18.408 Topics in Theoretical Computer Science Fall 2022 Lectures 7,8

Dor Minzer

Last time we presented the sum-check protocol which enabled us to test whether a given assignment $A_0\colon \mathbb{F}_q^m \to \mathbb{F}_q$ that is promised to be a low degree polynomial satisfies a given equation or not, using only $\mathsf{poly}(\log n)$ many queries. Today, we will introduce representations of low degree polynomials that enable one to test that a given table of values A_0 indeed represents a low degree polynomial using only constantly many queries. In subsequent lectures we combine this with the sum check protocol and construct a PCP with $\mathsf{poly}(\log n)$ many queries.

1 Low Degree Testing

Throughout this lecture, we are working over the field $\mathbb{F}_q$ and with the parameters $m, d \in \mathbb{N}$, where d is the total degree and m is the number of variables.

1.1 The Line versus Point Scheme

Suppose $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ is a polynomial of total degree at most d. The most natural encoding of f is its table of values; this encoding however, is not good enough for our purposes since it doesn't admit a tester with constantly many queries. A natural idea thus is to consider the table of restriction to "higher dimensional" objects than points. For example, one may consider the table of restrictions of f to *lines*.

Definition 1.1. *We define $S_1(\mathbb{F}_q^m)$ to be the set of all lines in $\mathbb{F}_q^m$. That is, $S_1(\mathbb{F}_q^m)$ is the collection of sets of the form $L_{a,b} = \{at + b \mid t \in \mathbb{F}_q\}$, for $a, b \in \mathbb{F}_q^m$.*

Note that if $L \in S_1(\mathbb{F}_q^m)$, then the restriction $f|_L$ is a univariate polynomial of degree at most d. Indeed, if the line L is parameterized as $L = \{at + b \mid t \in \mathbb{F}_q\}$, the restriction can be thought of as the univariate function $f|_L(t) = f(a + tb)$, which has degree at most d. Thus, to encode f we can specify its table of values as well as the table of restrictions of f to all lines. Namely, we can encode a polynomial f by $B_0\colon \mathbb{F}_q^m \to \mathbb{F}_q$ defined as $B_0(x) = f(x)$, as well as $B_1\colon \mathsf{Lines}(\mathbb{F}_q^m) \to \{\text{degree } d \text{ univariate polynomials}\}$ defined as $B_1[L] = f|_L$.

First, we consider the size of the encoding. Letting $N = q^m$, the number of points in $\mathbb{F}_q^m$ is N, and the number of lines in $\mathbb{F}_q^m$ is about N^2 (since a line is specified by two points), hence the size of the encoding is about $N^2 + N$, which is polynomial in the size of the original object; this is good enough for us.

Second, we discuss the local test corresponding to this encoding. The most natural test associated with this scheme is the line versus point test. In this context, our input consists of two tables B_0 and B_1 (which are supposed encodings of a low-degree polynomial f), where B_0 assigns an $\mathbb{F}_q$-value to each point x, and B_1 assigns a univariate polynomial over $\mathbb{F}_q$ of degree at most d to each line in $S_1(\mathbb{F}_q^m)$. The test is:

1. Sample a point $x \in \mathbb{F}_q^m$ randomly and take a random line $L \in S_1(\mathbb{F}_q^m)$ containing x.

2. Query $B_0(x)$ and $B_1[L]$.
3. Check that $B_1[L](x) = B_0(x)$.

The completeness of this test is clear. That is, if B_0, B_1 are the tables of some polynomial $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ of degree at most d, then the test passes with probability 1. What about the soundness?

Theorem 1.2. *Suppose that B_0, B_1 are tables that pass the line versus point test with probability at least $1-\varepsilon$. Then there exists a polynomial $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ of total degree d, such that*

$$\Pr_{x\in\mathbb{F}_q^m}[f(x) = B_0(x)] \geqslant 1 - O(\varepsilon), \qquad \Pr_{L\in S_1(\mathbb{F}_q^m)}[f|_L \equiv B_1[L]] \geqslant 1 - O(\varepsilon).$$

In words, if the test passes with probability close to 1, then the tables B_0 and B_1 are close to the tables of some low-degree polynomial f. This regime of parameters is often called the "99% regime", since it makes a structural assertion on the assignment in the case that the test passes with probability close to 1. Such results are typically easier to prove, and they have been indeed utilized in early PCP constructions. However, such results cannot directly be used towards constructing PCPs with small error (i.e. large gap between the completeness and the soundness), and for that one needs to address the so-called "1%" regime. Here, one assumes that the test passes with probability at least ε (which is small but bounded away from 0), and wants to conclude that the assignments B_0, B_1 still must have a global structure. In this regime, we have the following theorem:

Theorem 1.3. *There are absolute constants $C > 0$ and $c > 0$ such that the following holds. Suppose that B_0, B_1 are tables that pass the line versus point test with probability at least ε, where $\varepsilon \geqslant \frac{d^C m^C}{q^c}$. Then there exists a polynomial $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ of total degree d, such that*

$$\Pr_{x\in\mathbb{F}_q^m}[f(x) = B_0(x)] \geqslant \Omega(\varepsilon), \qquad \Pr_{L\in \mathit{Lines}(\mathbb{F}_q^m)}[f|_L \equiv B_1[L]] \geqslant \Omega(\varepsilon).$$

The known proofs of Theorem 1.3 are quite complicated, and we will not present them here. Part of the issue is that the structure offered to us by lines, and in particular the bipartite graph between lines and points associated with the test, lacks enough "combinatorial structure" and "expansion". Indeed, the proof of Theorem 1.3 is heavily algebraic. To circumvent this, we will consider a different (but similar in spirit) encoding schemes of low degree polynomials that are easier to analyze.

1.2 The Plane versus Line and Plane versus Point Schemes

A natural idea of the previous scheme is to consider, instead of lines, higher dimensional affine subspaces.

