degree* d of a function $f : \mathbb{F}^m \to \mathbb{F}$ is $agr_{\leq d}(f) \doteq \max_{p \in \mathbb{F}_{\leq d}[x_1, \ldots, x_m]} agr(f, p)$.

In class we prove the following theorem:

Theorem 1 (Weak LDT Theorem) *For every natural d, there exists $\varepsilon = O(\sqrt{\frac{d}{|\mathbb{F}|}})$, such that for any function $f : \mathbb{F}^{k+1} \to \mathbb{F}$,*

$$agr_{\leq 2d}(f) \geq \left(\mathop{\mathbf{E}}_{s \in S_k^{k+1}} \left[agr_{\leq d}(f_{|s}) \right] \right)^2 - \varepsilon$$

The purpose of this exercise is to finish the analysis of the Plane vs. Point tester by proving that Theorem 1 implies the following stronger theorem:

Theorem 2 (Strong LDT Theorem) *For every natural d, there exists $\varepsilon = (\frac{d}{|\mathbb{F}|})^{\Omega(1)}$, such that for any function $f : \mathbb{F}^{k+1} \to \mathbb{F}$,*

$$agr_{\leq d}(f) \geq \mathop{\mathbf{E}}_{s \in S_k^{k+1}} \left[agr_{\leq d}(f_{|s}) \right] - \varepsilon$$

> To prove Theorem 2 you are asked to prove each of the lemmas stated below.
> Then you are asked to show that Theorem 2 indeed follows.
> In the proofs of the lemmas, you should rely on Theorem 1 as well as on your answers to the previous exercise.

Figure 1: Instructions.

Let us define a Hyperplane vs. Point tester, similar to the Plane vs. Point tester we saw in class. In what follows $f : \mathbb{F}^{k+1} \to \mathbb{F}$ is a function and $\pi : S_k^{k+1} \to \mathbb{F}_{\leq d}[t_1, \ldots, t_k]$ is an assignment of low degree polynomials to the hyperplanes.

Hyperplane-vs.-Point-tester$^{f,\pi}$

1. Pick a hyperplane $s \in S_k^{k+1}$ and a point $\vec{x} \in s$ uniformly at random. Assume that $\vec{x} = s(t_1, \ldots, t_k)$.
2. Check whether $\pi(s)(t_1, \ldots, t_k) = f(\vec{x})$.

Figure 2: Hyperplane vs. Point tester

Let $\mathcal{L} = \{q_1, \ldots, q_l\} \subseteq \mathbb{F}_{\leq 2d}[x_1, \ldots, x_{k+1}]$ be a set of low degree polynomials. We consider two events (depending on the randomness of the tester):

1. *List agreement on point $\vec{x}$:* there exists $p \in \mathcal{L}$ such that $f(\vec{x}) = p(\vec{x})$.
2. *List agreement on hyperplane s:* there exists $p \in \mathcal{L}$ such that $\pi(s) \equiv p_{|s}$.

Lemma 3 (List decoding I) *There exists $\delta_{min} \leq (\frac{d}{|\mathbb{F}|})^{\Omega(1)}$ as follows. Fix a function $f : \mathbb{F}^{k+1} \to \mathbb{F}$. For any $\delta \geq \delta_{min}$, there is a small set $\mathcal{L} \subseteq \mathbb{F}_{\leq 2d}[x_1, \ldots, x_{k+1}]$, $|\mathcal{L}| \leq (\frac{1}{\delta})^{O(1)}$, such that for any assignment $\pi : S_k^{k+1} \to \mathbb{F}_{\leq d}[t_1, \ldots, t_k]$, the following holds for $\mathcal{L}$:*

(*) The probability that the Hyperplane vs. Point tester passes on hyperplane s and point $\vec{x} \in s$, but there is no list agreement on the point $\vec{x}$, is at most $O(\delta)$.

Lemma 4 (List decoding II) *There exists $\delta_{min} \leq (\frac{d}{|\mathbb{F}|})^{\Omega(1)}$ as follows. Fix a function $f : \mathbb{F}^{k+1} \to \mathbb{F}$. For any $\delta \geq \delta_{min}$, there exists a small set $\mathcal{L} \subseteq \mathbb{F}_{\leq 2d}[x_1, \ldots, x_{k+1}]$, $|\mathcal{L}| \leq (\frac{1}{\delta})^{O(1)}$, such that for any assignment $\pi : S_k^{k+1} \to \mathbb{F}_{\leq d}[t_1, \ldots, t_k]$, the following holds for $\mathcal{L}$:*

(**) The probability that the Hyperplane vs. Point tester passes on hyperplane s and point $\vec{x} \in s$, but there is no list agreement on the hyperplane s, is at most $O(\delta)$.

If $\mathcal{L} \subseteq \mathbb{F}_{\leq 2d}[x_1, \ldots, x_{k+1}]$ satisfies (**), then we say that $\mathcal{L}$ is a *list decoding* of f for parameter δ. Note that a function f may have many different list decodings for a parameter δ.

In the following lemma, you should find concrete and suitable δ_{min} and l_{max}:

Lemma 5 (Agreement increase) *There exist a fraction $\varepsilon = (\frac{d}{|\mathbb{F}|})^{\Omega(1)}$ and a fraction $\delta_{min} \leq (\frac{d}{|\mathbb{F}|})^{\Omega(1)}$, as well as a decreasing function $l_{max} : (0,1] \to \mathbb{R}^+$ that satisfies $l_{max}(\delta) \geq (\frac{1}{\delta})^{\Omega(1)}$, as follows.*

For any function $f : \mathbb{F}^{k+1} \to \mathbb{F}$, for any fraction $\delta \geq \delta_{min}$, for every list decoding of f for parameter δ, $\{q_1, \ldots, q_l\} \subseteq \mathbb{F}_{\leq 2d}[x_1, \ldots, x_{k+1}]$, where $l \leq l_{max}(\delta)$, there exists $i \in [l]$, such that

$$agr(f, q_i) \geq \mathop{\mathbf{E}}_{s \in S_k^{k+1}} \left[agr_{\leq d}(f_{|s}) \right] - O(\delta + \varepsilon)$$

Lemma 6 (Degree decrease) *For any assignment $\pi : S_k^{k+1} \to \mathbb{F}_{\leq d}[t_1, \ldots, t_k]$ and polynomial $q \in \mathbb{F}_{\leq 2d}[x_1, \ldots, x_{k+1}]$,*

$$\Pr_{s \in S_k^{k+1}} \left[q_{|s} \equiv \pi(s) \right] \geq \frac{2d+1}{|\mathbb{F}|} \quad \Rightarrow \quad \deg q \leq d$$