Electronic Colloquium on Computational Complexity, Report No. 126 (2025)

Plane vs. Plane Low Degree Test

Amey Bhangale* Silas Richelson†

Abstract

In this work, we give an optimal analysis of the plane versus plane test of Raz and Safra (STOC'97). More specifically, consider a table $\mathcal{T}$ that assigns every plane P from $\mathbb{F}_q^m$ a bivariate degree d polynomial. The goal is to check if these polynomials are restrictions of a global degree d polynomial $f : \mathbb{F}_q^m \to \mathbb{F}_q$. Raz and Safra introduced the following natural test: sample two random planes P, P' intersecting in a line ℓ and check if $\mathcal{T}(\mathsf{P})|_\ell = \mathcal{T}(\mathsf{P}')|_\ell$, *i.e.*, the two table entries agree on the points on ℓ.

We show that if the test passes with probability at least $\varepsilon = \Omega(d/q)$, then there is a global degree d polynomial f such that for at least $\Omega(\varepsilon)$ fraction of the planes P, $\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}$. This improves on the previous best analysis of the test by Moshkovitz and Raz (STOC'06), where they proved the soundness of the test is at least $(\mathsf{poly}(d)/q)^{1/8}$. With $\Omega(1/q)$ as a natural lower bound on the soundness of this test, our result gets the optimal dependence on the field size, while also working for large degree parameters $d = \Omega(q)$. Our proof combines algebraic aspects from prior work on the lines vs lines test, with combinatorial aspects of recent works on the cubes vs cubes test.

1 Introduction

The main objects of study in this paper are low-degree tests, which check whether a given function $f : \mathbb{F}_q^m \to \mathbb{F}_q$ is a degree d polynomial or is far from the set of degree d polynomials, by querying f at a few random (but correlated) points. In other words, if f is a low-degree function, then the test should accept with probability 1, and if f is *far* from every low-degree function, then the test should reject with high probability. Such local tests were used in constructing Probabilistically Checkable Proofs (PCPs), and the original proofs of the PCP Theorem [ALM+98, AS98, FGL+96] relied on the query complexity and the soundness parameter of such tests. The query complexity is the number of locations queried from the truth table $\mathcal{T}$ of f. The soundness parameter of the test is the minimal quantity $\varepsilon > 0$ such that if the test passes with probability at least ε, then it is necessarily the case that f is *close* to some degree d polynomial.

Low-degree tests were introduced by Rubinfeld and Sudan [RS92], and they gave an $O(d^2)$-query test with soundness $1 - \Omega(1/d)$. Arora, Lund, Motwani, Sudan, and Szegedy [ALM+98], building on the work of Arora and Safra [AS98], improved the soundness parameter of the tests to $1 - \Omega(1)$, and this was a crucial ingredient in getting PCPs with $O(1)$-query complexity.

To get PCPs with smaller query complexity, the truth table representation of the function f is not sufficient – if f has degree d, the test must query $\mathcal{T}$ on at least $d+2$ points. If we want a test that makes

*University of California, Riverside. Email: ameyb@ucr.edu. Supported by the Hellman Fellowship award and NSF CAREER award 2440882.

†University of California, Riverside. Email: silas@cs.ucr.edu. Supported by NSF CAREER award 2441313.

ISSN 1433-8092

fewer queries while keeping the error small, it is useful to move to a more redundant representation of f. The most basic example is when the test has access to the "lines table" of f rather than the truth table. In this setting, the test is given a table $\mathcal{T}$ that maps every line ℓ in $\mathbb{F}_q^m$ to a degree d univariate polynomial $\mathcal{T}(\ell)$, and the question is to test whether these univariate polynomials are the restrictions of a "global" m-variate degree d polynomial $f : \mathbb{F}_q^m \to \mathbb{F}_q$. The following agreement test is one natural test that has access to such a table.

- Select two random lines ℓ and ℓ' intersecting at a point $\mathbf{x} \in \mathbb{F}_q^m$.
- Accept if $\mathcal{T}(\ell)|_{\mathbf{x}} = \mathcal{T}(\ell')|_{\mathbf{x}}$, *i.e.*, if the polynomials $\mathcal{T}(\ell)$ and $\mathcal{T}(\ell')$ agree at $\mathbf{x}$.

Certainly, if the table $\mathcal{T}$ is coming from restrictions of a fixed global degree d function, then the test passes with probability 1. The main question is the soundness of this test, which is stated as follows. For which value of $\varepsilon > 0$ is this following statement true: if the test passes with probability ε, then there is a global degree d function $f : \mathbb{F}^m \to \mathbb{F}$ such that on a considerable (say, $\Omega(\varepsilon)$) fraction of the lines ℓ, $\mathcal{T}(\ell) = f|_\ell$.

This all generalizes naturally to tables and tests of higher dimension. For $t \in \mathbb{N}$ with $t < m$, we say $\mathcal{T}$ is a t-planes table if, for every affine t-plane $\mathsf{H} \subset \mathbb{F}^m$, the entry $\mathcal{T}(\mathsf{H})$ is a t-variate degree d polynomial, which we think of as being defined on H. Given a t-planes table $\mathcal{T}$, a natural test samples two random t-planes $\mathsf{H}, \mathsf{H}' \subset \mathbb{F}^m$ whose intersection has dimension $t-1$ and accepts if $\mathcal{T}(\mathsf{H})|_{\mathsf{H}\cap\mathsf{H}'} = \mathcal{T}(\mathsf{H}')|_{\mathsf{H}\cap\mathsf{H}'}$. The soundness question in this context is for which values of $\varepsilon > 0$ is it true that if the test passes with probability ε, then there is a global degree d polynomial $f : \mathbb{F}^m \to \mathbb{F}$ such that $\mathcal{T}(\mathsf{H}) = f|_{\mathsf{H}}$ for an $\Omega(\varepsilon)$-fraction of the t-planes H.

Early work on low-degree testing [GLR+91, RS92, FS95, RS96, ALM+98, AS98] focused on the *high agreement regime* where the soundness parameter ε is close to 1. As the soundness parameter plays a key "bottleneck" role in efficient constructions of PCPs, it is important to establish soundness guarantees for these tests with ε as close to zero as possible. Two beautiful works of Arora and Sudan [AS98] and Raz and Safra [RS97] kicked off the study of these tests in the *low agreement regime*, where $\varepsilon = o(1)$ as a function of the other parameters − an area of study which remains active today.

1.1 Prior Work on Proving Soundness in the Low Agreement Regime

We now review the known results and key conceptual techniques which have been developed over the years for proving soundness of low-degree tests in the low agreement regime. We note that $\varepsilon = \Omega(1/q)$ is a natural lower bound, since one can construct tables on which the test passes with probability $\Theta(1/q)$, but all degree d-functions agree with at most $o(1/q)$ fraction of the entries (see, *e.g.*, the introduction of [MZ23]).

The Line vs Line Test. Arora and Sudan [AS98] gave the first proof of soundness for the line vs line test with $\varepsilon = (\mathsf{poly}(d)/q)^\tau$, for a small constant $\tau > 0$. Their analysis used an algebraic argument, based on the polynomial method, to prove a soundness theorem for the bivariate case, *i.e.*, when $m = 2$, and then a combinatorial "bootstrapping" argument to extend the bivariate theorem to larger m. The algebraic part of their analysis used the heavy machinery of Hilbert irreducibility in a black-box way. Recently, Harsha, Kumar, Saptharishi and Sudan [HKSS24] improved and simplified the algebraic argument and were able to prove soundness of the line vs line test with $\varepsilon = (d/q)^\tau$ for $\tau = 1/48$. Replacing the $\mathsf{poly}(d)$ in the numerator with simply d is significant as it means the soundness theorem is meaningful even for large degrees $d = \Omega(q)$.

The Plane vs Plane Test. Raz and Safra [RS97] gave the first proof of soundness for the plane vs plane test with $\varepsilon = (m \cdot \mathsf{poly}(d)/q)^{\tau}$, for a small constant $\tau > 0$.[1] Their analysis used a combinatorial argument for the trivariate case, *i.e.* when $m = 3$, and then an inductive bootstrapping argument to extend the trivariate result to larger m. Their combinatorial trivariate theorem is extremely elegant and uses the observation that when $\mathcal{T}(\mathsf{P})$ and $\mathcal{T}(\mathsf{P}')$ do not agree on the line $\mathsf{P} \cap \mathsf{P}'$, they must disagree at almost every point on this line, *i.e.*, test failure implies distance. This observation has been crucial to all subsequent work in the area (except work on the line vs line test where intersections consist of a single point). Motivated by issues related to PCP size, Moshkovitz and Raz [MR08] considered a derandomized planes vs planes test, and gave an improved proof of soundness with $\varepsilon = (\mathsf{poly}(d)/q)^{\tau}$, where $\tau = 1/8$.

The Cube vs Cube Test. Bhangale, Dinur, and Livni Navon [BDN17] gave the first proof of soundness for the cube vs cube test (by *cube*, we mean an affine 3-plane) with $\varepsilon = (\mathsf{poly}(d)/q)^{\tau}$ for $\tau = 1/2$. Their work was the first to deviate from the "prove soundness for low dimensions, then bootstrap" model, instead following the blueprint of [IKW12] for proving soundness theorems for direct product tests. Our argument uses this blueprint as well so we will overview it in Section 1.3 below. Recently, using this same blueprint, Minzer and Zheng [MZ23] proved a striking result: soundness for the cube vs cube test with $\varepsilon = \Omega(\mathsf{poly}(d)/q)$, *i.e.*, optimal dependence on the field size.

1.2 Our Result

In this work we prove soundness of the plane vs plane test with $\varepsilon = \Omega(d/q)$.

Theorem 1. *There is an absolute constant c such that the following holds. If $\mathcal{T}$ is a degree d planes table such that the plane vs plane test for $\mathcal{T}$ accepts with probability $\varepsilon \geq \frac{cd}{q}$, then there exists a global m-variate polynomial $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ of degree at most d such that $\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}$ holds for at least an $\varepsilon/10$-fraction of the planes $\mathsf{P} \subset \mathbb{F}^m$.*

That is, we obtain a soundness parameter for the planes vs planes test which is optimal in terms of the field size, while at the same time providing a non-trivial guarantee for large degrees $d = \Omega(q)$. Thus, we directly improve upon [RS97, MR08] by obtaining a significantly smaller soundness parameter. Moreover, we conceptually improve upon [BDN17, MZ23] by getting the blueprint of [IKW12] to work for planes, rather than requiring cubes. We believe that our techniques will be helpful in the future towards obtaining an optimal soundness proof for the most stringent line versus line tests. This is an interesting and important open problem for further research.

1.3 Our Techniques

In order to describe our technical contributions, we will need to discuss some of the techniques from prior work in more detail.