Definition 1.4. *We denote by $S_r(\mathbb{F}_q^m)$ the collection of all affine subspaces of $\mathbb{F}_q^m$ of dimension r. Whenever q and m are clear from context, we will drop them from the notation and simply write S_r.*

Note that letting $N = q^m$, we have that $|S_r| \approx N^r$, thus as long as r is constant, we can afford ourselves to use tables for S_r in our encodings. In this way, given a degree d polynomial $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$, we can define $B_r\colon S_r \to \{\text{total degree } d \text{ polynomial over } r \text{ variables}\}$ as $B_r[P] = f|_P$ for each $P \in S_r$. We will refer to this as the r-dimensional encoding of f.

For concreteness, we shall focus on the case that $r = 2$, in which case $S_2(\mathbb{F}_q^m)$ consists of all of the affine planes in $\mathbb{F}_q^m$. This will be good enough for our purposes, but we remark that there is some merit in considering higher r. First, we will have to do so in the analysis of the test for $r = 2$, and second, better analysis is known for larger r. Still, our focus shall be on $r = 2$.

So, if we have our (supposed) assignments B_0, B_1 to points and lines and B_2 to planes. How shall we go about testing them? The first option is the plane versus point test:

1. Sample a point $x \in \mathbb{F}_q^m$ randomly and take a plane $P \in S_2(\mathbb{F}_q^m)$ that contains x.
2. Query $B_0(x)$ and $B_2[P]$.
3. Check that $B_2[P](x) = B_0(x)$.

The second option is the plane versus line test:

1. Sample a line $L \in S_1(\mathbb{F}_q^m)$ randomly and take a plane $P \in S_2(\mathbb{F}_q^m)$ that contains L.
2. Query $B_1[L]$ and $B_2[P]$.
3. Check that $B_2[P]|_L \equiv B_1[L]$.

And yet, there are third and fourth options. Both go under the name "the plane versus plane test", but they vary in the dimension of space these planes intersect in. The first variant is the Plane versus Plane test on planes that intersect on a line:

1. Sample a line $L \in S_1(\mathbb{F}_q^m)$ randomly and take two plane $P, P' \in S_2(\mathbb{F}_q^m)$ that contain L.
2. Query $B_2[P]$ and $B_2[P']$.
3. Check that $B_2[P]|_L \equiv B_2[P']|_L$.

The second variant is the Plane versus Plane test on planes that intersect on a point:

1. Sample a point $x \in S_0(\mathbb{F}_q^m)$ randomly and take two plane $P, P' \in S_2(\mathbb{F}_q^m)$ that contain x.
2. Query $B_2[P]$ and $B_2[P']$.
3. Check that $B_2[P](x) = B_2[P'](x)$.

It turns out that all of these tests work, roughly equally well, in the sense that a result analogous to Theorem 1.3 holds for each one of the, albeit with somewhat different parameters. In fact, one can reduce the analysis of any one of them to any other; we will see some of these connections here, and some of them in the problem set. For the purposes of our future PCP application, we will have to analyze the plane versus point and plane versus plane tests; in particular, we will prove the following statement:

Theorem 1.5. *Suppose that B_0, B_2 are tables for the plane versus point test with probability at least $\varepsilon \geqslant \frac{d^2}{q^{1/10}}$. Then there exists a polynomial $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ of total degree d, such that*

$$\Pr_{x\in\mathbb{F}_q^m}[B_0(x) = f(x)] \geqslant \varepsilon - \frac{md}{q^{1/10}}.$$

In words, theorem 1.5 says that if the plane versus point passes with significant probability ε, then the points table B_0 agrees with a function f of degree at most d on at least $\varepsilon - o(1)$ of the points. This formulation will be quite important for us for the purpose of this lecture, since it admits a proof by induction on m (which is the route we are going to take). For future use, we need a corollary of it, which we state now and deduce from Theorem 1.5 later in Section 2.6.

Theorem 1.6. *Suppose that B_0, B_2 are tables for the plane versus point test with probability at least $\varepsilon \geqslant \frac{d^2}{q^{1/10}}$. Then for all $\delta > \frac{d^2}{q^{1/10}}$ there is $k \leqslant \frac{2}{\delta^2}$ and a list of polynomials $f_1, \dots, f_k \colon \mathbb{F}_q^m \to \mathbb{F}_q$ of total degree d, such that*

$$\Pr_{x \in P \in S_2(\mathbb{F}_q^m)} [B_0(x) = B_2[P](x) \wedge B_2[P] \neq f_j|_P \, \forall j] \leqslant 3\delta.$$

In words, we can find a short list of low-degree polynomials $f_1, \dots, f_k$ such that except for small probability, if the test passes, then it is because the plane table is consistent with one of the polynomials in the list.

2 Analysis of the Plane versus Plane Test

En route to proving Theorem 1.5, we need to consider the related Plane versus Plane test on planes that intersect on lines as described earlier. This is the content of this section and where most the "action" takes place.

Let $m = 3$, and suppose $B_2 \colon S_2(\mathbb{F}_q^3) \to \{\text{total degree } d \text{ polynomials in 2-variables}\}$ passes the plane versus plane test with probability at least ε. Then, in light of the formulation of Theorem 1.3, one expects to prove that there is a polynomial $f \colon \mathbb{F}_q^3 \to \mathbb{F}_q$ of total degree at most d that agrees with B_2 on $\Omega(\varepsilon)$ of the planes. This is true and will come as a byproduct of the argument we present, however for the purpose of Theorem 1.5, we need the following list-decoding statement.

Theorem 2.1. *Suppose that B_2 is a table that pass the plane versus plane test with probability at least ε, and let $\delta \geqslant \frac{2(d+1)}{q}$. Then there is $k \leqslant \frac{1}{\delta}$ and k polynomials $f_1, \dots, f_k \colon \mathbb{F}_q^3 \to \mathbb{F}_q$ of total degree d, such that*

$$\Pr_{\substack{P,P' \in S_2(\mathbb{F}_q^3) \\ \textit{as in the test}}} \left[B_2[P]_{P \cap P'} \equiv B_2[P']_{P \cap P'} \wedge \forall j (B_2[P] \not\equiv f_j \vee B_2[P'] \not\equiv f_j)\right] \leqslant \delta + 2\sqrt{\frac{d+1}{q}}.$$

In words, Theorem 2.1 provides a short list of polynomials $f_1, \dots, f_k$ such that all of the success of the test can be explained by it. Namely, for all but small fraction of the tests (P, P'), if the test passes on planes P and P', then there is some f_j in the list such that f_j is consistent with both $B_2[P]$ and $B_2[P']$.

