Limits of Approximation Algorithms 25 Mar, 2010 (TIFR)

Lec. 8: Low degree testing (Part II)

Lecturer: Prahladh Harsha *Scribe: Nutan Limaye*

In this lecture[1], we will continue the discussion on low-degree testing and prove the soundness of the plane-point test of Raz and Safra [RS97]. For the proof of the Raz-Safra low-degree test theorem, we will follow the presentation along the lines of that by Moshkovitz and Raz [MR08].

8.1 Recap from last lecture

Plane-Point Test

Inputs: $f : \mathbb{F}^m \to \mathbb{F}, \mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^2$.

1. Pick a plane at random, $s \in S_2^m$.
2. Query the plane oracle at this plane.
3. Pick a point x at random from s.
4. Accept if $f(x) = \mathcal{A}(s)(x)$

Our main goal was to prove the following soundness of the above test.

Theorem 8.1.1 (Soundness of Plane-point test)**.**
(decoding version) *There exists* $\varepsilon_0 = \text{poly}\left(\frac{md}{|\mathbb{F}|}\right)$ *such that for all functions* $f : \mathbb{F}^m \to \mathbb{F}$*, if there exists a plane oracle* $\mathcal{A}$ *for which*

$$\Pr_{s \in \mathcal{S}_2^m, x \in s} [\mathcal{A}(s)(x) = f(x)] \geq \delta$$

then there exists a degree d *polynomial* Q *such that* $\Pr_{x \in \mathbb{F}^m} [Q(x) = f(x)] \geq \delta - \varepsilon_0$.

or equivalently

(list-decoding version) *There exists* $\varepsilon_0 = \text{poly}\left(\frac{md}{|\mathbb{F}|}\right)$*. Let* $f : \mathbb{F}^m \to \mathbb{F}$ *be a function and* $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^2$ *a planes oracle. For every* $\delta > \varepsilon_0$ *there exist* $t \leq O(1/\delta)$ *polynomials* $Q^1, \ldots, Q^t : \mathbb{F}^m \to \mathbb{F}$ *such that*

$$\Pr_{s \in \mathcal{S}_2^m, x \in s} \left[\mathcal{A}(s)(x) = f(x) \text{ and } \nexists i \in [t], Q^i{}_{|_s} \equiv \mathcal{A}(s)\right] \leq \delta.$$

[1] Prahladh: These notes are far more detailed than the lecture it corresponds to. Thanks to the scribe Nutan for filling in all the missing details in the lecture.

We also need to prove the equivalence between the two versions. In the last lecture, we showed that to prove the above theorem, it suffices to prove the following.

Theorem 8.1.2. *There exists* $\varepsilon_0 = \text{poly}\left(\frac{d}{|\mathbb{F}|}\right)$ *such that for all functions* $f : \mathbb{F}^3 \to \mathbb{F}$*, if there exists a planes oracle* $\mathcal{A} : \mathcal{S}_2^3 \to \mathcal{P}_d^2$ *for which*

$$\Pr_{s \in \mathcal{S}_2^3, x \in s} [\mathcal{A}(s)(x) = f(x)] \geq \delta$$

then there exists a degree d *polynomial* Q *such that* $\Pr_{x \in \mathbb{F}^m} [Q(x) = f(x)] \geq \delta^2 - \varepsilon_0$.

As mentioned in last lecture, the above theorem falls short in the following aspect: the agreement is only δ^2 instead of δ. For the purpose of this lecture, we will gloss over this shortcoming (this is however fixed in the appendix).

8.2 Properties of the plane oracle

The plane oracle $\mathcal{A}$ is said to be *consistent* on two intersecting planes s_1, s_2 if the polynomials given by the oracle for the two planes when restricted to the line $s_1 \cap s_2$ are the same. We denote it by $\mathcal{A}(s_1) \equiv \mathcal{A}(s_2)$.

Let $\mathcal{A}$ be a fixed oracle. Consider the following graph $G_{\mathcal{A}}$: the vertex set, $V_{\mathcal{A}}$, consists of planes $\mathcal{S}_2^3$ and edge set is given by $E_{\mathcal{A}} = \{(s_1, s_2) \mid \mathcal{A} \text{ is consistent on } s_1, s_2\}$. We first observe that if a pair of vertices is not an edge in the graph, then the number of common neighbors between these two vertices is small.

Claim 8.2.1 (Non-edges have few neighbours)**.** *For every non-edge* $(s_1, s_2) \notin E$*,*

$$\Pr_{s_3} [(s_1, s_3) \in E \text{ and } (s_2, s_3) \in E] \leq \frac{d+1}{|\mathbb{F}|}.$$

Proof. Since $(s_1, s_2) \notin E$, we have $\mathcal{A}(s_1)(l) \neq \mathcal{A}(s_2)(l)$ where l denotes the line $s_1 \cap s_2$. . We will say that the plane s_3 is unlucky if $l \in s_3$ or s_3 is parallel to l. This means that the normal vector of s_3 is perpendicular to l. This happens with probability at most $1/q$, where q denotes $|\mathbb{F}|$. Otherwise s_3 interests l in a point. We call such an s_3 lucky. With probability at least $1 - d/q$, this point is an point of disagreement between $\mathcal{A}(s_1)(l)$ and $\mathcal{A}(s_2)(l)$ by Shwartz-Zippel. Hence, $\Pr[(s_1, s_3) \in E \text{ and } (s_2, s_3) \in E \mid s_3 \text{ is lucky}] \leq d/q$. Therefore we have the claim. □

We will now show that any graph that has the above property (very few common neighbors between endpoints of a non-edge) can be decomposed into a union of cliques by throwing very few edges.