The Blueprint of [IKW12]. At a high level, the IKW-blueprint as adopted to low-degree testing by [BDN17] works as follows. First, the argument "zooms in" to a set of cubes which contain a point $\mathbf{x} \in \mathbb{F}^m$ *and* whose polynomials agree with each other at $\mathbf{x}$. Specifically, for $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$, let $\mathcal{C}_{(\mathbf{x},\alpha)}$ denote the set of cubes $\mathsf{C} \subset \mathbb{F}^m$ which contain $\mathbf{x}$ and for which $\mathcal{T}(\mathsf{C})|_{\mathbf{x}} = \alpha$. The polynomials

[1] The works [AS98, RS97] came out around the same time and were independent of one another.

of the cubes in $\mathcal{C}_{(\mathbf{x},\alpha)}$ already agree at $\mathbf{x}$ and so they are more likely to agree at other points where their domains intersect. Raz and Safra's observation that "test failure implies distance" is used to show that, for many pairs $(\mathbf{x}, \alpha)$, when two cubes C and C' which intersect in a 2-plane are chosen from $\mathcal{C}_{(\mathbf{x},\alpha)}$, the polynomials $\mathcal{T}(\mathsf{C})$ and $\mathcal{T}(\mathsf{C}')$ will agree on the entire intersection $\mathsf{C} \cap \mathsf{C}'$ *with high probability*. We call the pairs $(\mathbf{x}, \alpha)$ with this property *excellent* (following [IKW12]). The agreement theorem of Rubinfeld and Sudan [RS96] which works in the high agreement regime is invoked to obtain a global degree d polynomial whose restrictions agree with $\mathcal{T}$ on most cubes in $\mathcal{C}_{(\mathbf{x},\alpha)}$ (note we are not done as $\mathcal{C}_{(\mathbf{x},\alpha)}$ contains a tiny fraction of all cubes in $\mathbb{F}^m$). Finally, a consistency argument is used to show that the same global polynomial is common to many zoom-ins, from which the soundness theorem follows. The IKW-blueprint makes extensive use of the expansion properties of various bipartite inclusion graphs (*e.g.*, the inclusion graph between lines and cubes which contain a fixed $\mathbf{x} \in \mathbb{F}^m$). And in fact, the reason that prior works have used the blueprint to prove soundness only for the cube vs cube test (rather than for the plane vs plane test) is that the extra degree of freedom afforded by working with cubes was needed to ensure that all of the inclusion graphs encountered in the argument are good expanders. Indeed, the technical challenges we faced in this work all had to do with making the IKW-blueprint work despite the fact that several of our inclusion graphs are not good expanders.

Technical Contribution $\#1$ – Mixing in Algebraic Methods. The most glaring "expansion failure" we encounter when trying to implement the IKW-blueprint in the planes vs planes setting comes up when attempting to invoke the high agreement theorem of [RS96]. Roughly speaking, this theorem says that for any degree d lines table which passes the line vs line test with probability close to 1, there exists a global degree d polynomial which agrees with almost all of the lines. In order to invoke this theorem, we need to convert our planes table restricted to the zoom-in set into a lines table. Recall that the zoom-in sets of interest are $\mathcal{P}_{(\mathbf{x},\alpha)}$ for an excellent pair $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$. In the cube vs cube setting this is easy: given any line ℓ, simply choose $\mathsf{C} \sim \mathcal{C}_{(\mathbf{x},\alpha)}$ such that C contains ℓ, and set the lines table polynomial to $\mathcal{T}(\mathsf{C})|_\ell$. The expansion of the "lines vs cubes through $\mathbf{x}$" inclusion graph implies that the resulting lines table passes the lines vs lines test with high probability. In the planes vs planes setting, we cannot argue in this way as the "lines vs planes through $\mathbf{x}$" inclusion graph is not an expander. Indeed, for any $\mathbf{x} \in \mathbb{F}^m$ and line $\ell \subset \mathbb{F}^m$ (which does not contain $\mathbf{x}$) there is a unique plane in $\mathbb{F}^m$ which contains both $\mathbf{x}$ and ℓ, and this plane might not be in $\mathcal{P}_{(\mathbf{x},\alpha)}$ at all.

So, in order to invoke the high agreement theorem, we need to work harder to convert our planes table restricted to $\mathcal{P}_{(\mathbf{x},\alpha)}$ into a lines table which passes the lines vs lines test with high probability. We argue as follows given a line $\ell \subset \mathbb{F}^m$. First, we choose a uniform $\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}$ which contains ℓ. The expansion of the "lines vs cubes through $\mathbf{x}$" graph implies that with high probability, a non-negligible fraction of the planes $\mathsf{P} \subset \mathbb{F}^m$ such that $\mathbf{x} \in \mathsf{P} \subset \mathsf{C}$ belong to $\mathcal{P}_{(\mathbf{x},\alpha)}$. Now a polynomial-method-based argument (similar to the ones in [AS98, HKSS24]) is used to obtain a trivariate polynomial, say $g_{(\mathbf{x},\alpha),\mathsf{C}}$, defined on C, whose restriction to almost all of the $\mathsf{P} \in \mathcal{P}_{(\mathbf{x},\alpha)}$ with $\mathsf{P} \subset \mathsf{C}$ equals $\mathcal{T}(\mathsf{P})$. Finally, the lines table polynomial is set to $g_{(\mathbf{x},\alpha),\mathsf{C}}|_\ell$. Relatively standard combinatorial arguments are then used to show that both 1) this lines table passes the lines vs lines test with probability close to 1; and 2) the global polynomial (obtained by invoking the high agreement theorem of [RS96]) agrees with most planes in the zoom-in set.

The interface between the IKW-blueprint and the algebraic argument of [AS98, HKSS24] is very clean and we expand here a bit on it. At a high level, the algebraic argument works in three stages. First, an interpolation lemma is established which says that given any set $S \subset \mathcal{P}_{(\mathbf{x},\alpha)}$ which is not too big, there exists a non-zero low-degree 4-variate polynomial $A_S(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ which vanishes on the planes in S and their bivariate polynomials from $\mathcal{T}$. When we say that A_S vanishes on $\mathsf{P} \in S$, we

mean that the bivariate polynomial which maps $\mathbf{x}' \in \mathsf{P}$ to $A_S\big(\mathbf{x}', \mathcal{T}(\mathsf{P})|_{\mathbf{x}'}\big)$, is identically zero. The interpolation theorem is proved via a dimension counting argument which imposes an upper bound on the size of S. Next, a "vanishing amplification" lemma is proved which says that if the small set S is properly chosen, then the interpolation polynomial $A_S(\mathbf{X}, Z)$ will actually vanish at almost all of the planes in $\mathcal{P}_{(\mathbf{x},\alpha)}$. Finally, it is shown that such an extensive vanishing requirement means that A_S must have a "trivariate root", *i.e.*, it must be divisible by a polynomial of the form $Z - f(\mathbf{X})$ where $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ is the trivariate, degree d polynomial that we are looking for: its restrictions agree with $\mathcal{T}(\mathsf{P})$ at almost every $\mathsf{P} \in \mathcal{P}_{(\mathbf{x},\alpha)}$.

The first and third steps are very similar to the corresponding steps in [HKSS24], but the vanishing amplification step is noteworthy as it works particularly nicely in our setting. Roughly speaking, in order to show that A_S vanishes on almost every $\mathsf{P} \in \mathcal{P}_{(\mathbf{x},\alpha)}$, we consider the lines of intersection $\mathsf{P} \cap \mathsf{P}'$ for the planes $\mathsf{P}' \in S$ (the planes all intersect in lines because we are working inside a fixed cube). Note that for any $\mathbf{x}' \in \mathsf{P} \cap \mathsf{P}'$, we expect to have

$$A\big(\mathbf{x}', \mathcal{T}(\mathsf{P})|_{\mathbf{x}'}\big) = A\big(\mathbf{x}', \mathcal{T}(\mathsf{P}')|_{\mathbf{x}'}\big) = 0,$$

where the first equality holds because we expect $\mathcal{T}(\mathsf{P})$ and $\mathcal{T}(\mathsf{P}')$ to agree on $\mathsf{P} \cap \mathsf{P}'$ (since they are both in $\mathcal{P}_{(\mathbf{x},\alpha)}$ and $(\mathbf{x}, \alpha)$ is excellent), and where the second equality holds because A_S was interpolated to vanish on the planes in S. Thus, most $\mathsf{P} \in \mathcal{P}_{(\mathbf{x},\alpha)}$ will contain roughly $|S|$ lines on which A_S vanishes, from which it follows by Schwartz-Zippel that A_S vanishes on P. This part of our argument appears in Section 4.

An Idea "In the Air". The high agreement theorem of Rubinfeld and Sudan [RS96] requires starting with a lines table which passes the lines vs lines test with probability $1 - \frac{1}{\mathsf{poly}(d)}$, due to its proof which uses a union-bound-type argument. The improved high agreement theorem of Friedl and Sudan [FS95] uses a more sophisticated polynomial-method-type argument and works starting with a lines table which passes the test with probability $1 - \Omega(1)$. It was noted in [HKSS24] that using [FS95] instead of [RS96] for the high agreement component of the IKW-blueprint would have been a better choice as it would have allowed replacing the $\mathsf{poly}(d)$ terms with simply d in the soundness parameters obtained in [BDN17, MZ23]. We implement this change and take the improvement to our soundness parameter, but we do not consider this to be one of our contributions.

The Analysis of [MZ23]. Minzer and Zheng [MZ23] obtained a surprisingly sharp soundness parameter for the cubes vs cubes test by carefully refining the analysis of [BDN17] in several key places. As our work builds on theirs, we identify here what we feel were the main parts of their argument. However, to make it as relevant to our work as possible, we use planes for the context of this discussion, even though [MZ23] worked with cubes. Broadly speaking, the main insight of [MZ23] is that if one considers an experiment which includes drawing two uniform planes, say $\mathsf{P}, \mathsf{P}' \subset \mathbb{F}^m$, which intersect in a line, then the "agreement event" $\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}$ correlates strongly with other, extremely structured behavior. Specifically, [MZ23] consider the distribution which draws uniform planes $\mathsf{P}, \mathsf{P}' \subset \mathbb{F}^m$ which intersect in a line, and then draws $\mathbf{x}, \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}'$, and they prove that conditioned on the agreement event, all of the following also occurs with constant probability: 1) both $(\mathbf{x}, \alpha)$ and $(\mathbf{x}', \alpha')$ are *excellent*, where $(\alpha, \alpha') = \big(\mathcal{T}(\mathsf{P})|_{\mathbf{x}}, \mathcal{T}(\mathsf{P})|_{\mathbf{x}'}\big)$ (meaning that the zoom-in sets $\mathcal{P}_{(\mathbf{x},\alpha)}$ and $\mathcal{P}_{(\mathbf{x}',\alpha')}$ are both amenable to the IKW-blueprint); 2) the global degree d polynomials $f_{(\mathbf{x},\alpha)}$ and $f_{(\mathbf{x}',\alpha')}$ obtained from implementing the IKW-blueprint on $\mathcal{P}_{(\mathbf{x},\alpha)}$ and $\mathcal{P}_{(\mathbf{x}',\alpha')}$, when restricted to P and P' both agree with $\mathcal{T}(\mathsf{P})$ and $\mathcal{T}(\mathsf{P}')$; and 3) $f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')}$. In other words, conditioned on the agreement event occurring, *everything else good that can possibly happen, happens with constant probability*.

This is almost good enough to derive the soundness theorem. Indeed, having $f_{(\mathbf{x},\alpha)}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})$ *and* $f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')}$ for a pair $(\mathbf{x}', \alpha')$ which is completely uncorrelated from $(\mathbf{x}, \alpha)$ would mean that the global polynomial $f = f_{(\mathbf{x}',\alpha')}$ agrees with $\mathcal{T}$ on a non-negligible fraction of the planes in $\mathcal{P}_{\mathbf{x}}$ for a non-negligible fraction of the $\mathbf{x} \in \mathbb{F}^m$, *i.e.*, it agrees with $\mathcal{T}$ on a non-negligible fraction of all planes in $\mathbb{F}^m$. The problem is that it is not immediately clear whether $\mathbf{x}$ and $\mathbf{x}'$ are uncorrelated enough, given that they both are drawn from the intersection $\mathsf{P} \cap \mathsf{P}'$. Minzer and Zheng show that, indeed, $\mathbf{x}$ and $\mathbf{x}'$ drawn in this way are uncorrelated enough, albeit via somewhat *ad hoc* means, using a dyadic partition argument. Working in the stringent planes vs planes setting, we encounter this type of situation several times, and our second technical contribution is the development of a somewhat more principled method for handling it.