The main feature which of the fact that $m = 3$, is that two randomly chosen planes intersect on a line, proved in the following fact. [1]

Fact 2.2. $\Pr_{P,P' \in S_2(\mathbb{F}_q^3)} [\mathsf{dim}(P \cap P') \neq 1] \leqslant \frac{1}{q^2}$.

Proof. The number of planes in $\mathbb{F}_q^3$ is exactly $\frac{q^3(q^3-1)(q^3-q)}{q^2(q^2-1)(q^2-q)}$; here, the numerator counts the number of ways to choose 3 points that span an affine plane, and the denominator counts the number of times a given plane P is counted. Simplifying, this is $N = q\frac{q^3-1}{q-1} = q(q^2+q+1)$. Thus, the number of pairs of planes is N^2.

If two planes do not intersect on a line, then they either are identical – there are N such pairs, or are parallel – there are $N \cdot (q-1)$ such pairs. Indeed, they cannot intersect at a point, since if P, P' intersect on a point x, we can write them as $P = x + L$, $P' = x + L'$ for two subspaces L, L', and as $\mathsf{dim}(L \cap L') = \mathsf{dim}(L) + \mathsf{dim}(L') - \mathsf{dim}(L \oplus L') \geqslant 4 - 3 = 1$ it follows that P and P' intersect on a line.

It follows that

$$\Pr_{P,P' \in S_2(\mathbb{F}_q^3)} \left[\mathsf{dim}(P \cap P') \neq 1\right] = \frac{N + N(q-1)}{N^2} = \frac{1}{N} \leqslant \frac{1}{q^2}. \qquad \square$$

[1] We remark that importantly, the analogous statement for $m = r+1$ is true for r-dimensional affine subspaces of $\mathbb{F}_q^m$. Namely, two random r-dimensional affine subspaces of $\mathbb{F}_q^{r+1}$ intersect on an $r-1$-dimensional affine subspace except with small probability. Thus, the proof we presents works in this more general setting, and we will in fact use it later on in this generality.

2.1 The Assignment Graph

Consider the graph $G = (V, E)$ whose vertex set is $S_2(\mathbb{F}_q^3)$, and two vertices $P, P' \in V$ are adjacent if $B_2[P]_{P\cap P'} \equiv B_2[P']_{P\cap P'}$. Note that $|E| \geqslant \varepsilon\left(1-\frac{1}{q^2}\right)|V|^2$, so thinking of ε as bounded away from 0, the graph G is dense. We will want to study the combinatorial structure of G, and in particular show that it is roughly a union of cliques. We will then consider the cliques that are sizable, which are collections of planes that are all around consistent, and for each one of them we will construct a degree d function f that is consistent it. This will be our list.

2.2 Making G Transitive

The heart of the analysis of the Plane versus Plane test is the fact that the graph G is close to being a *transitive* graph.

Definition 2.3. *A graph $H = (V, E)$ is called transitive if there are no triple of vertices $u, v, w \in V$ such that $(u, v) \in E$, $(v, w) \in E$ but $(u, w) \notin E$.*

We show that G is nearly transitive, in the sense that we can remove a few edges from it and make it transitive. To do so, define the parameter $\beta(H)$ which captures the distance of H from being transitive.

Definition 2.4. *Let $H = (V, E)$ be a graph. For each non-edge $(u, w) \notin E$, define*

$$\beta(u, w) = \Pr_{v\in V}\left[(u, v) \in E, (v, w) \in E\right], \qquad \textit{and subsequently } \beta(H) = \max_{(u,w)\notin E} \beta(u, w).$$

We prove the following two lemmas with respect to the parameter $\beta(H)$. The first lemma asserts that if $\beta(H)$ is small, then one can remove a few edges from H and make it transitive. The second lemma asserts that $\beta(G)$ is small.

Lemma 2.5. *Given a graph $H = (V, E)$, one can remove from it at most $2\sqrt{\beta(H)}\,|V|^2$ edges to get a graph $H' = (V, E')$ which is transitive.*

Proof. The proof is by a iterative process. Denote $\beta = \beta(H)$, and perform the following iterations as long as they change the graph H:

1. If there is v such that $d(v) \leqslant \sqrt{\beta}\,|V|$, remove all edges adjacent to v.
2. Else, take some $v \in V$ and remove all edges between neighbours of v and non-neighbours of v.

It is clear that when the process terminates, the graph is transitive, and the main task is to upper bound the total number of edges removed by the process. Clearly, the first operation can remove at most $\sqrt{\beta}\,|V|^2$ edges in total. For the second operation, consider an invocation of it and denote by $N(v)$ the set of neighbours of v, and by $C(v)$ the connected component of v. The second operation removes edges between $N(v)$ and $C(V) \setminus (N(v) \cup \{v\})$. Prior to the removal, define

$$\begin{aligned} E_{\textsf{non}} &= \{\, (u, w) \mid w \in C(V) \setminus (N(v) \cup \{v\}), u \in N(v)\}\,, \\ E_{\textsf{remove}} &= \{\, (u, w) \in E \mid w \in C(V) \setminus (N(v) \cup \{v\}), u \in N(v)\}\,. \end{aligned}$$

By definition of $\beta(H)$, for each w such that $(v, w) \notin E$, there are at most $\beta\,|V|$ such $u \in N(v)$ that $(u, w) \in E$. Thus,

$$|E_{\textsf{remove}}| \leqslant |C(V) \setminus (N(v) \cup \{v\})| \cdot \beta\,|V|\,.$$

On the other hand, the total number of pairs u, w such that $u \in N(v)$ and $w \notin N(v)$ is at least $d(v) \cdot |C(V) \setminus (N(v) \cup \{v\})|$, and since the first step of the process was not executed, we get

$$|E_{\mathsf{non}}| \geqslant \sqrt{\beta}\,|V|\,|C(V) \setminus (N(v) \cup \{v\})|\,.$$

It follows that $|E_{\mathsf{remove}}| \leqslant \sqrt{\beta}\,|E_{\mathsf{non}}|$. Thus, the total number of edges removed is at most $\sqrt{\beta}$ times the total number of pairs that were in the sets E_{non}, and to finish the argument we argue that each pair of vertices may appear in E_{non} in at most a single iteration.