Lemma 8.2.2 (Decomposition of consistency graph into cliques)**.** *Let* G *be a graph such that between any two vertices that do not share an edge, the number of common neighbors is* $\varepsilon|V|$*, then the vertex set of* G *can be partitioned,* $V = \cup_i V_i$*, such that*

- *For all i, either $|V_i| = 1$ or V_i is a clique and $|V_i| > 2\sqrt{\varepsilon}|V|$*
- $\Pr_{(u,v)\in V^2}[(u,v) \notin E \text{ or } \exists i : (u,v) \in V_i] \geq 1 - 5\sqrt{\varepsilon}$

Proof. Keep applying one of the following two steps to the graph G till neither of them can be applied any more:
I_1: If a vertex v has degree less than $2\sqrt{\varepsilon}|V|$ then delete all the edges out of v.
I_2: Else consider the BFS tree rooted at v and remove all the edges between the first and the second layer in the tree.

The step I_1 gives rise to singletons. These singletons are never reconsidered by the algorithm. The step I_2 partitions the graph and reduces the number of non-edges by at least 1. When none of them can be applied anymore each resulting component of the graph has no non-edges to be removed, i.e. they are either singletons or cliques. Now let's bound the number of edges removed in the process:

The number of edges removed by I_1 is $\leq 2\sqrt{\varepsilon}|V|^2$ (for each vertex at most $2\sqrt{\varepsilon}|V|$ edges are removed.)

The number of edges removed in I_2: Let $v_1, \ldots, v_l$ be the sequence of vertices on which step I_2 is performed. Consider any $v = v_i$ for some $i \in [l]$. Let $N(v)$ and $N^2(v)$ denote the vertices in the layers 1 and 2 respectively, in the BFS tree of v. Step I_2 removes all edges between $N(v)$ and $N^2(v)$. Notice that steps I_1 and I_2 keep splitting the graph into disjoint components and a pair of vertices that are removed in one stage are never considered again later. For this reason, $\sum_{i=1}^{l} |N(v_i)| \cdot |N^2(v_i)| \leq |V|^2$. For each $u \in N^2(v)$ such that (v,u) is not an edge, there are at most $\varepsilon|V|$ vertices in $N(v)$ adjacent to u (hypothesis).

$$\begin{aligned}
\text{Number of edges removed in } I_2 &\leq \sum_{i=1}^{l} |N^2(v_i)| \cdot \varepsilon|V| \\
&\leq \sum_{i=1}^{l} |N^2(v_i)| \cdot \varepsilon \frac{|N(v_i)|}{2\sqrt{\varepsilon}} \qquad \text{as } |N(v_i)| > 2\sqrt{\varepsilon}|V| \\
&= \frac{\sqrt{\varepsilon}}{2} \sum_{i=1}^{l} |N(v_i)| \cdot |N^2(v_i)| \\
&\leq \frac{\sqrt{\varepsilon}}{2}|V|^2
\end{aligned}$$

Thus the total number of edges removed is at most $5/2\sqrt{\varepsilon}|V|^2$. The lemma follows as we are considering all pairs of vertices (i.e., both (u,v) and (v,u)). □

At this point, we have decomposed the consistency graph corresponding to $\mathcal{A}$ into cliques which explains almost all the consistency between a random pair of planes in $\mathcal{A}$. Consider any clique in $G_{\mathcal{A}}$. All the planes in this clique are mutually consistent, i.e., they are pairwise consistent with each other. Intuitively, if the clique is large enough, this must be because there is a global polynomial from which all plane polynomials arise. This intuition is formalized in the following lemma.

Lemma 8.2.3 (Large cliques $\implies$ global polynomial)**.** *Let $U \subseteq V$ be a clique in $G_{\mathcal{A}}$ and $|U| \geq \frac{2d+1}{q}|V|$. Then there exists a polynomial Q of degree at most d, such that for all $s \in U$, $\mathcal{A}(s) \equiv Q_{|s}$.*

We do not have time to prove the above lemma, it follows from a simple interpolation (see Appendix A for details). The number of large cliques is small. Therefore, we will get a small list of polynomials, each polynomial explaining the agreement for one clique. Thus combining Lemma 8.2.2 and Lemma 8.2.3, we get the following theorem (list decoding version).

Lemma 8.2.4. *There exists $\delta_0 = O\left(\sqrt{\frac{d}{q}}\right)$ such that for all $\delta > \delta_0$, there exists a list of $4/\delta$ polynomials $Q^1, Q^2, \ldots, Q^{4/\delta}$, each of degree at most d such that*

$$\Pr_{s_1,s_2}\left[(s_1,s_2) \notin E_{\mathcal{A}} \text{ or } \exists i : Q^i_{|s_1} \equiv \mathcal{A}(s_1) \text{ and } Q^i_{|s_2} \equiv \mathcal{A}(s_2)\right] \geq 1-\delta$$