Technical Contribution $\#2$ – Analyzing Intersection Distributions. In order to isolate the core problem, consider the following simplified setting. Let $\mathbf{x} \in \mathbb{F}^m$ be fixed and let $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density $\Omega(\varepsilon)$. Consider the distribution on $\mathbb{F}^m$ which draws $\mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x}}$ such that $\mathsf{P} \cap \mathsf{P}'$ is a line, and then draws $\mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}'$ and outputs $\mathbf{x}'$. Is this distribution close to the uniform distribution on $\mathbb{F}^m$? A similar, but incompatible situation was considered in [BDN17] (see Lemma 2.5). In [BDN17], the set $\mathcal{C}'_{\mathbf{x}} \subset \mathcal{C}_{\mathbf{x}}$ has much larger density (since their ε is much larger than ours), and their inclusion graph is a much better expander than ours (since they work with cubes not planes), and so they are able to show that the intersection distribution is $\Omega(q^{-1/2})$-close to uniform.

In our setting, this cannot possibly be the case. Indeed, take $m = 3$, choose lines $\ell_1, \ldots, \ell_d$ through $\mathbf{x}$, and let $\mathcal{P}'_{\mathbf{x}}$ be the set of planes which contain at least one of the ℓ_i. Note $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ has density $\Omega(d/q) = \Omega(\varepsilon)$. However, if two planes $\mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x}}$ are drawn, they will both contain the same ℓ_i with probability roughly $1/d$, in which case the intersection distribution outputs a point from ℓ_i. Thus, the intersection distribution cannot be much closer than $\frac{1}{d}$ to the uniform distribution in statistical distance. Notice however that, at least in this case, when P and P' do not contain the same ℓ_i, then the intersection distribution output is uniform. And indeed, we show in general (*i.e.*, for arbitrary $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ of density $\Omega(\varepsilon)$ and for larger m) that the intersection distribution is within statistical distance $\Omega(d^{-1/2})$ of uniform. See Section 6 for more discussion.

2 Preliminaries

Let $\mathbb{F}$ be a finite field of size $|\mathbb{F}| = q$, let $d \in \mathbb{N}$ with $d < q$ be a degree parameter, and let $m \in \mathbb{N}$ be a dimension parameter.

Low Degree Polynomials. Given an m-variate polynomial $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$, the *degree* of f refers to the maximum total degree of any monomial of f. We will make heavy use of the Schwartz-Zippel Lemma, *i.e.*, $\Pr_{\mathbf{x}\sim\mathbb{F}^m}[f(\mathbf{x}) = 0] \leq d/q$ for all non-zero polynomials $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ of degree d. We will also use "Schwartz-Zippel variants" such as that a non-zero bivariate polynomial of degree d can vanish on at most d lines in the plane. Given an $(m+1)$-variate $A(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$, the $(1, \ldots, 1, d)$-degree of A is the maximum degree of all univariate polynomials of the form $A\big(\vec{\ell}(T), \varphi(T)\big) \in \mathbb{F}[T]$ where $\vec{\ell} : \mathbb{F} \to \mathbb{F}^m$ is a parametrization of a line and where $\varphi(T) \in \mathbb{F}[T]$ is a univariate polynomial of degree at most d. Given an affine 2-plane $\mathsf{P} \subset \mathbb{F}^m$ and a bivariate polynomial Φ defined on P, we write $A(\mathsf{P}, \Phi)$ for the bivariate polynomial which maps $\mathbf{x} \in \mathsf{P}$ to $A\big(\mathbf{x}, \Phi(\mathbf{x})\big)$. Note that if Φ has degree d, then the degree of $A(\mathsf{P}, \Phi)$ is at most the $(1, \ldots, 1, d)$-degree of A.

The Discriminant. If $A(Z) = a_d Z^d + a_{d-1} Z^{d-1} + \cdots + a_1 Z + a_0 \in \mathbb{F}[Z]$ is a degree d univariate polynomial over $\mathbb{F}$, then the *discriminant* of A, denoted $\mathsf{Disc}(A)$, is the quantity

$$\mathsf{Disc}(A) := a_d^{2d-2} \prod_{i<j} (r_i - r_j)^2,$$

where $\{r_1, \ldots, r_d\}$ are the (not necessarily distinct) roots of A in an algebraic closure of $\mathbb{F}$. The two important facts about the discriminant for this work are first that $\mathsf{Disc}(A) = 0$ iff A has a repeated root, and second that $\mathsf{Disc}(A)$ can be represented as a degree $2d-2$ polynomial in the coefficients of A, so in particular $\mathsf{Disc}(A) \in \mathbb{F}$. If $A(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ is an $(m+1)$-variate polynomial, then $\mathsf{Disc}_Z(A)(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ is the m-variate polynomial such that for $\mathbf{x} \in \mathbb{F}^m$, $\mathsf{Disc}_Z(A)(\mathbf{x})$ is the discriminant of the univariate polynomial $A(\mathbf{x}, Z) \in \mathbb{F}[Z]$. The degree of $\mathsf{Disc}_Z(A)$ is at most $2dd_Z$, where d and d_Z are, respectively, the degree and Z-degree of A.

Planes Tables, the Grassmannian Graph and Agreement Tests. Let $\mathcal{P}$ denote the set of affine 2-planes in $\mathbb{F}^m$. We denote by $\mathbb{G}$ the uniform edge distribution of the affine Grassmannian graph whose vertex set is $\mathcal{P}$ and where $(\mathsf{P}, \mathsf{P}')$ is an edge iff P and P' intersect in a line. So $\mathbb{G}$ outputs a uniform pair of planes whose intersection is a line. A degree d, planes table $\mathcal{T}$ assigns to every $\mathsf{P} \in \mathcal{P}$, a degree d bivariate polynomial, denoted $\mathcal{T}(\mathsf{P})$, which we think of as being defined on P. We denote by $\mathsf{TEST}_{2,m}(\mathcal{T})$ the experiment which draws $(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}$, and accepts iff $\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}$, *i.e.*, if the bivariate polynomials $\mathcal{T}(\mathsf{P})$ and $\mathcal{T}(\mathsf{P}')$ agree on the line $\mathsf{P} \cap \mathsf{P}'$.

Expansion Facts. Our proof uses several facts which are derived from the expansion of various bipartite inclusion graphs or Grassmannian graphs. In order to clarify how the non-expansion-related ideas of our argument fit together, we remove essentially all discussion of graph expansion from the main body of the proof in Sections 3, 4 and 5. Throughout the main proof we will state the expansion facts we need, and we will prove them all in Section 6. Many of the expansion facts assert that two distributions are close in statistical distance, and we will use the following concise notation to implicitly state such facts. If $\mathcal{D}$ and $\mathcal{D}'$ are two distributions and EVENT is some event, we will write

$$\Pr_{\mathcal{D}}\big[\mathsf{EVENT}\big] \overset{(\mathsf{ExpFact.X})}{\approx_\delta} \Pr_{\mathcal{D}'}\big[\mathsf{EVENT}\big]$$

to indicate that we are invoking Expansion Fact X which states that $\mathcal{D}$ and $\mathcal{D}'$ are within statistical distance δ of each other. Then in Section 6, the expander fact will be stated and proved.

3 Our Main Result

Theorem 1 (Restated). *Let $\mathbb{F}$ be a finite field of size $|F| = q$, let $c, m, d \in \mathbb{N}$ be integers such that $d < q$, and let $\varepsilon > 0$ be such that $\varepsilon \geq \frac{cd}{q}$. Assume, furthermore, that $c \geq 10^7$, $cd \geq 10^9$, and $\frac{d}{q} \leq 10^{-7}$ all hold. If $\mathcal{T}$ is a degree d planes table such that $\mathsf{TEST}_{2,m}(\mathcal{T})$ passes with probability ε, then there is an m-variate, degree d polynomial $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ such that $\Pr_{\mathsf{P}\sim\mathcal{P}}\big[\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}\big] \geq \varepsilon/10$.*

3.1 Proof Setup and the Key Lemmas

In this section we define excellence and we reduce the proof of Theorem 1 to two lemmas which we will prove in the next sections.

Notation. Let $\gamma > 0$ be an absolute constant ($\gamma = 10^{-12}$ works). For $\mathbf{x} \in \mathbb{F}^m$, denote by $\mathcal{P}_{\mathbf{x}}$ the planes in $\mathcal{P}$ which contain $\mathbf{x}$, *i.e.*, $\mathcal{P}_{\mathbf{x}} = \{\mathsf{P} \in \mathcal{P} : \mathbf{x} \in \mathsf{P}\}$. Let $\mathbb{G}_{\mathbf{x}}$ be the distribution which outputs a uniform pair of planes in $\mathcal{P}_{\mathbf{x}}$ which intersect in a line. For $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$, let $\mathcal{P}_{(\mathbf{x},\alpha)} = \{\mathsf{P} \in \mathcal{P}_{\mathbf{x}} : \mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \alpha\}$ be the set of planes which contain $\mathbf{x}$ and which are such that the polynomial given by $\mathcal{T}$ evaluates at $\mathbf{x}$ to α. We write $\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})$ for the density of $\mathcal{P}_{(\mathbf{x},\alpha)}$ in $\mathcal{P}_{\mathbf{x}}$.

Definition 1 (Excellent). *We say that* $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ *is* excellent *if* $\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \varepsilon/8$ *and*

$$\Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\left[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'} \middle| \mathsf{P}, \mathsf{P}' \in \mathcal{P}_{(\mathbf{x},\alpha)}\right] \geq 1 - \gamma.$$

Lemma 1 (Global Polynomials From Excellent Points). *If* $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ *is excellent, then there is an* m*-variate, degree* d *polynomial* $f_{(\mathbf{x},\alpha)}(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ *such that* $\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}[\mathcal{T}(\mathsf{P}) = f_{(\mathbf{x},\alpha)}|_{\mathsf{P}}] \geq 9/10$.

Lemma 2 (Excellent Points Come in Bunches). *There exists an excellent* $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ *such that* $\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)},\mathbf{x}'\sim\mathsf{P}}[(\mathbf{x}', \alpha') \text{ excellent } \& \ f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')}] \geq 1/6$ *holds, where* $\alpha' = \mathcal{T}(\mathsf{P})|_{\mathbf{x}'}$.