Indeed, if $(u, w) \in E_{\mathsf{non}}$ when the iteration is invoked on v, then at that point of the process w and u are in the same connected component. However, after this point there are no edges between $C(v) \setminus (N(v) \cup \{v\})$ and $N(v) \cup \{v\}$, which means that v and w are in different connected components, and as v and u are in the same connected component at that time, it follows that u and w are in different connected components. In other words, when the pair (u, w) appears in E_{non} the vertices u and w are in the same connected component, and after that step they are not, hence each pair appears in E_{non} at most once. □

Thus, to prove that G is almost transitive, it suffices to prove an upper bound on $\beta(G)$, and this is the content of the following lemma.

Lemma 2.6. *For our graph $G = (V, E)$ above, $\beta(G) \leqslant \frac{d+1}{q}$.*

Proof. Consider any non-edge (P_1, P_3) in G.

Sample $P_2 \in V$; what is the probability that (P_1, P_2) and (P_2, P_3) are all edges? In that case, we get that either P_2 is disjoint from the line $P_1 \cap P_3$, which happens with probability at most $\frac{1}{q}$, or else $P_1 \cap P_2 \cap P_3$ is a point x. In that case, the point x is distributed uniformly in $P_1 \cap P_3$, and we have that $B_2[P_1]$, $B_2[P_2]$ agree on $P_1 \cap P_2$ and $B_2[P_2]$, $B_2[P_3]$ agree on $P_2 \cap P_3$, so $B_2[P_1](x) = B_2[P_3](x)$. However, since (P_1, P_3) is a non edge, $B_2[P_1]|_{P_1 \cap P_3}$ and $B_2[P_3]|_{P_1 \cap P_3}$ are two distinct degree d univariate polynomials, and hence this is the probability that they agree on a randomly chosen point from $P_1 \cap P_3$, which is at most $\frac{d}{q}$. □

Summarizing, applying Lemmas 2.5, 2.6 on $G = (V, E)$ we may find $G' = (V, E')$ with $E' \subseteq E$ and $|E'| \geqslant |E| - 2\sqrt{(d+1)/q}N^2$ which is transitive. Note that a transitive graph is a union of cliques, so we may write $V = C_1 \cup \ldots \cup C_k$ where each C_i in V is a clique. Thus, the number of edges in G' is $\sum\limits_{i=1}^{k} \binom{|C_i|}{2} = |E'|$, and we show that almost all edges of G' are covered by large cliques. Let $\delta > 0$ to be chosen, and set $I = \{i \mid |C_i| \geqslant \delta N\}$. Then

$$\sum_{i \notin I} \binom{|C_i|}{2} \leqslant \frac{1}{2} \sum_{i \notin I} |C_i|^2 \leqslant \frac{\delta N}{2} \sum_{i \notin I} |C_i| \leqslant \delta N^2.$$

Thus, we find that

$$\sum_{i \in I} \binom{|C_i|}{2} \geqslant |E'| - \delta N^2 \geqslant \varepsilon N^2 - \left(2\sqrt{\frac{d+1}{q}} + \delta\right) N^2.$$

Also, clearly $|I| \leqslant \frac{1}{\delta}$. In the rest of the argument, we will find a list of polynomials $(f_i)_{i \in I}$ which "explain" all of the edges inside the cliques $(C_i)_{i \in I}$, which finishes the proof of Theorem 2.1.

2.3 Interpolating a Low-degree Polynomial in Each C_i

Next, we show that for each C_i, we may find a polynomial $f_i\colon \mathbb{F}_q^3 \to \mathbb{F}_q$ of total degree at most d that agrees with $B_2[P]$ for all $P \in C_i$.

Claim 2.7. *Suppose that $\delta \geqslant \frac{2(d+1)}{q}$, and let $i \in I$. Then there exists a polynomial $f_i\colon \mathbb{F}_q^3 \to \mathbb{F}_q$ of total degree d such that $f_i|_P \equiv B_2[P]$ for all $P \in C_i$.*

Proof. Choose linearly independent vectors $x, y \in \mathbb{F}_q^3$, set $T = \mathsf{Span}(x, y)$ and take $a \in \mathbb{F}_q^3 \setminus T$ uniformly. Note that each $\lambda \in \mathbb{F}_q$, the distribution of $\lambda a + T$ is uniform over S_2. Thus, it follows that

$$\mathop{\mathbb{E}}_{a,T}\left[\sum_{\lambda\in\mathbb{F}_q} 1_{\lambda a+T\in C_i}\right] = q\frac{|C_i|}{|S_2|} \geqslant \delta q \geqslant 2(d+1),$$

hence there are a and T such that $\sum\limits_{\lambda\in\mathbb{F}_q} 1_{\lambda a+T\in C_i} \geqslant 2(d+1)$, and we fix such a and T. Without loss of generality, we assume that $T = \mathsf{Span}(e_1, e_2)$ and $a = e_3$, otherwise we can apply an affine linear transformation. Let $\Lambda = \{\lambda \in \mathbb{F}_q \mid \lambda a + T \in C_i\}$, and take $\Lambda' \subseteq \Lambda'$ of size $2(d+1)$. Note that the probability that a randomly chosen plane is parallel to $a + T$ is $\frac{1}{(q^3-1)(q^3-q)/(q^2-1)(q^2-q)} \leqslant \frac{1}{q^2}$, so it follows that the probability that a randomly chosen plane is in C and not parallel to $a + T$ is at least $\delta - \frac{1}{q^2}$, and using the same technique as above we may find T' that intersects T on a line, such that has at least $d + 1$ of the affine shifts of T' in C. That is, there are $b \in \mathbb{F}_q^3$ and T' such that $b \notin T'$, $\mathsf{dim}(T \cap T') = 1$ and $\Gamma \subseteq \mathbb{F}_q$ of size $d+1$ such that $\{\gamma b+T'\}_{\gamma\in\Gamma} \subseteq C_i$. By applying linear transformations again we may assume $b = e_2$ and $T' = \mathsf{Span}(e_1, e_3)$.