Proof. Let $\delta_0 = \max\left\{\frac{\sqrt{\varepsilon}}{4}, \frac{4(2d+1)}{q}\right\}$ and $\delta > \delta_0$. Let a clique be called small if it has less than $\frac{\delta}{4}|V|$ number of vertices. The number of edges in any small clique is therefore upper bounded by $\frac{\delta}{4}|V|^2$. Therefore we have,

$$\Pr_{(s_1,s_2)}[(s_1,s_2) \text{ belong to a small clique}] \leq \frac{\delta}{4} \tag{8.2.1}$$

Let $L_1, L_2, \ldots, L_t$ be large cliques. As the number of vertices in each large clique is $> \frac{\delta}{4}|V|$, the number of such large cliques $t \leq \frac{4}{\delta}$. We have from Lemma 8.2.2 and (8.2.1) that

$$\Pr_{(s_1.s_2)}[(s_1,s_2) \notin E_{\mathcal{A}} \text{ or } \exists i : (s_1,s_2) \in L_i] \geq 1 - 5\sqrt{\varepsilon} - \frac{\delta}{4} \geq 1-\delta,$$

since $\delta \geq \sqrt{\varepsilon}/4$. Using Lemma 8.2.3, if $\frac{\delta}{4} \geq \frac{2d+1}{|\mathbb{F}|}$ then for each large clique L there is an associated polynomial Q of degree $\leq d$ such that for for all $s \in L$, we have $Q_{|s} \equiv \mathcal{A}(s)$. Therefore, the statement

$$\Pr_{(s_1.s_2)}[(s_1,s_2) \notin E_{\mathcal{A}} \text{ or } \exists i : (s_1,s_2) \in L_i] \geq 1-\delta$$

can be rewritten as

$$\Pr_{(s_1.s_2)}\left[(s_1,s_2) \notin E_{\mathcal{A}} \text{ or } \exists i : Q^i_{|s_1} \equiv \mathcal{A}(s_1) \text{ and } Q^i_{|s_2} \equiv \mathcal{A}(s_2)\right] \geq 1-\delta,$$

where Q^i is the polynomial of degree d associated with the large clique L_i. □

8.3 Analysis of the plane-point test

The analysis from the previous section says that *most* of the agreement of the plane oracle is explained by *few* polynomials. But this tells us nothing about the point oracle. In this section, we will show the soundness of the plane-point test. More precisely, we will show

the following. Let $\mathcal{A}$ be a plane oracle and f a point-oracle satisifying the plane-point test with probability at least γ, ie., $\Pr[\mathcal{A}(s)(x) = f(x)] \geq \gamma$. Then, there exists a degree d polynomial Q such that $\Pr[f(x) = Q(x)] \geq \gamma^2 - \varepsilon_0$.

A plane oracle $\mathcal{A}$ is said to be α-good, if $\Pr_{s_1,s_2}[\mathcal{A}(s_1) \equiv \mathcal{A}(s_2)] \geq \alpha$.

Lemma 8.3.1 (If the plane-point test passes with good probability then there exists a *good* planes oracle.)**.** *For any plane oracle* $\mathcal{A}$

$$\Pr_x[\mathcal{A}(s)(x) = f(x)] \geq \gamma \Rightarrow \mathcal{A} \text{ is } (\gamma^2 - d/q - 1/q)\text{-good}$$

Proof. Let $H = (U_H \cup V_H, E_H)$ be a bipartite graph where U_H consists of points from $\mathbb{F}^m$ and V_H consists of set of all planes. Let (x, s) be an edge if $x \in s$. Note that this graph is regular on both the partitions. Let an edge be called *good* if the plane-point test passes on this edge, i.e. $A(s)(x) = f(x)$. There are at least γ fraction of good edges. For a fixed x_i, let γ_i denote $\Pr_s[\mathcal{A}(s)(x_i) = f(x_i)]$. Therefore, we know that $\frac{1}{|U_H|}\sum_{i=1}^{q^m} \gamma_i = \gamma$.

$$\mathop{\mathbb{E}}_{x \in U_H}[\Pr_{s_1,s_2 \in V_H}[\mathcal{A}(s_1)(x) = f(x) = \mathcal{A}(s_2)(x)]] = \frac{1}{|U_H|}\sum_i \gamma_i^2$$

But sum of squares is at least as large as square of the sums. Therefore,

$$\mathop{\mathbb{E}}_{x \in U_H}[\Pr_{s_1,s_2 \in V_H}[\mathcal{A}(s_1)(x) = f(x) = \mathcal{A}(s_2)(x)]] \geq \gamma^2$$

It may happen that $\mathcal{A}(s_1) \not\equiv \mathcal{A}(s_2)$ but $\mathcal{A}(s_1)(x) = f(x) = \mathcal{A}(s_2)(x)$. However, due to Swartz-Zippel this will happen with very small probability. Therefore, we have

$$\mathop{\mathbb{E}}_{x \in U_H}[\Pr_{s_1,s_2 \in V_H}[\mathcal{A}(s_1) \equiv \mathcal{A}(s_2)]] \geq \gamma^2 - \frac{d}{q}$$

Also, with probability $1/q$, the two planes may be non-intersecting. Therefore,

$$\Pr_{s_1,s_2 \in V_H}[\mathcal{A}(s_1) \equiv \mathcal{A}(s_2)]] \geq \gamma^2 - \frac{d}{q} - \frac{1}{q}$$

□

Note that, the *goodness* of the plane oracle $\mathcal{A}$ directly translates to many edges in the graph $G_{\mathcal{A}}$. Intuitively, more edges in $G_{\mathcal{A}}$ means more large cliques, which in turn means fewer polynomials explaining the edges/agreement due to Lemma 8.2.4.