Proof of Theorem 1. We need to show the existence of an m-variate polynomial $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ of degree at most d such that $\Pr_{\mathsf{P}\sim\mathcal{P}}[\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}] \geq \varepsilon/10$. For $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$, define

$$S_f := \left\{\mathbf{x}' \in \mathbb{F}^m : \exists\, \alpha' \in \mathbb{F} \text{ s.t. } (\mathbf{x}', \alpha') \text{ excellent } \& \ f_{(\mathbf{x}',\alpha')} = f\right\}.$$

For any $\mathbf{x}' \in S_f$ and $\alpha' \in \mathbb{F}$ such that $(\mathbf{x}', \alpha')$ is excellent and $f_{(\mathbf{x}',\alpha')} = f$, we have

$$\Pr_{\mathsf{P}\sim\mathcal{P}_{\mathbf{x}'}}[\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}] = \mu_{\mathbf{x}'}(\mathcal{P}_{(\mathbf{x}',\alpha')}) \cdot \Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x}',\alpha')}}[\mathcal{T}(\mathsf{P}) = f_{(\mathbf{x}',\alpha')}|_{\mathsf{P}}] \geq \frac{\varepsilon}{8} \cdot \frac{9}{10} > \frac{\varepsilon}{9},$$

using Lemma 1 and $\mu_{\mathbf{x}'}(\mathcal{P}_{(\mathbf{x}',\alpha')}) \geq \varepsilon/8$ since $(\mathbf{x}', \alpha')$ is excellent. If there exists an f such that $\mu(S_f) \geq \frac{1}{7}$, then we are done since

$$\frac{\varepsilon}{9} \leq \Pr_{\substack{\mathbf{x}'\sim S_f \\ \mathsf{P}\sim\mathcal{P}_{\mathbf{x}'}}}[\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}] \overset{\text{(ExpFact.3)}}{\approx_{\frac{3}{q}}} \Pr_{\mathsf{P}\sim\mathcal{P}}[\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}].$$

We show that $\mu(S_f) \geq \frac{1}{7}$ when $f = f_{(\mathbf{x},\alpha)}$ for the excellent $(\mathbf{x}, \alpha)$ promised by Lemma 2. So let $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ be this point, and let $f_{(\mathbf{x},\alpha)}(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ be the m-variate degree d polynomial promised by Lemma 1, and write f instead of $f_{(\mathbf{x},\alpha)}$ and S instead of $S_{f_{(\mathbf{x},\alpha)}}$. We have

$$\frac{1}{6} \leq \Pr_{\substack{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)} \\ \mathbf{x}'\sim\mathsf{P} \\ \alpha'=\mathcal{T}(\mathsf{P})|_{\mathbf{x}'}}}\left[(\mathbf{x}', \alpha') \text{ exc } \& \ f_{(\mathbf{x}',\alpha')} = f\right] \leq \Pr_{\substack{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)} \\ \mathbf{x}'\sim\mathsf{P}}}[\mathbf{x}' \in S] \overset{\text{(ExpFact.4)}}{\approx_{\frac{1}{100}}} \Pr_{\mathbf{x}'\sim\mathbb{F}^m}[\mathbf{x}' \in S],$$

where the first inequality is Lemma 2. Rearranging gives $\mu(S) \geq \frac{1}{7}$, as desired. □

4 Excellent Pairs to Global Polynomials

In this section we prove Lemma 1.

Lemma 1 (Restated). *Let* $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ *be an excellent pair (see Definition 1). There exists an* m*-variate polynomial* $f_{(\mathbf{x},\alpha)}(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ *of degree at most* d *such that* $\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}[\mathcal{T}(\mathsf{P}) = f_{(\mathbf{x},\alpha)}|_{\mathsf{P}}] \geq \frac{9}{10}$.

Our proof goes in two stages. First, we give a "bootstrapping" argument which reduces Lemma 1 to the trivariate case (*i.e.*, $m = 3$). This part uses an agreement theorem of Friedl and Sudan [FS95] for a lines table which passes the lines vs lines test in $\mathbb{F}^m$ with high probability. We then handle the trivariate case using a polynomial-method argument following the one in [HKSS24].

Notation. In this section we will need to reason about lines and cubes (*i.e.*, affine 3-planes), in addition to planes. We let $\mathcal{L}$ and $\mathcal{C}$ denote the sets of affine lines and cubes in $\mathbb{F}^m$. Just as $\mathcal{P}_{\mathbf{x}}$, for $\mathbf{x} \in \mathbb{F}^m$, is the set of planes which contain $\mathbf{x}$, so we let $\mathcal{L}_{\mathbf{x}}$ and $\mathcal{C}_{\mathbf{x}}$ denote the sets of lines and cubes which contain $\mathbf{x}$. For $\mathsf{C} \in \mathcal{C}$, we let $\mathcal{L}_{\mathsf{C}}$ and $\mathcal{P}_{\mathsf{C}}$ be the sets of lines and planes which are contained in C. For $\mathbf{x}, \mathbf{x}' \in \mathbb{F}^m$, $\alpha \in \mathbb{F}$, $\ell \in \mathcal{L}$, $\mathsf{C} \in \mathcal{C}$, we write $\mathcal{L}_{\mathbf{x},\mathsf{C}}$, $\mathcal{P}_{\mathbf{x},\mathsf{C}}$, $\mathcal{C}_{\mathbf{x},\ell}$, $\mathcal{P}_{(\mathbf{x},\alpha),\mathbf{x}'}$, and $\mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}$ for the intersections $\mathcal{L}_{\mathbf{x}} \cap \mathcal{L}_{\mathsf{C}}$, $\mathcal{P}_{\mathbf{x}} \cap \mathcal{P}_{\mathsf{C}}$, $\mathcal{C}_{\mathbf{x}} \cap \mathcal{C}_{\ell}$, $\mathcal{P}_{(\mathbf{x},\alpha)} \cap \mathcal{P}_{\mathbf{x}'}$ and $\mathcal{P}_{(\mathbf{x},\alpha)} \cap \mathcal{P}_{\mathsf{C}}$. For $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ and $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$, we write $\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})$ for the density of $\mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}$ inside $\mathcal{P}_{\mathbf{x},\mathsf{C}}$. Given a degree d lines table $\mathcal{D}$ which assigns a univariate degree d polynomial to every $\ell \in \mathcal{L}$, we denote by $\mathsf{TEST}_{1,m}(\mathcal{D})$, the experiment which draws $\mathbf{x}' \sim \mathbb{F}^m$, $\ell, \ell' \sim \mathcal{L}_{\mathbf{x}'}$ and outputs 1 iff the polynomials $\mathcal{D}(\ell)$ and $\mathcal{D}(\ell')$ agree at $\mathbf{x}'$, *i.e.*, if $\mathcal{D}(\ell)|_{\mathbf{x}'} = \mathcal{D}(\ell')|_{\mathbf{x}'}$. Let $\gamma' = 3000\gamma$.

Definition 2 (An Excellent Pair for a Cube). *We say that* $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ *is* excellent *for* $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$ *if* $\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \frac{8}{9} \cdot \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})$ *and* $\Pr_{\mathsf{P},\mathsf{P}' \sim \mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}\big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}\big] \geq (1 - \gamma')$.

Expansion Fact 1. *If* $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ *is excellent, then* $\Pr_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[(\mathbf{x}, \alpha) \text{ excellent for } \mathsf{C}\big] \geq \frac{499}{500}$.

We prove the following trivariate version of Lemma 1 in the next section.

Lemma 3 (The Trivariate Version). *If* $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ *is excellent for* $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$*, then there exists a trivariate, degree* d *polynomial* $g_{(\mathbf{x},\alpha),\mathsf{C}}$*, defined on* C*, such that* $\Pr_{\mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}\big[\mathcal{T}(\mathsf{P}) = g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}}\big] \geq \frac{499}{500}$.

Of course when $m = 3$, Lemma 3 directly implies Lemma 1. When $m > 3$, however, we still need to show how to recover a global degree d polynomial which agrees with most planes in $\mathcal{P}_{(\mathbf{x},\alpha)}$. For this, we use the following result of Friedl and Sudan [FS95].

Lemma 4 (Implied by [FS95], Theorem 13). *Let* $\mathcal{D}$ *be a randomized degree* d *lines table, so that for every* $\ell \in \mathcal{L}$*,* $\mathcal{D}(\ell)$ *is a distribution which outputs a univariate polynomial of degree at most* d*. If* $\mathsf{TEST}_{1,m}(\mathcal{D})$ *passes with probability at least* $\frac{49}{50}$*, then there exists an* m*-variate* $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ *of degree at most* d *such that* $\Pr_{\ell \sim \mathcal{L}}\big[\mathcal{D}(\ell) = f|_{\ell}\big] \geq \frac{19}{20}$.

Proof of Lemma 1. Let $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ be excellent. Let $\mathcal{D}$ be the randomized lines table where for $\ell \in \mathcal{L}$, $\mathcal{D}(\ell)$ is the distribution which:

1. draws $\mathsf{C} \sim \mathcal{C}_{\mathbf{x},\ell}$; if $(\mathbf{x}, \alpha)$ is not excellent for C, $\mathcal{D}$ aborts, giving no output;
2. outputs $g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\ell}$, where $g_{(\mathbf{x},\alpha),\mathsf{C}}$ is a trivariate, degree d polynomial $g_{(\mathbf{x},\alpha),\mathsf{C}}$, defined on C, such that $\Pr_{\mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}\big[\mathcal{T}(\mathsf{P}) = g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}}\big] \geq \frac{499}{500}$ (exists when $(\mathbf{x}, \alpha)$ is excellent for C by Lemma 3).

Note that we have

$$\Pr_{\substack{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}} \\ \mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}}\Big[g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})\Big] \geq \Pr_{\substack{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}} \\ \mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}}\Big[(\mathbf{x}, \alpha) \text{ exc for } \mathsf{C} \;\&\; g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})\Big] \geq \frac{249}{250},$$

by Expansion Fact 1 and Lemma 3. We prove Lemma 1 by showing two things. First, we show that $\mathsf{TEST}_{1,m}(\mathcal{D})$ passes with probability at least $\frac{49}{50}$. Thus, by invoking Lemma 4, we obtain an m-variate degree d polynomial $f_{(\mathbf{x},\alpha)}(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ such that $\Pr_{\ell \sim \mathcal{L}}\big[f_{(\mathbf{x},\alpha)}|_{\ell} = \mathcal{D}(\ell)\big] \geq \frac{19}{20}$. Next, we show that this $f_{(\mathbf{x},\alpha)}(\mathbf{X})$ agrees with a $\frac{9}{10}$-fraction of the planes in $\mathcal{P}_{(\mathbf{x},\alpha)}$, and so completes the proof of Lemma 1.

Lower Bounding the Test-Passing Probability. Let $\mathsf{q} := \Pr\big[\mathsf{TEST}_{1,m}(\mathcal{D}) \text{ passes}\big]$ be shorthand for the probability we want to bound. We have

$$\begin{aligned}
\mathsf{q} &= \Pr_{\substack{\mathbf{x}'\sim\mathbb{F}^m\\ \ell,\ell'\sim\mathcal{L}_{\mathbf{x}'}}}\big[\mathcal{D}(\ell)|_{\mathbf{x}'} = \mathcal{D}(\ell')|_{\mathbf{x}'}\big] = \Pr_{\substack{\mathbf{x}'\sim\mathbb{F}^m\\ \mathsf{C},\mathsf{C}'\sim\mathcal{C}_{\mathbf{x},\mathbf{x}'}}}\big[g_{(\mathbf{x},\alpha),\mathsf{C}}(\mathbf{x}') = g_{(\mathbf{x},\alpha),\mathsf{C}'}(\mathbf{x}')\big]\\
&\overset{(\mathsf{ExpFact.7})}{\approx_{\frac{1}{2000}}} \Pr_{\substack{\mathbf{x}'\sim\mathbb{F}^m\\ \mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathbf{x}'}\\ \mathsf{C}\sim\mathcal{C}_{\mathsf{P}},\mathsf{C}'\sim\mathcal{C}_{\mathsf{P}'}}}\big[g_{(\mathbf{x},\alpha),\mathsf{C}}(\mathbf{x}') = g_{(\mathbf{x},\alpha),\mathsf{C}'}(\mathbf{x}')\big]\\
&\geq \Pr_{\substack{\mathbf{x}'\sim\mathbb{F}^m\\ \mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathbf{x}'}\\ \mathsf{C}\sim\mathcal{C}_{\mathsf{P}},\mathsf{C}'\sim\mathcal{C}_{\mathsf{P}'}}}\Big[g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P}) \;\&\; g_{(\mathbf{x},\alpha),\mathsf{C}'}|_{\mathsf{P}'} = \mathcal{T}(\mathsf{P}') \;\&\; \mathcal{T}(\mathsf{P})|_{\mathbf{x}'} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}'}\Big]\\
&\geq \Pr_{\substack{\mathbf{x}'\sim\mathbb{F}^m\\ \mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathbf{x}'}}}\big[\mathcal{T}(\mathsf{P})|_{\mathbf{x}'} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}'}\big] - 2\cdot\Pr_{\substack{\mathbf{x}'\sim\mathbb{F}^m\\ \mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathbf{x}'}\\ \mathsf{C}\sim\mathcal{C}_{\mathsf{P}}}}\big[g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}} \neq \mathcal{T}(\mathsf{P})\big]\\
&\overset{(\mathsf{ExpFact.5})}{\approx_{\frac{1}{2000}}} \Pr_{\substack{\mathbf{x}'\sim\mathbb{F}^m\\ \mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathbf{x}'}}}\big[\mathcal{T}(\mathsf{P})|_{\mathbf{x}'} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}'}\big] - 2\cdot\Pr_{\substack{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}\\ \mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}}\big[g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}} \neq \mathcal{T}(\mathsf{P})\big]\\
&\geq \Pr_{\substack{\mathbf{x}'\sim\mathbb{F}^m\\ \mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathbf{x}'}}}\big[\mathcal{T}(\mathsf{P})|_{\mathbf{x}'} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}'}\big] - \frac{1}{125}\\
&\overset{(\mathsf{ExpFact.9})}{\approx_{\frac{1}{100}}} \Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\Big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}\Big|\mathsf{P},\mathsf{P}'\in\mathcal{P}_{(\mathbf{x},\alpha)}\Big] - \frac{1}{125} \geq 1-\gamma-\frac{1}{125}
\end{aligned}$$

which rearranges to give $\mathsf{q} \geq \frac{49}{50}$. The inequality on the second to last line has used the bound derived above for $\Pr_{\substack{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}\\ \mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}}\big[g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}} \neq \mathcal{T}(\mathsf{P})\big]$. The final inequality holds because $(\mathbf{x},\alpha)$ is excellent.