We will show, using interpolation, that there is $f_i\colon \mathbb{F}_q^3 \to \mathbb{F}_q$ of total degree at most $2d$ that agrees with $B_2[\gamma b + T']$ for all $\gamma \in \Gamma$, we will then argue that f_i must agree with $B_2[\lambda a + T]$ for all $\lambda \in \Lambda'$, and then that f_i must agree with $B[P]$ for all $P \in C_i$. Finally, we will show that the degree of f_i must be in fact at most d.

Let $\ell_\gamma(y) = \prod\limits_{\gamma'\in\Gamma\setminus\{\gamma\}} \frac{y-\gamma'}{\gamma-\gamma'}$, and define

$$f_i(x, y, z) = \sum_{\gamma\in\Gamma'} \ell_\lambda(y) B_2[\gamma a + T](x, z).$$

Clearly, f_i has degree at most $|\Gamma| + d - 1 \leqslant 2d$ and $f_i|_{\gamma b+T'} = f(x, \gamma, z) = B_2[\gamma b + T'](x, z)$ for $\gamma \in \Gamma'$. Thus, f_i agrees with all $\{\gamma b + T'\}_{\gamma\in\Gamma}$, and additionally the individual degree of y in f_i is at most d. Fix $\lambda \in \Lambda'$ and consider the plane $\lambda a + T$. Within this plane, consider for each α the line $\ell_{\alpha,\lambda}$ defined by $x = \alpha, z = \lambda$. Note that the line $\ell_{\alpha,\lambda}$ intersects each one of the planes $\{\gamma b + T'\}$ at a point $p = (\alpha, \gamma, \lambda)$ which is inside $(\lambda a + T) \cap (\gamma b + T')$, and hence

$$f_i(p) = B[\gamma b + T'](p) = B[\lambda a + T](p),$$

so we get that $f_i|_{\ell_{\alpha,\lambda}}$ and $B[\lambda a + T]|_{\ell_{\alpha,\lambda}}$ agree on all points $(\alpha, \gamma, \lambda)$ for $\gamma \in \Gamma$, which constitute at $d + 1$ points on $\ell_{\alpha,\lambda}$. Since these are two degree d polynomials, we conclude that they must be the same, hence f_i agrees with $B[\lambda a + T]$ on all lines $\ell_{\alpha,\lambda}$ and therefore $f_i|_{\lambda a+T} \equiv B[\lambda a + T]$ for all $\lambda \in \Lambda'$.

Next, note that any plane P is either parallel to $\lambda a + T$ or intersects it in a line. For $P \in C_i$ that intersect it on a line, we get that $B_2[P]$ and $B_2[\lambda a + T]$ agree on the intersection line for all $\lambda \in \Lambda'$, and as f_i and

$B_2[\lambda a + T]$ agree, we get that $B_2[P]$ and f_i agree on $\cup_{\lambda\in\Lambda'}(\lambda a + T) \cap P$. As this set has size $|\Lambda'|\, q$, we conclude that $f_i|_P$ and $B_2[P]$ agree on at least $2(d+1)q$ points $p \in P$, hence

$$\Pr_{p\in P}\left[f_i|_P(p) = B_2[P](p)\right] \geqslant \frac{2(d+1)q}{q^2} = \frac{2(d+1)}{q},$$

and by the Schwarz-Zippel lemma, as the degrees of $f_i|_P, B_2[P]$ are both are most $2d$, it follows that $f_i|_P \equiv B_2[P]$. Thus, we conclude that $f_i|_P$ and $B_2[P]$ agree on all planes that are not parallel to T.

For planes parallel to T, say $P' = b + T \in C_i$, sampling $P = w + T' \in S_2$ we get that with probability $\geqslant 1 - 1/q$ it intersects P' in a line; conditioned on that and looking at the shifts $\lambda w + T'$ we get as before that in expectation, at least $\left(\delta - \frac{1}{q}\right) q \geqslant 2d+1$ of them are in C_i. Thus, we can find w, T' such that at least $2d+1$ of $\lambda \in \mathbb{F}_q$, we have $\lambda w + T' \in C_i$. Then get that $B_2[P']$ and $B_2[\lambda w + T']$ agree on $P' \cap (\lambda w + T')$ for these λ's, hence we get that $f_i|_{P'}$ and $B_2[P']$ agree on at least $(2d+1)q$ points, and again by Schwarz-Zippel $B_2[P'] \equiv f_i|_{P'}$.

Finally, we argue that f_i has degree at most d. Suppose this is not the case, and consider monomial $x^{m_1}y^{m_2}z^{m_3}$ of maximal degree, and furthermore take $x^{m_1}y^{m_2}z^{m_3}$ of that degree that maximizes m_2. Choosing a random plane amounts to looking at all points (x,y,z) such that $ax + by + cz = e$ for randomly chosen $(a,b,c) \neq 0$ and uniformly chosen $e \in \mathbb{F}_q$. With probability $\geqslant 1 - \frac{1}{q}$ we have $b \neq 0$, so we can choose a value for b so that under the remaining probability over a, c, d, we have that this plane is in C_i with probability at least $\delta - \frac{1}{q}$. Then we can write this as $y = -\frac{a}{b}x - \frac{c}{b}y + \frac{e}{b}$, and the monomial we are inspecting yields

$$(-1)^{m_2}\frac{a^{m_2}}{b^{m_2}}x^{m_1+m_2}z^{m_3} + \text{other monomials.}$$

We look at the function $f_i(x, -\frac{a}{b}x - \frac{c}{b}y + \frac{d}{b}, z)$, and in particular at the coefficient of $x^{m_1+m_2}z^{m_3}$ as a function of a, c, e. Then $x^{m_1}y^{m_2}z^{m_3}$ gives us $(-1)^{m_2}\frac{a^{m_2}}{b^{m_2}}$, and no other monomial can give this power of a (indeed, this could only come from a monomial $x^{m_1'}y^{m_2'}z^{m_3'}$ such that $m_1' + m_2' + m_3' = m_1 + m_2 + m_3$ and $m_1' = m_1$, $m_2' \geqslant m_2$, but we chose the monomial to maximize m_2 so that then $m_2' = m_2$, $m_1' = m_1$ and $m_3' = m_3$), so the coefficient of $x^{m_1+m_2}z^{m_3}$ is a polynomial in a, c, e of degree at most $2d$, hence choosing the values of a, c, e randomly, it is non-zero with probability at least $1 - \frac{2d}{q}$. With probability at least $\delta - \frac{1}{q} \geqslant \frac{2d+1}{q}$ the chosen plane is in C_i, and as the sum of these two probabilities exceeds 1, it means that there is a plane P specified by the equation $ax + by + cz = e$ in C_i such that the monomial $x^{m_1+m_2}z^{m_3}$ appears in $f_i|_P$, but then $B_2[P] = f_i|_P$ has degree larger than d, and contradiction. □

2.4 Proof of Theorem 1.5 for $m = 3$

Having established Theorem 2.1, we can now prove Theorem 1.5 for $m = 3$. The proof uses the connection between the plane versus plane and the plane versus point test we earlier eluded to.