Given f and $\mathcal{A}$, let $Q^1, \ldots, Q^{4/\delta}$ be the list of degree d polynomials that explains the success of the planes oracle $\mathcal{A}$ as in Lemma 8.2.4. Pick a point x at random and pick two planes s_1, s_2 passing through it at random. Consider the following events.

$$\begin{array}{lcl} X & : & \mathcal{A}(s_1)(x) = f(x) = \mathcal{A}(s_2)(x) \\ E & : & \text{There exists an } i \in [4/\delta] \text{ such that } Q^i_{|s_1} \equiv \mathcal{A}(s_1) \text{ and } Q^i_{|s_2} \equiv \mathcal{A}(s_2) \\ C & : & (s_1, s_2) \in E_{\mathcal{A}}. \end{array}$$

We are interested in the probability of the event $X \wedge E$. We know that $\Pr_{x,s_1,s_2}[X] \geq \gamma^2$ (Lemma 8.3.1). And we also know that $\Pr[\neg C \wedge E] \geq 1 - \delta$ (Lemma 8.2.4).

$$\begin{aligned}
\Pr_{x,s_1,s_2}[X \wedge \neg E] &= \Pr_{x,s_1,s_2}[C \wedge X \wedge \neg E] + \Pr_{x,s_1,s_2}[\neg C \wedge X \wedge \neg E] \\
&\leq \Pr_{x,s_1,s_2}[C \wedge \neg E] + \Pr_{x,s_1,s_2}[\neg C \wedge X] \\
&\leq \delta + \Pr_{x,s_1,s_2}[X | \neg C] \\
&\leq \delta + \tfrac{d+1}{q}
\end{aligned}$$

(the last step: (s_1, s_2) not an edge but still X happen for two reasons; (1) s_1 and s_2 are parallel which happens with probability at most $1/q$ and (2) s_1 and s_2 intersect on a line they disagree but x happens to be a point of agreeement on this line which occurs with probability at most d/q by Schwartz-Zippel.)

Therefore,

$$\Pr_{x,s_1,s_2}[X \wedge E] \geq \gamma^2 - 2\delta \tag{8.3.1}$$

We have shown that there is a short list of polynomials which "explains" the success of the low-degree test. However, this is not the "explanantion" we had sought after as stated in Theorem 8.1.1. What we will now show is that the above explanation actually implies a list-decoding explanation of the right form for a related lines-oracle $\tilde{\mathcal{A}}$ and not the planes oracle $\mathcal{A}$. We will then use the equivalence between the list-decoding version and the decoding version of the low-degree test soundness to obtain a single polynomial that explains the success of the plane-point test. The lines-oracle $\tilde{\mathcal{A}}$ is constructed as follows. The lines-oracle $\tilde{\mathcal{A}}$ as expected uses the planes-oracle $\mathcal{A}$ as sub-oracle. A point to be noted is that the lines-oracle $\tilde{\mathcal{A}}$ is randomized.

LINES-ORACLE $\tilde{\mathcal{A}}$

Input: a line $l \in \mathcal{S}_1^3$.

1. Randomly choose two planes s_1, s_2 such that $l = s_1 \cap s_2$.
2. If there exists a $i \in [4/\delta]$ such that $Q^i_{|_{s_1}} \equiv A(s_1)$ and $Q^i_{|_{s_2}} \equiv A(s_2)$ then output the polynomial Q^i restricted on l.
3. Else output $\perp$.

Now for this lines-oracle $\tilde{\mathcal{A}}$ it is easy to see that the list of polynomials $Q^1, \ldots, Q^{4/\delta}$ completely explain the success of the lines-point test (in fact with probability 1).

$$\Pr_{l,x,\tilde{\mathcal{A}}}\left[\tilde{\mathcal{A}}(l)(x) \neq f(x) \text{ or } \exists i : Q^i_{|_l} \equiv \tilde{\mathcal{A}}(l)\right] = 1$$

This happens since if there does not exist a polynomial Q^i such that $\tilde{\mathcal{A}}(l) \equiv Q^i_{|_l}$, then the lines-oracle $\tilde{\mathcal{A}}$ returns $\perp$ and hence the lines-point test "$\tilde{\mathcal{A}}(l)(x) = f(x)$" fails.

Thus, the lines-oracle $\tilde{\mathcal{A}}$ satisfies the list-decoding version of the low-degree test theorem and hence by equivalence to the standard version, we have that it satisfies the standard version, ie., if the lines-point test "$\tilde{\mathcal{A}}(l)(x) = f(x)$" passes with significant probability, then there exists a low-degree polynomial that explains the points oracle. Thus, to show there exists a low-degree polynomial that explains the points oracle, it suffices to prove two things: (1) the list-decoding version implies the standard version of the low-degree test and (2) the lines-point test "$\tilde{\mathcal{A}}(l)(x) = f(x)$" passes with significant probability.