Agreement with Lines Implies Agreement with Planes. Let $f_{(\mathbf{x},\alpha)}(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ be an m-variate degree d polynomial such that $\Pr_{\ell\sim\mathcal{L}}\big[f_{(\mathbf{x},\alpha)}|_{\ell} = \mathcal{D}(\ell)\big] \geq \frac{19}{20}$. It follows that

$$\begin{aligned}
\frac{19}{20} &\leq \Pr_{\substack{\ell\sim\mathcal{L}\\ \mathsf{C}\sim\mathcal{C}_{\mathbf{x},\ell}}}\big[g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\ell} = f_{(\mathbf{x},\alpha)}|_{\ell}\big] \leq \Pr_{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}}\big[g_{(\mathbf{x},\alpha),\mathsf{C}} = f_{(\mathbf{x},\alpha)}|_{\mathsf{C}}\big] + \frac{d}{q}\\
&\leq \Pr_{\substack{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}\\ \mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}}\Big[g_{(\mathbf{x},\alpha),\mathsf{C}} = f_{(\mathbf{x},\alpha)}|_{\mathsf{C}} \;\&\; g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})\Big] + \Pr_{\substack{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}\\ \mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}}\big[g_{(\mathbf{x},\alpha),\mathsf{C}}|_{\mathsf{P}} \neq \mathcal{T}(\mathsf{P})\big] + \frac{d}{q}\\
&\leq \Pr_{\substack{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}\\ \mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}}\big[f_{(\mathbf{x},\alpha)}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})\big] + \frac{1}{250} + \frac{d}{q} \overset{(\mathsf{ExpFact.6})}{\approx_{\frac{1}{100}}} \Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[f_{(\mathbf{x},\alpha)}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})\big] + \frac{1}{250} + \frac{d}{q},
\end{aligned}$$

which rearranges to give $\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[f_{(\mathbf{x},\alpha)}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})\big] \geq \frac{9}{10}$, proving Lemma 1. □

4.1 Proving the Trivariate Agreement Theorem

Notation. In this section, we fix $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$ such that $(\mathbf{x},\alpha)$ is excellent for C, we identify C with $\mathbb{F}^3$ and drop C everywhere from the syntax. This will greatly simplify our expressions. The assumption that $(\mathbf{x},\alpha)$ is excellent for C implies $\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \frac{\varepsilon}{9}$, and $\Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}\big] \geq 1-\gamma'$, using the fact that any two distinct planes in 3-space who intersect, must intersect in a line.

We prove Lemma 3 using the polynomial-method, following the argument from [HKSS24] (which itself, follows and improves upon [AS03]). At a high level, this proceeds in three stages.

1. Interpolation: First, a set $S \subset \mathcal{P}_{(\mathbf{x},\alpha)}$ is specified, and a non-zero, 4-variate low degree polynomial $A(\mathbf{X},Z) \in \mathbb{F}[\mathbf{X},Z]$ is chosen so that $A\big(\mathsf{P},\mathcal{T}(\mathsf{P})\big) \equiv 0$ for all $\mathsf{P} \in S$. The ability to interpolate

such an A is proved using a dimension counting argument which imposes an upper bound on the size of S.

2. **Amplifying the Vanishing:** Next, the fact that $(\mathbf{x}, \alpha)$ is excellent is used to show that A necessarily vanishes on a much larger set than just S.

3. **Global Agreement via Low-Degree Roots:** Algebraic methods are used to argue that the extensive vanishing implies A has a factor of the form $\big(Z - f_{(\mathbf{x},\alpha)}(\mathbf{X})\big)$, where $f_{(\mathbf{x},\alpha)}(\mathbf{X})$ is the trivariate polynomial we are looking for. In particular, it is low-degree and its restriction to most planes in $\mathcal{P}_{(\mathbf{x},\alpha)}$ agrees with $\mathcal{T}$.

We now state three lemmas, one for each stage mentioned above, and then use them to prove Lemma 3. The interpolation lemma is very similar to lemmas proved in prior work so we include its proof in Appendix A. The proof of the amplification lemma is relatively short, we include it in this section directly after the proof of Lemma 3. The third lemma is proved in the next section.

Additional Parameters. The arguments in this section involve two additional integer parameters $D, r \in \mathbb{N}$, which are both $\mathcal{O}(d)$. We use D as an additional degree parameter, and r is an interpolation set size. The argument in this section will require $\frac{1}{1-\sqrt{\gamma'}} < \frac{r}{D} < \frac{s}{60}$, where $s = D/d$. We will choose $D = 64d$ and $r = 65d$ (so $s = 64$ for our choice of D). We also let $\zeta > 0$ hold the value $\zeta = \frac{1}{4000}$; writing s and ζ instead of 64 and $\frac{1}{4000}$ will clarify how the argument fits together. The arguments in this section will use $\sqrt{\gamma'} \leq \frac{1}{8000}$, $\frac{d}{q} \leq \frac{1}{2000s^2}$, $\frac{9r}{\varepsilon q} \leq \frac{1}{8000}$ (implied by our choice of $c \geq 10^7$), and $\frac{20}{\zeta^2 \eta q} < \frac{1}{2}$ (implied by $cd \geq 10^9$).

Lemma 5 (Interpolation). *For any $S \subset \mathcal{P}_{(\mathbf{x},\alpha)}$ of size $|S| = r$, there exists a 4-variate polynomial $A_S(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ of $(1,1,1,d)$-degree at most D, such that $\mathsf{Disc}_Z(A_S) \not\equiv 0$, and $A_S\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0$ for all $\mathsf{P} \in S$.*

Lemma 6 (Amplifying the Vanishing). *There exists a set $S \subset \mathcal{P}_{(\mathbf{x},\alpha)}$ of size $|S| = r$ such that $\Pr_{\mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha)}}\big[A_S\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0\big] \geq 1 - \zeta$, where $A_S(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ is the polynomial guaranteed by Lemma 5.*

Lemma 7 (Amplified Vanishing to Global List Agreement). *Let the set $S \subset \mathcal{P}_{(\mathbf{x},\alpha)}$ of size $|S| = r$ and the 4-variate $A_S(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ of $(1,1,1,d)$-degree at most D with non-vanishing discriminant be the set and polynomial from Lemma 6. So in particular, $\Pr_{\mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha)}}\big[A(\mathsf{P}, \mathcal{T}(\mathsf{P})) \equiv 0\big] \geq 1 - \zeta$ holds. Then there exists a set $\mathsf{U} \subset \mathbb{F}[\mathbf{X}]$ of trivariate, degree d polynomials such that $|\mathsf{U}| \leq s$ and such that $\Pr_{\mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha)}}\big[\mathcal{T}(\mathsf{P}) \in \{f|_{\mathsf{P}} : f \in \mathsf{U}\}\big] \geq 1 - 2\zeta$.*

Proof of Lemma 3. By Lemmas 5, 6, and 7, there exists a set $\mathsf{U} \subset \mathbb{F}[\mathbf{X}]$ of trivariate, degree d polynomials such that $|\mathsf{U}| \leq s$, and $\Pr_{\mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha)}}\big[\mathcal{T}(\mathsf{P}) \in \{f|_{\mathsf{P}} : f \in \mathsf{U}\}\big] \geq 1 - 2\zeta$. We complete the proof by showing that when $\mathcal{T}(\mathsf{P})$ and $\mathcal{T}(\mathsf{P}')$ agree on $\mathsf{P} \cap \mathsf{P}'$, they are almost surely the restrictions to P and P' of the same $f \in \mathsf{U}$. For this purpose, let

$$\mathsf{q} := \Pr_{\mathsf{P},\mathsf{P}' \sim \mathcal{P}_{(\mathbf{x},\alpha)}}\Big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'} \;\&\; \big(\mathcal{T}(\mathsf{P}), \mathcal{T}(\mathsf{P}')\big) \in \big\{(f|_{\mathsf{P}}, f'|_{\mathsf{P}'}) : f, f' \in \mathsf{U}\big\}\Big]$$

be shorthand. We give lower and upper bounds for q which will combine to prove Lemma 1. We have

$$\mathsf{q} \geq \Pr_{\mathsf{P},\mathsf{P}' \sim \mathcal{P}_{(\mathbf{x},\alpha)}}\Big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}\Big] - 4\zeta \geq 1 - \gamma' - 4\zeta,$$

where the first inequality has used Lemma 7 and second has used the definition of $(\mathbf{x}, \alpha)$ being excellent. On the other hand, we have

$$\begin{aligned}
\mathsf{q} &\leq \Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\Big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'} \;\&\; \exists\, f \in \mathsf{U} \text{ s.t. } \big(\mathcal{T}(\mathsf{P}), \mathcal{T}(\mathsf{P}')\big) = (f|_{\mathsf{P}}, f|_{\mathsf{P}'})\Big] + \\
&\quad + \Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\Big[\exists\, f, f' \in \mathsf{U} \text{ s.t. } f \neq f' \;\&\; f|_{\mathsf{P}\cap\mathsf{P}'} = f'|_{\mathsf{P}\cap\mathsf{P}'}\Big] \\
&\leq \Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\Big[\exists\, f \in \mathsf{U} \text{ s.t. } \big(\mathcal{T}(\mathsf{P}), \mathcal{T}(\mathsf{P}')\big) = (f|_{\mathsf{P}}, f|_{\mathsf{P}'})\Big] + \binom{|\mathsf{U}|}{2} \cdot \left(\frac{d}{q} + \frac{1}{1000s^2}\right) \\
&\leq \max_{f\in\mathsf{U}}\Big\{\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}\big]\Big\} + \frac{s^2}{2}\cdot\frac{d}{q} + \frac{1}{2000},
\end{aligned}$$

which combines with the lower bound to ensure an $f \in \mathsf{U}$ such that

$$\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[\mathcal{T}(\mathsf{P}) = f|_{\mathsf{P}}\big] \geq 1 - \gamma' - 4\zeta - \frac{s^2}{2}\cdot\frac{d}{q} - \frac{1}{2000} \geq \frac{499}{500},$$

using $\gamma = \frac{1}{4000}$ and $\gamma', \frac{s^2}{2}\cdot\frac{d}{q} \leq \frac{1}{4000}$. The inequality on the third line of the upper bound for q holds because for all distinct trivariate $f(\mathbf{X}), f'(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ of degree at most d,

$$\Pr_{\substack{\mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha)}\\ \mathbf{x}'\sim\mathsf{P}\cap\mathsf{P}'}}\big[f(\mathbf{x}') = f'(\mathbf{x}')\big] \overset{(\mathsf{ExpFact.8})}{\approx}_{\frac{1}{1000s^2}} \Pr_{\mathbf{x}'\sim\mathbb{F}^3}\big[f(\mathbf{x}') = f'(\mathbf{x}')\big] \leq \frac{d}{q},$$

by Schwartz-Zippel. □

Proof of Lemma 6. Since $(\mathbf{x}, \alpha)$ excellent implies $\Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}\big] \geq 1 - \gamma'$, by linearity of expectation, $\mathbb{E}_{S,\mathsf{P}}\big[N_S(\mathsf{P})\big] \geq (1-\gamma')r$ holds, where the expectation is over $\mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha)}$ and a random set $S = \{\mathsf{P}_1, \ldots, \mathsf{P}_r\} \subset \mathcal{P}_{(\mathbf{x},\alpha)}$, and where $N_S(\mathsf{P}) := {}^{\#}\big\{\mathsf{P}_i \in S : \mathcal{T}(\mathsf{P})|_{\mathsf{P}_i\cap\mathsf{P}} = \mathcal{T}(\mathsf{P}_i)_{\mathsf{P}_i\cap\mathsf{P}}\big\}$. By averaging,

$$1 - \sqrt{\gamma'} \leq \Pr_{S,\mathsf{P}}\Big[N_S(\mathsf{P}) \geq (1-\sqrt{\gamma'})r\Big] \leq \max_{S}\Big\{\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[N_S(\mathsf{P}) \geq (1-\sqrt{\gamma'})r\big]\Big\}.$$