Theorem 2.8. *Suppose that B_0, B_2 are tables that pass the plane versus point test with probability at least $\varepsilon \geqslant \frac{d^2}{q^{1/10}}$. Then there exists a polynomial $f\colon \mathbb{F}_q^3 \to \mathbb{F}_q$ of total degree d, such that*

$$\Pr_x\left[f(x) = B_0(x)\right] \geqslant \varepsilon - \frac{d}{q^{1/10}}.$$

Proof. We first observe a connection between the plane versus plane test and the plane versus point test. Namely, we argue that if B_2 and B_0 pass the plane versus point test with probability at least ε, then B_2

passes the plane versus plane test with probability at least $\varepsilon^2 - \frac{d+1}{q}$. Indeed, sample $x \in \mathbb{F}_q^3$ and two planes P_1, P_2 independently that contain x. Then

$$\mathop{\mathbb{E}}_{x,P_1,P_2}\left[1_{B[P_1](x)=B_0(x)}1_{B[P_2](x)=B_0(x)}\right] = \mathop{\mathbb{E}}_{x}\left[\mathop{\mathbb{E}}_{P\ni x}\left[1_{B[P](x)=B_0(x)}\right]^2\right] \geqslant \mathop{\mathbb{E}}_{x}\left[\mathop{\mathbb{E}}_{P\ni x}\left[1_{B[P](x)=B_0(x)}\right]\right]^2 \geqslant \varepsilon^2.$$

Thus, note that sampling P_1, P_2 that contain a common line means that P_1, P_2 intersect on a line ℓ, and so we get that

$$\mathop{\mathbb{E}}_{\ell,P_1,P_2}\left[\sum_{x\in\ell} 1_{B[P_1](x)=B_0(x)}1_{B[P_2](x)=B_0(x)}\right] \geqslant q\varepsilon^2,$$

meaning that with probability at least $\varepsilon^2 - \frac{d+1}{q}$, $B[P_1]$ and $B[P_2]$ agree on at least $d+1$ of the points in ℓ, in which case they are identical by Schwarz-Zippel. Overall, B_2 passes the plane versus plane test with probability at least $\varepsilon^2 - \frac{d+1}{q}$.

Take $\delta = \frac{d^C}{q^c}$ for $C, c > 0$ to be determined, and take all polynomials $f_1, \ldots, f_k \colon \mathbb{F}_q^3 \to \mathbb{F}_q$ that agree with $B_2[P]$ for at least δ fraction of planes; note that by Claim 2.12 we have $k \leqslant \frac{1}{\delta^2 - d/q} \leqslant \frac{2}{\delta^2}$. We now define

$$W_i = \{\, P \mid f_i|_P \equiv B_2[P]\,\},$$

and argue that the probability the plane versus point test picks a plane outside $W := \bigcup_{i=1}^k W_i$ but passes is very small. To see that, define an assignment B_2' to the planes such that $B_2'[P] = B_2[P]$ if $P \notin W$, and for each $P \in W$ we choose $B_2'[P]$ to be a randomly chosen degree d polynomial over P. By standard probabilistic arguments, after this re-randomization no degree d polynomial agrees with B_2' on more than $\delta + 10\frac{d\log(q^{d^3})}{q} \leqslant 11\delta$ fraction of the planes P, and we fix such randomization. We claim that this randomization implies that the success probability of the test is at most $10\sqrt{\delta}$. Indeed, otherwise by the above connection we would be able to conclude that B_2' passes the plane versus plane test with probability at least 99δ, and by Theorem 2.1 we can find a function degree d function $f \colon \mathbb{F}_q^3 \to \mathbb{F}_q$ that agrees with B_2' for at least 50δ of the planes, which contradicts the property of the randomization. This means that prior to the randomization,

$$\Pr_{x\in P\in \mathrm{S}_2(\mathbb{F}_q^3)}\left[f(x) = B_2[P](x) \wedge \forall j f_j|_P \not\equiv B_2[P]\right] \leqslant \Pr_{x\in P\in \mathrm{S}_2(\mathbb{F}_q^3)}\left[f(x) = B_2'[P](x)\right] \leqslant 10\sqrt{\delta}.$$

The following claim finishes the proof.

Claim 2.9. *For $\eta = \max\left(\left(\frac{100\varepsilon}{q^2\delta^2}\right)^{1/3}, \frac{100\sqrt{\delta}}{\varepsilon}\right)$, there is j such that $\Pr_{x\in\mathbb{F}_q^3}[f_j(x) = B_0(x)] \geqslant \varepsilon - \eta$.*