Proposition 8.3.2 (list-decoding to decoding)**.** *Let $f : \mathbb{F}^m \to \mathbb{F}$ be a function and $\mathcal{A} : \mathcal{S}_k^m \to \mathcal{P}_d^2$ (possibly randomized) such that*

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

where the probability is also taken over the randomness of the oracle $\mathcal{A}$. Furthermore suppose that for some $\delta \geq \text{poly}(d/q)$ that there exist $t \leq O(1/\delta)$ polynomials $Q^1, \ldots, Q^t : \mathbb{F}^m \to \mathbb{F}$ that explains almost all the success of the low-degree test, i.e.,

$$\Pr_{s \in \mathcal{S}_2^m, x \in s}\left[\mathcal{A}(s)(x) = f(x) \text{ and } \nexists i \in [t], Q^i{}_{|_s} \equiv \mathcal{A}(s)\right] \leq \delta.$$

Then, there exists $i \in [t]$, such that $\Pr_x\left[f(x) = Q^i(x)\right] \geq \gamma - \delta - \text{poly}\left(\frac{d}{q}\right)$.

We will defer the proof of this proposition to the next section and complete the analysis of the plane-point test assuming it.

Since, the plane-point test passes with probability at least γ, we have from Equation 8.3.1 that $\Pr[X \wedge E] \geq \gamma^2 - 2\delta$ which when written in the language of the line-oracle $\tilde{\mathcal{A}}$ translates to the following.

$$\mathop{\mathbb{E}}_{\tilde{A}}\left[\mathop{\mathbb{E}}_{l}\left[\Pr_{x \in l}\left[\tilde{\mathcal{A}}(l)(x) = f(x)\right]\right]\right] \geq \gamma^2 - 2\delta \tag{8.3.2}$$

And now assuming Proposition 8.3.2 holds, we get a polynomial Q of degree d such that it agrees with $f(x)$ with probability at least $\gamma^2 - 2\delta - \text{poly}(d/q) = \gamma^2 - \varepsilon_0$, where $\varepsilon_0 = \text{poly}(d/q)$. This completes the proof of Theorem 8.1.2

8.4 List decoding version to standard version

In this section, we prove the list-decoding version of the low-degree test implies the standard version (i.e., Proposition 8.3.2). The converse is also true (see Appendix B.1 for details).

Note that this proposition works for both planes ($\mathcal{S}_2^m$) as well as lines $\mathcal{S}_1^m$).

Proof of Proposition 8.3.2. Suppose we are given a oracle $\tilde{\mathcal{A}}$ (possibly randomized) and points-oracle f such that there exists a list of functions $Q^1, \ldots, Q^t : \mathbb{F}^m \to \mathbb{F}$ such that

$$\Pr_{s,x,\tilde{\mathcal{A}}}\left[\tilde{\mathcal{A}}(s)(x) \neq f(x) \text{ or } \exists i : Q^i_{|_s} \equiv \tilde{\mathcal{A}}(s)\right] \geq 1 - \delta$$

Assume for the sake of contradiction,

$$\forall i \in t : \quad \Pr_x[f(x) = Q(x)] < \gamma - \delta - 2\varepsilon$$

where ε is a parameter to be decided.

Now we will prove that

$$\mathop{\mathbb{E}}_{\tilde{A}}\left[\mathop{\mathbb{E}}_{s}\left[\Pr_{x \in s}\left[\tilde{\mathcal{A}}(s)(x) = f(x)\right]\right]\right] < \gamma$$

which will prove the proposition.

Let for each $i \in [t]$, $T_i := \{x \mid Q_i(x) = f(x)\}$. By assumption $|T_i|/q^m \leq \gamma - \delta - 2\varepsilon$ for all i.

The points in random s are pairwise independent. Applying Chebyshev's inequality, we get

$$\Pr_s \left[\frac{|s \cap T_i|}{|s|} \geq |T_i|/q^m + \varepsilon \right] \leq 1/q^2.$$

In other words, s is a good sampler of the space $\mathbb{F}^m$. We now apply union bound,

$$\Pr_s \left[\exists i \in [t] : \quad \frac{|s \cap T_i|}{|s|} \geq \gamma - \delta - \varepsilon \right] \leq t/q^2.$$

Choose ε such that $t/q^2 \leq \varepsilon$. This occurs if $\varepsilon \geq \text{poly}(d/q)$ for some fixed polynomial since $t = 4/\delta$ and $\delta = \text{poly}(d/q)$.

Now consider picking a random s and a random point $x \in s$. Consider the following events based on s and x.

B : l is a bad sampler, i.e., $\exists i \in [t] : \frac{|l \cap T_i|}{|l|} \geq \gamma - \delta - \varepsilon$.

C : $\tilde{\mathcal{A}}$ is consistent with the point oracle, i.e. $\tilde{\mathcal{A}}(s)(x) = f(x)$.

E : There exists a function Q^i that explains $\tilde{A}(s)$, i.e. $\exists i : Q^i_{|_s} \equiv \tilde{\mathcal{A}}(s)$.