Let S be such that the probability is maximized, let $A_S(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ be the polynomial guaranteed by Lemma 5, and let $\mathcal{P}'_{(\mathbf{x},\alpha)} \subset \mathcal{P}_{(\mathbf{x},\alpha)}$ be the set of $\mathsf{P} \in \mathcal{P}_{(\mathbf{x},\alpha)}$ such that $N_S(\mathsf{P}) \geq (1-\sqrt{\gamma'})r$ *and* so that the r lines of intersection between P and the $\mathsf{P}_i \in S$ are all unique. Since for any $\ell \in \mathcal{L}_{\mathbf{x}}$, $\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[\ell \subset \mathsf{P}\big] \leq \frac{|\mathcal{P}_\ell|}{|\mathcal{P}_{(\mathbf{x},\alpha)}|} \leq \frac{9|\mathcal{P}_\ell|}{\varepsilon|\mathcal{P}_{\mathbf{x}}|} \leq \frac{9}{\varepsilon q}$ (using $\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \frac{\varepsilon}{9}$ since $(\mathbf{x}, \alpha)$ is excellent), we see that $\Pr_{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)}}\big[\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha)}\big] \geq 1 - \sqrt{\gamma'} - \frac{9r}{\varepsilon q} \geq 1 - \zeta$, since $\zeta = \frac{1}{4000}$ and $\sqrt{\gamma'}, \frac{9r}{\varepsilon q} \leq \frac{1}{8000}$. We complete the proof by showing that for every $\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha)}$, the bivariate polynomial $A_S\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big)$ vanishes.

Fix any $\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha)}$ and consider the r lines $\big\{\mathsf{P} \cap \mathsf{P}_i : \mathsf{P}_i \in S\big\}$. For $N_S(\mathsf{P})$ of these lines, we have $\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}_i} = \mathcal{T}(\mathsf{P}_i)|_{\mathsf{P}\cap\mathsf{P}_i}$, and any time this happens $A_S\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big)$ vanishes on $\mathsf{P} \cap \mathsf{P}_i$ since

$$A_S\big(\mathsf{P} \cap \mathsf{P}_i, \mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}_i}\big) \equiv A_S\big(\mathsf{P} \cap \mathsf{P}_i, \mathcal{T}(\mathsf{P}_i)|_{\mathsf{P}\cap\mathsf{P}_i}\big) \equiv 0,$$

since $A_S\big(\mathsf{P}_i, \mathcal{T}(\mathsf{P}_i)\big) \equiv 0$. Thus, the bivariate polynomial $A_S\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big)$ has degree at most D, but vanishes on $N_S(\mathsf{P}) \geq (1-\sqrt{\gamma'})r > D$ lines in P. By Schwartz-Zippel, $A_S\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0$. □

4.2 Proof of Lemma 7

Finally, in this section we complete the proof of Lemma 1 by proving Lemma 7.

Notation. Let $(\mathbf{x}, \alpha) \in \mathbb{F}^3 \times \mathbb{F}$ be excellent. Let $A(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ be a 4-variate polynomial of $(1,1,1,d)$-degree at most $D = sd$, with $\mathsf{Disc}_Z(A) \not\equiv 0$. Let $\mathsf{ROOTS}(A)$ be the set of trivariate, degree d polynomials $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ such that $\big(Z - f(\mathbf{X})\big)$ is a factor of $A(\mathbf{X}, Z)$. Note $|\mathsf{ROOTS}(A)| \leq s$. Let $\mathcal{P}'_{(\mathbf{x},\alpha)} \subset \mathcal{P}_{(\mathbf{x},\alpha)}$ be a subset of density $\mu_{\mathbf{x}}(\mathcal{P}'_{(\mathbf{x},\alpha)}) = \eta \geq (1-\zeta) \cdot \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})$, where $\zeta = \frac{1}{4000}$, such that $A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0$ for all $\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha)}$. Given $(\mathbf{x}', \alpha') \in \mathbb{F}^3 \times \mathbb{F}$, we write $\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}$ for the intersection $\mathcal{P}'_{(\mathbf{x},\alpha)} \cap \mathcal{P}'_{(\mathbf{x}',\alpha')}$, and we write $\mu_{\mathbf{x},\mathbf{x}'}\big(\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}\big)$ for the density of $\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}$ inside $\mathcal{P}_{\mathbf{x},\mathbf{x}'}$.

Lemma 8 (Sufficient for Lemma 7). *Assuming the above setup,*

$$\Pr_{\mathsf{P} \sim \mathcal{P}'_{(\mathbf{x},\alpha)}}\Big[\exists\, f \in \mathsf{ROOTS}(A) \text{ s.t. } f|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})\Big] \geq 1 - \zeta.$$

Our proof will invoke the following lemma which is very similar to a lemma proved in [HKSS24]. For completeness, we include a proof in Appendix A.

Lemma 9 (Similar to [HKSS24], Lemma 3.1). *Let the pair $(\mathbf{x}', \alpha') \in \mathbb{F}^3 \times \mathbb{F}$ be such that all of the following hold:*

$$1)\ \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}) \geq \tfrac{\zeta\eta}{4s};\quad 2)\ \mathsf{Disc}_Z(A)(\mathbf{x}') \neq 0;\quad 3)\ A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0\ \forall\, \mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}.$$

Then there exists a trivariate polynomial $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ of degree at most d such that $A\big(\mathbf{X}, f(\mathbf{X})\big) \equiv 0$, and so that $f|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})$ for all $\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}$.

We will need an expander fact.

Expansion Fact 2. *Let $\mu, \delta > 0$. Let $\Sigma_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be any set of density $\mu_{\mathbf{x}}(\Sigma_{\mathbf{x}}) = \mu$. Then*

$$\Pr_{\mathbf{x}' \sim \mathbb{F}^3}\Big[\big|\mu_{\mathbf{x},\mathbf{x}'}(\Sigma_{\mathbf{x}}) - \mu\big| > \delta\Big] \leq \frac{\mu}{\delta^2 q}.$$

Proof of Lemma 8. Let $\mathsf{E} \subset \mathcal{P}'_{(\mathbf{x},\alpha)}$ be the set of planes which are "explained by A"; more specifically, $\mathsf{E} := \big\{\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha)} : \mathcal{T}(\mathsf{P}) \in \{f|_{\mathsf{P}} : f \in \mathsf{ROOTS}(A)\}\big\}$. We will show that $\mu_{\mathbf{x}}(\mathsf{E}) \geq (1-\zeta)\cdot\eta$, which proves the lemma as it gives $\Pr_{\mathsf{P} \sim \mathcal{P}'_{(\mathbf{x},\alpha)}}\big[\mathsf{P} \in \mathsf{E}\big] = \frac{\mu_{\mathbf{x}}(\mathsf{E})}{\eta} \geq 1 - \zeta$, as desired. Towards this end, let $\mathsf{G} := \big\{\mathbf{x}' \in \mathbb{F}^3 : \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),\mathbf{x}'}) \geq (1-\zeta/2)\cdot\eta\ \&\ \mathsf{Disc}_Z(A)(\mathbf{x}') \neq 0\big\}$. The crux of the proof is the following claim that we prove below, outside the current proof.

Claim 1. *For any $\mathbf{x}' \in \mathsf{G}$, $\mu_{\mathbf{x},\mathbf{x}'}(\mathsf{E}) \geq \big(1 - \frac{3\zeta}{4}\big)\cdot\eta$.*

We prove the lemma by giving contradictory upper and lower bounds for $\mu(\mathsf{G})$ under the assumption that $\mu_{\mathbf{x}}(\mathsf{E}) < (1-\zeta)\cdot\eta$. Indeed, under this assumption, Claim 1 gives us the following upper bound for $\mu(\mathsf{G})$:

$$\mu(\mathsf{G}) \leq \Pr_{\mathbf{x}' \sim \mathbb{F}^3}\Big[\big|\mu_{\mathbf{x},\mathbf{x}'}(\mathsf{E}) - \mu_{\mathbf{x}}(\mathsf{E})\big| > \zeta\eta/4\Big] \leq \frac{16}{\zeta^2\eta q},$$

using Expander Fact 2. On the other hand, we can lower bound $\mu(\mathsf{G})$ directly since there are two ways that $\mathbf{x}' \in \mathbb{F}^3$ could fail to belong to G. It could either be that 1) $\mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),\mathbf{x}'}) < \big(1 - \frac{\zeta}{2}\big)\cdot\eta$, or 2) $\mathsf{Disc}_Z(A)(\mathbf{x}') = 0$. By Expansion Fact 2, the first type of failure occurs with probability at most

$$\Pr_{\mathbf{x}' \sim \mathbb{F}^3}\Big[\big|\mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),\mathbf{x}'}) - \eta\big| > \zeta\eta/2\Big] \leq \frac{4}{\zeta^2\eta q}.$$

Moreover, since $\mathsf{Disc}_Z(A)$ is a non-zero trivariate polynomial of degree at most $2s^2d$, the second failure occurs with probability at most $\frac{2s^2d}{q}$ over $\mathbf{x}' \sim \mathbb{F}^3$. Thus, $\mu(\mathsf{G}) \geq 1 - \frac{2s^2d}{q} - \frac{4}{\zeta^2\eta q}$. However, this gives: $1 - \frac{2s^2d}{q} - \frac{4}{\zeta^2\eta q} \leq \frac{16}{\zeta^2\eta q}$ which rearranges to $1 \leq \frac{2s^2d}{q} + \frac{20}{\zeta^2\eta q}$, which is a contradiction since $\frac{2s^2d}{q}, \frac{20}{\zeta^2\eta q} < \frac{1}{2}$. Thus, we conclude that $\mu_{\mathbf{x}}(\mathsf{E}) \geq \big(1-\zeta\big)\cdot\eta$, as needed. □