Proof. Assume otherwise, so that the set $X_j = \{x \mid f_j(x) = B_0(x)\}$ contains at most $\varepsilon - \eta$ elements for each j. By the assumption on the test, $\mathbb{E}_P\left[\sum_{x\in P} 1_{B_0(x)=B_2[P](x)}\right] \geqslant \varepsilon q^2$, so by Claim 2.10 with probability at least η over P, $\sum_{x\in P} 1_{B_0(x)=B_2[P](x)} \geqslant (\varepsilon-\eta)q^2$. However, if we choose P at random, then by Claim 2.11 and the union bound we have $|P \cap X_j| \leqslant (\varepsilon - 50\eta)q^2$ for all j except with probability $\frac{k\varepsilon}{q^2\eta^2} \leqslant \frac{2\varepsilon}{q^2\eta^2\delta^2}$. Thus with probability at least $\eta - \frac{2\varepsilon}{q^2\eta^2\delta^2} \geqslant \frac{\eta}{2}$ both events hold together. In this case we get that $f_j|_P \not\equiv B_2[P]$ for all j, as otherwise we would have that $|P \cap X_j| = \sum_{x\in P} 1_{B_0(x)=B_2[P](x)}$. In conclusion, we get that with probability at least $\frac{\eta}{2}$ we have that $\sum_{x\in P} 1_{B_0(x)=B_2[P](x)} \geqslant (\varepsilon-\eta)q^2$ and $f_j|_P \not\equiv B_2[P]$, and so

$$\Pr_{x\in P\in S_2(\mathbb{F}_q^3)}\left[B_0(x) = B_2[P](x), f_j|_P \not\equiv B_2[P]\ \forall j\right] \geqslant \frac{\eta}{2}\cdot(\varepsilon-\delta) > 10\sqrt{\delta},$$

and contradiction. □

To finish the proof we choose $\delta = \varepsilon^2 \frac{d}{q^{1/5}}$ and $\eta = \frac{d}{q^{1/10}}$. □

2.4.1 Auxiliary Claims

In this section we prove auxiliary claims that were used in the proof of Theorem 2.8. The first one is an averaging argument:

Claim 2.10. $\Pr_P \left[\sum\limits_{x \in P} 1_{B_0(x) = B_2[P](x)} \geqslant (\varepsilon - \delta) q^2\right] \geqslant \delta.$

Proof. The expectation of $\sum\limits_{x \in P} 1_{B_0(x) = B_2[P](x)}$ is at least εq^2, and it is never more than q^2, so letting z denote the probability in question, we get that $zq^2 + (1-z)(\varepsilon - \delta)q^2 \geqslant \varepsilon q^2$, hence $zq^2 \geqslant \delta q^2$, and so $z \geqslant \delta$. □

The second is a sampling lemma, saying that a random plane P samples points well:

Claim 2.11. *Let $X \subseteq \mathbb{F}_q^3$ be a set, then*

$$\Pr_P \left[|P \cap X| \geqslant q^2 \frac{|X|}{|\mathbb{F}_q^3|} + q^2 \delta\right] \leqslant \frac{1}{q^2 \delta^2} \frac{|X|}{|\mathbb{F}_q^3|}$$

Proof. Write a randomly chosen plane as $P = \{x_1, \ldots, x_{q^2}\}$, denote $Z_i = 1_{x_i \in X}$, and note that $|P \cap X| = \sum\limits_{i=1}^{q^2} Z_i$. By linearity of expectation, $\mathbb{E}_P\left[|P \cap X|\right] = q^2 \frac{|X|}{|\mathbb{F}_q^3|}$. Also, we note that for all $i \neq j$, the points x_i, x_j are distributed uniformly over tuples of distinct points in $\mathbb{F}_q^3 \times \mathbb{F}_q^3$. Thus,

$$\mathop{\mathbb{E}}_P\left[|P \cap X|^2\right] = q^2 \frac{|X|}{|\mathbb{F}_q^3|} + \sum_{i \neq j} \mathop{\mathbb{E}}_P\left[1_{x_i, x_j \in X}\right] \leqslant q^2 \frac{|X|}{|\mathbb{F}_q^3|} + q^2(q^2 - 1) \frac{|X|}{|\mathbb{F}_q^3|} \frac{|X| - 1}{|\mathbb{F}_q^3| - 1},$$

which yields $\mathbb{E}_P\left[|P \cap X|^2\right] \leqslant q^2 \frac{|X|}{|\mathbb{F}_q^3|} + \left(q^2 \frac{|X|}{|\mathbb{F}_q^3|}\right)^2$. Thus $\mathsf{var}(|P \cap X|) \leqslant q^2 \frac{|X|}{|\mathbb{F}_q^3|}$, and by Chebyshev's inequality the left hand side of the claim is at most

$$\Pr_P\left[\left||P \cap X| - q^2 \frac{|X|}{|\mathbb{F}_q^3|}\right| \geqslant q^2 \delta\right] \leqslant \frac{q^2 \frac{|X|}{|\mathbb{F}_q^3|}}{q^4 \delta^2} \leqslant \frac{1}{q^2 \delta^2} \frac{|X|}{|\mathbb{F}_q^3|}.$$

□

The third claim is a list decoding size bound, and we prove it in a rather general form. In our case, the code will be the planes code, in which a polynomial f is encoded by its table of restrictions; this code has relative distance at least $\frac{d}{q}$

Claim 2.12. *Suppose C is an error correcting code over $\mathbb{F}_q^n$ with relative distance $1 - s$, and let $\delta > \sqrt{s}$. When for every $w \in \mathbb{F}_q^n$, the number of codewords $c \in C$ such that w and c agree on at least δn coordinates, is at most $\frac{1}{\delta^2 - s}$.*

Proof. Let $c_1, \dots, c_k \in C$ be all codewords that agree with w on at least δ fraction of coordinates. Then we have that $\mathbb{E}_{i\in[k]}\left[\mathbb{E}_{x\in[n]}\left[1_{c_i(x)=w(x)}\right]\right] \geqslant \delta$, so by Cauchy-Schwarz

$$\delta^2 \leqslant \mathop{\mathbb{E}}_{x\in[n]}\left[\mathop{\mathbb{E}}_{i\in[k]}\left[1_{c_i(x)=w(x)}\right]\right]^2 \leqslant \mathop{\mathbb{E}}_{x\in[n]}\left[\mathop{\mathbb{E}}_{i\in[k]}\left[1_{c_i(x)=w(x)}\right]^2\right]$$
$$= \mathop{\mathbb{E}}_{x\in[n]}\left[\frac{1}{k^2}\sum_{i=1}^{k} 1_{c_i(x)=w(x)} + \frac{1}{k^2}\sum_{i\neq j} 1_{c_i(x)=w(x)=c_j(x)}\right].$$

Note that for $i \neq j$, we have that $\mathbb{E}_{x\in[n]}\left[1_{c_i(x)=w(x)=c_j(x)}\right] \leqslant \eta$ since the relative distance of C is at least $1-s$, and c_i, c_j are codewords. Plugging this above we get $\delta^2 \leqslant \frac{1}{k} + s$, hence $k \leqslant \frac{1}{\delta^2 - s}$. □

2.5 The Inductive Argument

Finally, we explain how to get Theorem 1.5 by induction on m. For that, we need the following generalization of Theorem 2.8.