We have that $\Pr_s[B] \leq \varepsilon$ and $\Pr_{\tilde{\mathcal{A}},s,x}[\neg C \vee E] \geq 1 - \delta$, i.e. $\Pr_{\tilde{\mathcal{A}},s,x}[C \wedge \neg E] < \delta$. We wish to bound $\Pr_{\tilde{\mathcal{A}},s,x}[C]$.

$$\begin{aligned} \Pr_{\tilde{\mathcal{A}},s,x}[C \wedge E] &= \Pr_{\tilde{\mathcal{A}},s,x}[C \wedge E \wedge B] + \Pr_{\tilde{\mathcal{A}},s,x}[C \wedge E \wedge \neg B] \\ &\leq \Pr_s[B] + \Pr_{\tilde{\mathcal{A}},s,x}[C | E \wedge \neg B] \\ &\leq \varepsilon + \gamma - \delta - \varepsilon \\ &\leq \gamma - \delta \end{aligned}$$

Therefore, $\Pr_{\tilde{\mathcal{A}},s,x}[C] < \gamma$ which is a contradiction. □

References

[MR08] Dana Moshkovitz and Ran Raz. *Sub-constant error low degree test of almost-linear size*. SIAM J. Computing, 38(1):140–180, 2008. (Preliminary Version in *38th STOC*, 2006). eccc:TR05-086, doi:10.1137/060656838.

[RS97] Ran Raz and Shmuel Safra. *A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP*. In *Proc. 29th ACM Symp. on Theory of Computing (STOC)*, pages 475–484. 1997. doi:10.1145/258533.258641.

A Interpolating cliques to polynomials

Recall that in Section Section 8.2, we defined a graph $G_{\mathcal{A}}$ corresponding to a plane-oracle $\mathcal{A}$. Let $\mathcal{A}$ be a fixed oracle. The vertex set, $V_{\mathcal{A}}$, of $G_{\mathcal{A}}$ consists of planes $\mathcal{S}_2^3$ and edge set is given by $E_{\mathcal{A}} = \{(s_1, s_2) \mid \mathcal{A} \text{ is consistent on } s_1, s_2\}$.

In this section we will prove that the existence of a large clique in $G_{\mathcal{A}}$ implies that there exists a polynomial Q which when restricted to each plane s in the clique agrees with $\mathcal{A}(s)$, i.e. there is a single polynomial that "explains" all the planes in the clique. Moreover, such a polynomial has "small" degree. We will first use interpolation to show that the polynomial has degree at most $2d$ and then use Schwartz-Zippel to further reduce the degree to d.

Lemma A.1 (Large cliques $\implies$ global polynomial)**.** *Let $U \subseteq V$ be a clique in $G_{\mathcal{A}}$ and $|U| \geq \frac{2d+1}{q}|V|$. Then there exists a polynomial Q of degree at most $2d$, such that for all $s \in U$, $\mathcal{A}(s) \equiv Q_{|s}$.*

Proof. As U is a clique in $G_{\mathcal{A}}$, for all $s_1, s_2 \in U$, $\mathcal{A}(s_1) \equiv \mathcal{A}(s_2)$.

We say that a plane is *along* a direction v if the normal to the plane is parallel to v. First, we observe that there exists a direction (say v) along which there are at least $2d+1$ planes in U. The assumption on the size of the clique implies that there are at least $\frac{2d+1}{q}|V|$ many planes. Note that,

$$\begin{aligned} |V| &= \#\text{2-dimensional subspaces} \times \#\text{ affine shifts} \\ &= \tfrac{(q^3-1)(q^3-q)}{(q^2-1)(q^2-q)} \times q \\ &= q(q^2+q+1) \end{aligned}$$

Therefore, we have that in U there are at least $(2d+1)(q^2+q+1)$-many planes. The number of directions is equal to the number of 1-dimensional subspaces in $\mathbb{F}_q^3$, i.e $\frac{q^3-1}{q-1} = q^2+q+1$. Hence there is a direction (say v) along which there are at least $2d+1$ planes. This direction could have at most q planes leaving at least $(2d+1)(q^2+q+1)-q \geq (d+1)(q^2+q)$ planes in U in directions other than v which are themselves q^2+q in number. Hence, there is another direction (say w) along which there are at least $d+1$-many planes.

By a change of axes, we can assume that the direction w is e_x and v is e_y. Let S_x (S_y) be the set of planes along the direction e_x (e_y, respectively). Let $S_x = \{s_0, s_1, \ldots, s_d\}$ and $S_y = \{s'_0, s'_1, \ldots, s'_t\}$. From above we know that $2d \leq t \leq q-1$. We will first find a polynomial that agrees with the above $(d+1)$ planes in S_x as follows. For all $0 \leq i \leq d$, let the plane s_i be given $x = a_i$ and let $P_i(y,z)$ denote $\mathcal{A}(s_i)$. Also, let us define $f_i(x)$ for each i as follows:

$$f_i(x) = \frac{\prod_{0 \leq j \leq d; j \neq i}(x - a_j)}{\prod_{0 \leq j \leq d; j \neq i}(a_i - a_j)}$$

Now, let $Q(x,y,z) = \sum_{i=0}^{d} P_i(y,z) f_i(x)$

Note that Q is a degree $2d$ polynomial and for all i, $0 \leq i \leq d$: $Q(a_i, y, z) = P_i(y,z)$, i.e. Q "explains" the $(d+1)$ planes in S_x (and S_x is a subset of U).