Proof of Claim 1. Let us say that the pair $(\mathbf{x}', \alpha') \in \mathbb{F}^3 \times \mathbb{F}$ is *good* if conditions are such that Lemma 9 can be invoked. So in particular, $(\mathbf{x}', \alpha')$ is good if

$$\mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}) \geq \tfrac{\zeta\eta}{4s}; \quad \mathsf{Disc}_Z(A)(\mathbf{x}') \neq 0; \quad A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0 \; \forall \, \mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}$$

all hold. Note that the third condition automatically holds since $A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0$ for all $\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha)}$. Moreover, since for any $\mathbf{x}' \in \mathbb{F}^3$ and $\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha),\mathbf{x}'}$ $A\big(\mathbf{x}', \mathcal{T}(\mathsf{P})|_{\mathbf{x}'}\big) = 0$ holds, $\mathcal{T}(\mathsf{P})|_{\mathbf{x}'}$ must be a root of the univariate polynomial $A(\mathbf{x}', Z) \in \mathbb{F}[Z]$ which has degree at most s (and hence has at most s roots). Thus, for any $\mathbf{x}' \in \mathbb{F}^3$, there are at most s values of α' such that $\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}$ is not empty, and so

$$\sum_{\alpha' : \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}) < \frac{\zeta\eta}{4s}} \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}) < \frac{\zeta\eta}{4}.$$

Thus, for any $\mathbf{x}' \in \mathsf{G}$,

$$\big(1 - \zeta/2\big) \cdot \eta \leq \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),\mathbf{x}'}) = \sum_{\alpha'} \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}) \leq \sum_{\alpha' : (\mathbf{x}',\alpha') \text{ good}} \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}) + \frac{\zeta\eta}{4},$$

and so $\sum_{\alpha' : (\mathbf{x}',\alpha') \text{ good}} \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}) \geq \big(1 - \frac{3\zeta}{4}\big) \cdot \eta$. By Lemma 9, for any good $(\mathbf{x}', \alpha')$ there exists a trivariate degree d polynomial $f_{(\mathbf{x}',\alpha')}(\mathbf{X})$ such that $A\big(\mathbf{X}, f_{(\mathbf{x}',\alpha')}(\mathbf{X})\big) \equiv 0$ and $f_{(\mathbf{x}',\alpha')}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})$ for all $\mathsf{P} \in \mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')}$. In other words, when $(\mathbf{x}', \alpha')$ is good, $\mathcal{P}'_{(\mathbf{x},\alpha),(\mathbf{x}',\alpha')} \subset \mathsf{E}$ holds, and thus we have $\mu_{\mathbf{x},\mathbf{x}'}(\mathsf{E}) \geq \big(1 - \frac{3\zeta}{4}\big) \cdot \eta$ for every $\mathbf{x}' \in \mathsf{G}$, and we are done. □

5 Excellent Points Come in Bunches

In this section we prove Lemma 2.

Lemma 2 (Restated). *There exists $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ which is excellent, and is moreover such that*

$$\Pr_{\substack{\mathsf{P} \sim \mathcal{P}_{(\mathbf{x},\alpha)} \\ \mathbf{x}' \sim \mathsf{P}}} \Big[(\mathbf{x}', \alpha') \text{ excellent } \& \; f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')} \Big] \geq \frac{1}{6}. \tag{5.1}$$

Proof of Lemma 2. Let Π be the distribution which draws $(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}$, $\mathbf{x}, \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}'$ and outputs $(\mathsf{P}, \mathsf{P}', \mathbf{x}, \mathbf{x}', \alpha, \alpha')$ where $(\alpha, \alpha') = \big(\mathcal{T}(\mathsf{P})|_{\mathbf{x}}, \mathcal{T}(\mathsf{P})|_{\mathbf{x}'}\big)$, and let AGR be shorthand for the "agreement event" $\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}$. We will show

$$\Pr_{\Pi} \Big[\mathsf{AGR} \; \& \; (\mathbf{x}, \alpha), (\mathbf{x}', \alpha') \text{ exc. } \& \; f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')} \Big] \geq \frac{\varepsilon}{4}. \tag{5.2}$$

Deriving the Lemma from (5.2). Let Ψ be the distribution on $\mathbb{F}^m \times \mathbb{F}$ which draws a sample $(\mathsf{P}, \mathsf{P}', \mathbf{x}, \mathbf{x}', \alpha, \alpha') \sim \Pi$ conditioned on $\mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}}$ holding, and outputs $(\mathbf{x}, \alpha)$. Given an excellent pair $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$, let

$$\mathsf{q}_{(\mathbf{x},\alpha)} := \Pr_{\substack{(\mathsf{P},\mathsf{P}') \sim \mathbb{G}_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P}\cap\mathsf{P}'}} \Big[(\mathbf{x}', \alpha') \text{ excellent } \& \; f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')} \Big| \mathsf{P}, \mathsf{P}' \in \mathcal{P}_{(\mathbf{x},\alpha)} \Big],$$

where $\alpha' = \mathcal{T}(\mathsf{P})|_{\mathbf{x}'}$. With these shorthands in place, we start with (5.2) and obtain:

$$\begin{aligned}\frac{\varepsilon}{4} &\le \Pr_{\Pi}\Big[\mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}} \;\&\; (\mathbf{x},\alpha),(\mathbf{x}',\alpha') \text{ exc.} \;\&\; f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')}\Big] \\ &= \Pr_{\Pi}\big[\mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}}\big] \cdot \mathbb{E}_{(\mathbf{x},\alpha)\sim\Psi}\Big[\mathbb{1}_{(\mathbf{x},\alpha)\text{ exc}} \cdot \mathsf{q}_{(\mathbf{x},\alpha)}\Big] \\ &\le \left(\varepsilon + \frac{d}{q}\right) \cdot \mathbb{E}_{(\mathbf{x},\alpha)\sim\Psi}\Big[\mathbb{1}_{(\mathbf{x},\alpha)\text{ exc}} \cdot \mathsf{q}_{(\mathbf{x},\alpha)}\Big] \le \frac{5\varepsilon}{4} \cdot \mathbb{E}_{(\mathbf{x},\alpha)\sim\Psi}\Big[\mathbb{1}_{(\mathbf{x},\alpha)\text{ exc}} \cdot \mathsf{q}_{(\mathbf{x},\alpha)}\Big],\end{aligned}$$

where the first inequality on the final line holds because there are two ways that $\mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}}$ can occur: either $\mathcal{T}(\mathsf{P})$ and $\mathcal{T}(\mathsf{P}')$ agree on the entire line $\mathsf{P} \cap \mathsf{P}'$ (occurs with probability ε), or they disagree on the line but agree at $\mathbf{x}$ (occurs with probability at most $\frac{d}{q}$ by Schwartz-Zippel). It follows that there exists an excellent $(\mathbf{x},\alpha) \in \mathbb{F}^m \times \mathbb{F}$ such that $\mathsf{q}_{(\mathbf{x},\alpha)} \ge \frac{1}{5}$, which implies (5.1):

$$\begin{aligned}\frac{1}{5} \le \mathsf{q}_{(\mathbf{x},\alpha)} &= \Pr_{\substack{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}} \\ \mathbf{x}'\sim\mathsf{P}\cap\mathsf{P}'}}\Big[(\mathbf{x}',\alpha') \text{ excellent} \;\&\; f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')}\Big|\mathsf{P},\mathsf{P}' \in \mathcal{P}_{(\mathbf{x},\alpha)}\Big] \\ &\overset{\text{(ExpFact.10)}}{\approx_{\frac{1}{100}}} \Pr_{\substack{\mathsf{P}\sim\mathcal{P}_{(\mathbf{x},\alpha)} \\ \mathbf{x}'\sim\mathsf{P}}}\Big[(\mathbf{x}',\alpha') \text{ excellent} \;\&\; f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')}\Big].\end{aligned}$$

Establishing (5.2). We establish (5.2) by showing that all of the other "nice behavior" specified in (5.2) correlates heavily with AGR. For this purpose, we set some shorthand for the nice behavior we are interested in. Given a sample from Π, let EXC and POLYS denote the events:

- EXC: $(\mathbf{x},\alpha)$ and $(\mathbf{x}',\alpha')$ are both excellent; and
- POLYS: EXC $\&\; f_{(\mathbf{x},\alpha)}|_{\mathsf{P}} = \mathcal{T}(\mathsf{P}) = f_{(\mathbf{x}',\alpha')}|_{\mathsf{P}}$ and $f_{(\mathbf{x},\alpha)}|_{\mathsf{P}'} = \mathcal{T}(\mathsf{P}') = f_{(\mathbf{x}',\alpha')}|_{\mathsf{P}'}$,

where $f_{(\mathbf{x},\alpha)}$ and $f_{(\mathbf{x}',\alpha')}$ are the polynomials guaranteed by Lemma 1. The following two claims are very similar to claims proved in [MZ23]. We include proofs in Appendix A.

Claim 2. $\Pr_{\Pi}\big[\mathsf{AGR} \;\&\; (\mathbf{x},\alpha) \text{ not excellent}\big] < \frac{\varepsilon}{7}$.

Claim 3. $\Pr_{\Pi}\big[\mathsf{AGR} \;\&\; (\mathbf{x},\alpha) \text{ excellent} \;\&\; \mathcal{T}(\mathsf{P}) \ne f_{(\mathbf{x},\alpha)}|_{\mathsf{P}}\big] < \frac{11\varepsilon}{100}$.

Claims 2 and 3 imply $\Pr_{\Pi}\big[\mathsf{AGR} \;\&\; \mathsf{EXC} \;\&\; \mathsf{POLYS}\big] \ge \Pr_{\Pi}\big[\mathsf{AGR}\big] - 2\cdot\frac{\varepsilon}{7} - 4\cdot\frac{11\varepsilon}{100} \ge \frac{\varepsilon}{4} + \frac{d}{q}$, from which (5.2) follows:

$$\frac{\varepsilon}{4} + \frac{d}{q} \le \Pr_{\Pi}\big[\mathsf{AGR} \;\&\; \mathsf{EXC} \;\&\; f_{(\mathbf{x},\alpha)} = f_{(\mathbf{x}',\alpha')}\big] + \Pr_{\Pi}\big[\mathsf{AGR} \;\&\; \mathsf{EXC} \;\&\; \mathsf{POLYS} \;\&\; f_{(\mathbf{x},\alpha)} \ne f_{(\mathbf{x}',\alpha')}\big]$$

and the second term is at most $\mathbb{E}_{\substack{\mathsf{P}\sim\mathcal{P} \\ \mathbf{x},\mathbf{x}'\sim\mathsf{P}}}\Big[\mathbb{1}_{\mathsf{EXC}} \cdot \mathbb{1}_{f_{(\mathbf{x},\alpha)}\ne f_{(\mathbf{x}',\alpha')}} \cdot \Pr_{\mathsf{P}'\sim\mathcal{P}_{\mathbf{x},\mathbf{x}'}}\big[f_{(\mathbf{x},\alpha)}|_{\mathsf{P}'} = f_{(\mathbf{x}',\alpha')}|_{\mathsf{P}'}\big]\Big] \le \frac{d}{q}$, by Schwartz-Zippel. □

6 Proving the Expansion Facts

Finally, in this section we complete the proof by establishing all of the expansion facts we used.

6.1 Bipartite Inclusion Graph Expansion

Definition 3 (Bipartite Expansion). *Let $\lambda > 0$. We say a biregular bipartite graph is a* λ-expander *if*

$$\lambda \geq \max_{\mathbf{v} \perp \mathbf{1}} \left\{ \frac{\|\mathbf{M}\mathbf{v}\|}{\|\mathbf{v}\|} \right\},$$

where $\mathbf{M}$ is the normalized adjacency matrix of the graph, where $\mathbf{v} \perp \mathbf{1}$ means that $\mathbf{v}$ is perpendicular to the all 1's vector, and where $\|\cdot\|$ is the ℓ_2-norm.

The following claim is proved in [BDN17].