Theorem 2.13. *Suppose that B_0, B_{m-1} are tables that pass the $(m-1)$-dimensional space versus point test with probability at least $\varepsilon \geqslant \frac{d^2}{q^{1/10}}$. Then there exists a polynomial $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ of total degree d, such that*

$$\Pr_{x\in\mathbb{F}_q^m}\left[f(x) = B_0(x)\right] \geqslant \varepsilon - \frac{d^{10}}{q^{1/10}}.$$

Proof. The argument is similar to the argument in Theorem 2.8, and we do not give the details. We remark that following the strategy therein, the bulk of the proof boils down to proving an analog of Theorem 2.1 for the $(m-1)$-dimensional affine subspace vs $(m-1)$-dimensional affine subspace test in $\mathbb{F}_q^m$, and the same analysis that we showed works. Therein, the main fact we used $m = 3$ for is that random two planes in $\mathbb{F}_q^3$ intersect, with high probability, on a line. In the current setting it is true that two randomly chosen $(m-1)$-dimensional affine subspaces in $\mathbb{F}_q^m$ intersect, with high probability, in an affine subspace of dimension $m-2$. □

We can now prove Theorem 1.5 by induction on m, restated below.

Theorem 1.5 (Restated) . *Suppose that B_0, B_2 are tables that pass the plane versus point test with probability at least $\varepsilon \geqslant \frac{d^2}{q^{1/10}}$. Then there exists a polynomial $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ of total degree d, such that*

$$\Pr_{x\in\mathbb{F}_q^m}\left[f(x) = B_0(x)\right] \geqslant \varepsilon - m\frac{d^{10}}{q^{1/10}}.$$

Proof. We prove by induction on m. For $m = 3$, the statement is true from Theorem 2.8. Assume the statement for $m \geqslant 3$, and prove for $m+1$. Then we are working over $\mathbb{F}_q^{m+1}$. For each $W \subseteq \mathbb{F}_q^{m+1}$ of dimension m, we may consider the plane versus point test there; let ε_W be the acceptance probability of it there, and note that $\mathbb{E}_W\left[\varepsilon_W\right] = \varepsilon$. By induction hypothesis, we may find $f_W\colon W \to \mathbb{F}_q$ of degree d such that

$$\Pr_{x\in W}\left[f_W(x) = B_0(x)\right] \geqslant \varepsilon_W - m\frac{d^{10}}{q^{1/10}},$$

so we may define an assignment B_m that assigns to each m dimensional subspace $W \in B_m(\mathbb{F}_q^{m+1})$ the function f_W, and get that B_0, B_m pass the m-dimensional subspace versus point test with probability

$$\mathop{\mathbb{E}}_{W}\left[\Pr_{x\in P\in \mathrm{S}_2(W)}[f_W(x) = B_0(x)]\right] \geqslant \mathop{\mathbb{E}}_{W}\left[\varepsilon_W - m\frac{d^{10}}{q^{1/10}}\right] = \varepsilon - m\frac{d^{10}}{q^{1/10}}.$$

Applying Theorem 2.13 we find a polynomial $f\colon \mathbb{F}_q^{m+1} \to \mathbb{F}_q$ of degree at most d satisfying that

$$\Pr_{x\in W\in \mathrm{S}_m(\mathbb{F}_q^{m+1})}[B_0(x) = f(x)] \geqslant \left(\varepsilon - m\frac{d^{10}}{q^{1/10}}\right) - \frac{d^{10}}{q^{1/10}} = \varepsilon - (m+1)\frac{d^{10}}{q^{1/10}}. \qquad \square$$

2.6 Proof of the List Decoding Statement, Theorem 1.6

Proof of Theorem 1.6. Let $f_1, \ldots, f_k$ be all degree d functions that agree with B_0 on at least δ fraction of points; by Claim 2.12, $k \leqslant \frac{2}{\delta^2}$, and we next perform a randomization argument as before. Let $W_i \subseteq \mathbb{F}_q^m$ be the set of points on which f_i and B_0 agree, and $W = W_1 \cup \ldots \cup W_k$. We claim that if we randomize the values of B_0 on all $x \in W$, then with high probability the acceptance probability of the plane versus point test is at most 10δ. Indeed, with high probability after the randomization no degree d function agrees with B_0 on more than 2δ fraction of points, and hence by Theorem 2.13 the plane versus point test passes with probability at most 2δ. Thus, it follows that before the randomization, except with probability 2δ, whenever the test passes, B_0 agrees with at least one of the functions f_j.

Sample P, and let E be the event that $f_j|_P = B_2[P]$ for some j. If E fails, then $f_j|_P$ and $B_2[P]$ agree on at most $\frac{d}{q}$ of the points of $x \in P$, and so $B_2[P](x) = f_j(x)$ for some j for at most $\frac{dk}{q}$ fraction of points $x \in P$. Thus,

$$\begin{aligned}
&\Pr_{x\in P\in S_2(\mathbb{F}_q^m)}\left[B_0(x) = B_2[P](x) \wedge \bar{E} \wedge \exists j B_0(x) = f_j(x)\right]\\
&\leqslant \Pr_{x\in P\in S_2(\mathbb{F}_q^m)}\left[\exists j, B_0(x) = B_2[P](x) = f_j(x) \mid \bar{E}\right]\\
&\leqslant \frac{dk}{q}.
\end{aligned}$$

Hence,

$$\Pr_{x\in P\in S_2(\mathbb{F}_q^m)}\left[B_0(x) = B_2[P](x) \wedge \bar{E}\right] \leqslant \Pr_{x\in P\in S_2(\mathbb{F}_q^m)}[B_0(x) = B_2[P](x) \wedge \forall j B_0(x) \neq f_j(x)] + \frac{dk}{q},$$

which is at most $2\delta + \frac{dk}{q} \geqslant 2\delta + \frac{2d}{q\delta^2} \leqslant 3\delta$. □