We will now prove that the same polynomial Q explains all the planes in S_y. Consider one of the planes in S_y, say s. Let R denote $\mathcal{A}(s)$. Recall that R is a degree d polynomial. Therefore, R restricted to any line $l \in s$ is also a degree d polynomial. We partition s into lines.

$$s = \bigcup_{c \in \mathbb{F}_q} l_{z=c}$$

where, $l_{z=c}$ is the line $s_{|_{z=c}}$ for $c \in \mathbb{F}_q$. Now observe that Q restricted to any line $l_{z=c}$ is a univariate polynomial in x and has degree d. As $\{s\} \cup S_x \subseteq U$, we know that for all $0 \leq i \leq d$: $\mathcal{A}(s) \equiv \mathcal{A}(s_i)$. Therefore R and Q agree on at least $d+1$-many points on $l_{z=c}$ and are each degree at most d when restricted to $l_{z=c}$. Therefore by Schwartz-Zippel they must be the same polynomial restricted to $l_{z=c}$. And hence Q restricted to s is R, i.e. Q explains s. Thus, Q explains all planes s in S_y. We have now explained all the planes in U which lie in S_y (ie., have direction along e_y). Any other plane s in U (including the ones

with direction along e_x) intersect all the planes in S_y. Thus, for at least $(2d+1)/q$ fraction of points in s, $\mathcal{A}(s)$ agrees with Q. Hence, $\mathcal{A}(s) \equiv Q_{|_s}$. □

We have thus used interpolation to show that there exists a polynomial of degree at most $2d$ that agrees with the planes in U. However, the restriction of this polynomial to all planes in U is a degree d polynomial and not a degree $2d$ polynomial. We will use this fact to further reduce the degree of Q from $2d$ to d.

Lemma A.2 (degree reduction)**.** *Suppose there exists a polynomial Q of degree D such that*

$$\Pr_{s \in \mathcal{S}_2^m}\left[Q|_s \in \mathcal{P}_d^2\right] > \frac{D}{q}$$

then Q is in fact a degree d polynomial.

Proof. Let s be a plane given by $a, b, c \in \mathbb{F}^m$ consisting of the following points.

$$s = \{a + bt_1 + ct_2 \mid t_1, t_2 \in \mathbb{F}\}$$

Let $Q^{=D}$ be the degree D homogeneous part of Q. $Q^{=D} \neq 0$ by our assumption. $Q^{=D}|_s$ is a bivariate polynomial in t_1, t_2. The coefficient of t_1^D in $Q^{=D}|_s$ is $Q^{=D}(b)$, which is an m-variate polynomial in b of degree D and is not identically zero. $Q^{=D}|_s$ is a zero poynomial if coefficient of each $t_1^i t_2^j$ term appearing in $Q^{=D}|_s$ is zero. If we have an upper bound for the probability of one of them being zero, that gives an upper bound for $\Pr_s\left[Q^{=D}|_s \equiv 0\right]$.

$$\begin{aligned}\Pr_s\left[Q^{=D}|_s \equiv 0\right] &\leq \Pr_{a,b,c}\left[\text{coefficient of } t_1^D \text{ is zero}\right] \\ &= \Pr_b\left[Q^{=D}(b) \equiv 0\right] \\ &\leq \tfrac{D}{q}\end{aligned}$$

The last inequality is due to Schwartz-Zippel. □

B Fixing the parameters: from γ^2 to γ

In this section, we will show how we can improve the agreement from $\gamma^2 - \varepsilon_0$ to $\gamma - \varepsilon_0'$ (of course for $\varepsilon_0' \geq \varepsilon_0$). This will use the equivalence between the standard version of the low-degree test and the list-decoding version. Recall that we proved in lecture that the list-decoding version implies the standard version (Proposition 8.3.2). We now show that the other direction also holds.

B.1 Standard version implies list-decoding version

Proposition B.1 (decoding to list-decoding)**.** *Let $d \in \mathbb{Z}^{\geq 0}$. Let $f : \mathbb{F}^m \to \mathbb{F}$ be a function. Suppose f satisfies the low-degree test theorem, i.e., there exists some $\alpha : [0,1] \to [0,1]$ such that for every planes oracle $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^m$, we have*

$$\Pr[\mathcal{A}(s)(x) = f(x)] \geq \gamma \implies \exists Q \in \mathcal{P}_d^m, \Pr[f(x) = Q(x)] \geq \alpha(\gamma).$$

Then, f also satisfies the list-decoding version. In other words, there exists $\varepsilon_0 = poly(d/q)$ such that for all $\delta > \varepsilon_0$ and $\delta' = \alpha(\delta - \varepsilon_0) - \varepsilon_0 \geq 2\varepsilon_0$ such that for every planes oracle

$\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^m$ *there exists a list of* $t \leq 2/\delta'$ *polynomials* $Q^1, \ldots, Q^t : \mathbb{F}^m \to \mathbb{F}$ *of degree* d *such that*

$$\Pr_{s \in \mathcal{S}_2^m, x \in s}\left[\mathcal{A}(s)(x) = f(x) \text{ and } \nexists i \in [t], {Q^i}_{|_s} \equiv \mathcal{A}(s)\right] \leq \delta.$$

This was problem 7 in problem set 2. For completeness, we reproduce the proof verbatim from the paper of Moshkovitz and Raz [MR08]

Proof. Let $\varepsilon_0 = \sqrt{d/q}$ and $\delta \in (\varepsilon_0, 1)$. Set $\delta' = \alpha(\delta - \varepsilon_0) - \varepsilon_0 \geq 2\varepsilon_0$. We will show that for any function $f : \mathbb{F}^m \to \mathbb{F}$ and planes oracle $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^m$, 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

$$\Pr_{s \in \mathcal{S}_2^m, x \in s}\left[\mathcal{A}(s)(x) \neq f(x) \wedge \left(\exists i, Q^i_{|_s} \equiv \mathcal{A}(s)\right)\right] \geq 1 - \delta.$$

Suppose for contradiction that the statement if false.

Let $Q^1, Q^2, \ldots, Q^t$ be the list of all degree d polynomials that have at least δ' agreement with f. By lemma from last lecture, $t \leq 2/\delta'$. As we have assumed the statement is false, it is false in particular for this list of polynomials. Consider the following 3 events for a random $s \in \mathcal{S}_2^m$ and $x \in s$.

- $C : \mathcal{A}(s)(x) = f(x)$
- $P : \exists i \in [t], f(x) = Q^i(x)$
- $S : \exists i \in [t], \mathcal{A}(s) \equiv Q^i_{|_s}$

From the assumption, we have that $\Pr[C \wedge \bar{S}] > \delta$. Now suppose S does not happen, ie., for all i we have $\mathcal{A}(s) \not\equiv Q^i_{|_s}$. In this, case by Schwartz-Zippel, it cannot be the case that $\mathcal{A}(s)(x) = f(x)$ and $f(x)$ agrees with one of the polynomials Q^i at x with probability larger than td/q. Hence,

$$\Pr[C \wedge \bar{P} | \neg S] \leq \frac{td}{q} \leq \frac{2'}{\delta} \cdot \varepsilon_0^2 \leq \frac{1}{\varepsilon} \cdot \varepsilon_0^2 \leq \varepsilon_0.$$

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

$$\begin{aligned}
\Pr\left[\mathcal{A}(s)(x) = f'(x)\right] &\geq \Pr[\left[\mathcal{A}(s)(x) = f(x) \wedge f(x) = f'(x)\right] \\
&\geq \Pr\left[C \wedge \neg P\right] \\
&\geq \Pr\left[C \wedge \neg P \wedge \neg S\right] \\
&= \Pr[C \wedge \neq S] - \Pr[C \wedge P \wedge \neq S] \\
&> \delta - \Pr[C \wedge P | \neq S] \\
&\geq \delta - \varepsilon_0
\end{aligned}$$

We now apply the standard version of the low-degree test theorem to the points oracle f' and plane oracle $\mathcal{A}$ to conclude that there exists a polynomial Q of degree at most d such that $\Pr[f'(x) = Q(x)] \geq \alpha(\delta - \varepsilon_0)$. Note that Q and Q' are distinct polynomials and hence,

$$\Pr[f'(x) = Q(x) \wedge f'(x) \neq f(x)] \leq \Pr[Q'(x) = Q(x)] \leq \frac{d+1}{q} \leq \varepsilon_0.$$

Therefore,

$$\begin{aligned}\Pr[f(x) = Q(x) = f'(x)] &= \Pr[f'(x) = Q(x)] - \Pr[f'(x) = Q(x) \wedge f'(x) \neq f(x)] \\ &\geq f(\delta - \varepsilon_0) - \varepsilon_0 = \delta'.\end{aligned}$$

Hence, f and Q agree on at least δ'-fraction of points, which implies that Q is identical to one of the polynomials Q^i in the list. Suppose $Q \equiv Q^i$. Now consider any point x such that $f(x) = Q^i(x)$, by definition at this point $f'(x) = Q'(x)$. Hence, we have that $f(x) = Q^i(x) = f'(x)$ implies $Q'(x) = Q^i(x)$. However, this leads to the following contradiction.

$$\delta' \leq \Pr[f(x) = Q^i(x) = f'(x)] \leq \Pr[Q'(x) = Q^i(x)] \leq \varepsilon_0,$$

which completes the proof of the proposition.

□

B.2 $\gamma^2 \longrightarrow \gamma$

We now return to our original goal of improving the agreement from $\gamma^2 - \varepsilon_0$ to $\gamma - \varepsilon_0'$.

Fix a point oracle $f : \mathbb{F}^m \to \mathbb{F}$. By Theorem 8.1.2, we know that f satisfies the standard version of the low-degree test theorem. In other words for all planes-oracle $\mathcal{A}$ such that $\Pr_{s \in \mathcal{S}_2^m, x \in s}[\mathcal{A}(s)(x) = f(x)] \geq \gamma$, we know that there is a degree d polynomial Q such that $\Pr_x[Q(x) = f(x)] \geq \gamma^2 - \varepsilon_0$. Hence, by Proposition B.1, f also satisfies the list-decoding version. More precisely, there exists a $\mu_0 = \text{poly}(d/q)$ such that for all $\delta > \mu_0$, and planes oracle $\mathcal{A}$, there exists a list of $t \leq O(1/\delta^2)$ polynomails $Q^1, \ldots, Q^t$ such that

$$\Pr_{s \in \mathcal{S}_2^m, x \in s}\left[\mathcal{A}(s)(x) \neq f(x) \vee \exists i : Q^i_{|_s} \equiv \mathcal{A}(s)\right] \geq 1 - \delta$$

Now suppose we are given a planes oracle $\mathcal{A}$ such that $\Pr[\mathcal{A}(s)(x) = f(x)] \geq \gamma$. We can now use the other direction (Proposition 8.3.2: list-decoding to standard) to conclude that there exists a $j \in [t]$ such that $\Pr_s\left[(Q^j(x) = f(x)\right] \geq \gamma - \mu_0 - \text{poly}(d/q) = \gamma - \varepsilon_0'$. Thus, proved.