Claim 4 ([BDN17], Lemma 2.3). *Let $\mu, \lambda > 0$. Let $(A \cup B, E)$ be a biregular bipartite graph which is a λ-expander, and let $B' \subset B$ be a subset of density μ. Then*

$$\left\{ (a,b) : \begin{array}{c} b \sim B' \\ a \sim A(b) \end{array} \right\} \approx_{\frac{\lambda}{\sqrt{\mu}}} \left\{ (a,b) : \begin{array}{c} a \sim A \\ b \sim B(a) \cap B' \end{array} \right\},$$

where $A(b)$ and $B(a)$ denote the neighborhoods of b in A and a in B, respectively.

Proving Our First Batch of Expansion Facts. Several of the expansion facts used in the body follow immediately from Claim 4, invoked on various bipartite inclusion graphs whose expansions are well known. We simplify the discussion by ignoring lower order terms in the expansion formulas, so for example if a graph is a λ-expander for $\lambda = q^{-1} \cdot \big(1 \pm o(1)\big)$, we will just say that the graph is a q^{-1}-expander.

Expansion Fact 3. *Let $S \subset \mathbb{F}^m$ be a subset of density at least $\mu(S) \geq \frac{1}{7}$. Then*

$$\left\{ \mathsf{P} : \begin{array}{c} \mathbf{x} \sim S \\ \mathsf{P} \sim \mathcal{P}_{\mathbf{x}} \end{array} \right\} \approx_{\frac{3}{q}} \mathsf{Unif}(\mathcal{P}).$$

Proof. Invoke Claim 4 on the bipartite graph $A = \mathcal{P}$, $B = \mathbb{F}^m$, which is a q^{-1}-expander. □

Expansion Fact 4. *Let $\mathbf{x} \in \mathbb{F}^m$ and let $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density at least $\mu_{\mathbf{x}}(\mathcal{P}'_{\mathbf{x}}) \geq \frac{\varepsilon}{8}$. Then*

$$\left\{ \mathbf{x}' : \begin{array}{c} \mathsf{P} \sim \mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P} \end{array} \right\} \approx_{\frac{1}{100}} \mathsf{Unif}(\mathbb{F}^m).$$

Proof. Invoke Claim 4 on the bipartite graph $A = \mathbb{F}^m$, $B = \mathcal{P}_{\mathbf{x}}$, which is a $q^{-1/2}$-expander. □

Expansion Fact 5. *Let $\mathbf{x} \in \mathbb{F}^m$ and let $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density at least $\mu_{\mathbf{x}}(\mathcal{P}'_{\mathbf{x}}) \geq \frac{\varepsilon}{8}$. Then*

$$\left\{ (\mathsf{P},\mathsf{C}) : \begin{array}{c} \mathbf{x}' \sim \mathbb{F}^m \\ \mathsf{P} \sim \mathcal{P}'_{\mathbf{x},\mathbf{x}'} \\ \mathsf{C} \sim \mathcal{C}_{\mathsf{P}} \end{array} \right\} \approx_{\frac{1}{4000}} \left\{ (\mathsf{P},\mathsf{C}) : \begin{array}{c} \mathsf{C} \sim \mathcal{C}_{\mathbf{x}} \\ \mathsf{P} \sim \mathcal{P}'_{\mathbf{x},\mathsf{C}} \end{array} \right\},$$

where $\mathcal{P}'_{\mathbf{x},\mathbf{x}'}$ and $\mathcal{P}'_{\mathbf{x},\mathsf{C}}$ are shorthands for the intersections $\mathcal{P}'_{\mathbf{x}} \cap \mathcal{P}_{\mathbf{x}'}$ and $\mathcal{P}'_{\mathbf{x}} \cap \mathcal{P}_{\mathsf{C}}$.

Proof. We have

$$\left\{ (\mathsf{P},\mathsf{C}) : \begin{array}{c} \mathbf{x}' \sim \mathbb{F}^m \\ \mathsf{P} \sim \mathcal{P}'_{\mathbf{x},\mathbf{x}'} \\ \mathsf{C} \sim \mathcal{C}_{\mathsf{P}} \end{array} \right\} \approx_{\frac{1}{8000}} \left\{ (\mathsf{P},\mathsf{C}) : \begin{array}{c} \mathsf{P} \sim \mathcal{P}'_{\mathbf{x}} \\ \mathsf{C} \sim \mathcal{C}_{\mathsf{P}} \end{array} \right\} \approx_{\frac{1}{8000}} \left\{ (\mathsf{P},\mathsf{C}) : \begin{array}{c} \mathsf{C} \sim \mathcal{C}_{\mathbf{x}} \\ \mathsf{P} \sim \mathcal{P}'_{\mathbf{x},\mathsf{C}} \end{array} \right\},$$

by invoking Claim 4 on the bipartite graphs $A = \mathbb{F}^m$, $B = \mathcal{P}_{\mathbf{x}}$ and $\hat{A} = \mathcal{C}_{\mathbf{x}}$, $\hat{B} = \mathcal{P}_{\mathbf{x}}$, both of which are $q^{-1/2}$-expanders. □

Expansion Fact 6. *Let $\mathbf{x} \in \mathbb{F}^m$ and let $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density at least $\mu_{\mathbf{x}}(\mathcal{P}'_{\mathbf{x}}) \geq \frac{\varepsilon}{8}$. Then*

$$\left\{ \mathsf{P} : \begin{array}{c} \mathsf{C} \sim \mathcal{C}_{\mathbf{x}} \\ \mathsf{P} \sim \mathcal{P}'_{\mathbf{x},\mathsf{C}} \end{array} \right\} \approx_{\frac{1}{100}} \mathsf{Unif}(\mathcal{P}'_{\mathbf{x}}).$$

Proof. Invoke Claim 4 on the bipartite graph $A = \mathcal{C}_{\mathbf{x}}$, $B = \mathcal{P}_{\mathbf{x}}$, which is a $q^{-1/2}$-expander. □

6.2 Expansion in Grassmannian Graphs

It is well known that, for any $\mathbf{x} \in \mathbb{F}^m$, the Grassmannian graph whose vertices are $\mathcal{P}_{\mathbf{x}}$ and whose edges connect planes which intersect in a line is a q^{-1}-expander. The following useful claim is the *expander mixing lemma*.

Claim 5 (Expander Mixing Lemma for the Grassmannian Graph). *For any $\mathbf{x} \in \mathbb{F}^m$, and subsets $\mathcal{P}^1_{\mathbf{x}}, \mathcal{P}^2_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$, we have*

$$\left| \Pr_{(\mathsf{P},\mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}} \left[\mathsf{P} \in \mathcal{P}^1_{\mathbf{x}} \;\&\; \mathsf{P}' \in \mathcal{P}^2_{\mathbf{x}} \right] - \mu^1 \mu^2 \right| \leq \frac{1}{q} \cdot \sqrt{\mu^1 \mu^2},$$

where $\mu^i := \mu_{\mathbf{x}}(\mathcal{P}^i_{\mathbf{x}})$ for $i = 1, 2$.

The following tail bounds (which includes Expansion Fact 2) follow from Claim 5.

Claim 6 (Expansion Based Tail Bounds). *Let $\mu, \delta > 0$. Let $\mathbf{x} \in \mathbb{F}^m$ and let $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density $\mu_{\mathbf{x}}(\mathcal{P}'_{\mathbf{x}}) = \mu$. Then*

- **Expansion Fact 2:** $\Pr_{\mathbf{x}' \sim \mathbb{F}^m} \left[\left| \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{\mathbf{x}}) - \mu \right| > \delta \right] \leq \frac{\mu}{\delta^2 q}$.
- $\Pr_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}} \left[\left| \mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}'_{\mathbf{x}}) - \mu \right| > \delta \right] \leq \frac{\mu}{\delta^2 q}$.

Proof. Let $\mathsf{q} := \Pr_{\mathbf{x}' \sim \mathbb{F}^m} \left[\left| \mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{\mathbf{x}}) - \mu \right| > \delta \right]$ and $\mathsf{q}' := \Pr_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}} \left[\left| \mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}'_{\mathbf{x}}) - \mu \right| > \delta \right]$ be the probabilities we want to bound. By Markov's inequality, we have

$$\mathsf{q} \leq \Pr_{\mathbf{x}' \sim \mathbb{F}^m} \left[\left(\mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{\mathbf{x}}) - \mu \right)^2 > \delta^2 \right] \leq \delta^{-2} \cdot \left[\mathbb{E}_{\mathbf{x}' \sim \mathbb{F}^m} \left[\mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{\mathbf{x}})^2 \right] - \mu^2 \right],$$

and similarly, $\mathsf{q}' \leq \delta^{-2} \cdot \left[\mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}} [\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}'_{\mathbf{x}})^2] - \mu^2 \right]$. Note, $\mathbb{E}_{\mathbf{x}' \sim \mathbb{F}^m} \left[\mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{\mathbf{x}})^2 \right]$ and $\mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}} \left[\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}'_{\mathbf{x}})^2 \right]$ are both equal to

$$\Pr_{\substack{\mathbf{x}' \sim \mathbb{F}^m \\ \mathsf{P},\mathsf{P}' \sim \mathcal{P}_{\mathbf{x},\mathbf{x}'}}} \left[\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}} \right] = \Pr_{(\mathsf{P},\mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}} \left[\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}} \right] = \Pr_{\substack{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}} \\ \mathsf{P},\mathsf{P}' \sim \mathcal{P}_{\mathbf{x},\mathsf{C}}}} \left[\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}} \right],$$

and so the result follows from Claim 5. □

Expander Fact 7 follows immediately from Claims 6 and 4.

Expansion Fact 7. *If $\mathbf{x} \in \mathbb{F}^m$ and $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ is a subset of density $\mu_{\mathbf{x}}(\mathcal{P}'_{\mathbf{x}}) \geq \frac{\varepsilon}{8}$, then*

$$\left\{ (\mathbf{x}', \mathsf{C}, \mathsf{C}') : \begin{array}{c} \mathbf{x}' \sim \mathbb{F}^m \\ \mathsf{C}, \mathsf{C}' \sim \mathcal{C}_{\mathbf{x},\mathbf{x}'} \end{array} \right\} \approx_{\frac{1}{2000}} \left\{ (\mathbf{x}', \mathsf{C}, \mathsf{C}') : \begin{array}{c} \mathbf{x}' \sim \mathbb{F}^m \\ \mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x},\mathbf{x}'} \\ (\mathsf{C}, \mathsf{C}') \sim \mathcal{C}_{\mathsf{P}} \times \mathcal{C}_{\mathsf{P}'} \end{array} \right\}.$$

Proof. Let Δ be the statistical distance we are trying to bound, and for $\mathbf{x}' \in \mathbb{F}^m$, let $\Delta(\mathbf{x}')$ be the statistical distance between $\mathsf{Unif}(\mathcal{C}_{\mathbf{x},\mathbf{x}'})$ and the distribution which draws $\mathsf{P} \sim \mathcal{P}'_{\mathbf{x},\mathbf{x}'}$, $\mathsf{C} \sim \mathcal{C}_{\mathsf{P}}$, and outputs C. Note that $\Delta \leq \mathbb{E}_{\mathbf{x}' \sim \mathbb{F}^m}\big[2\Delta(\mathbf{x}')\big]$. Also note that if $\mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{\mathbf{x}}) \geq \frac{\varepsilon}{16}$, then $\Delta(\mathbf{x}') \leq \frac{1}{5000}$. This is seen by invoking Claim 4 on the graph $A = \mathcal{C}_{\mathbf{x},\mathbf{x}'}$, $B = \mathcal{P}_{\mathbf{x},\mathbf{x}'}$, which is a $q^{-1/2}$-expander. Therefore, Expansion Fact 2 gives

$$\Delta \leq \Pr_{\mathbf{x}' \sim \mathbb{F}^m}\big[\mu_{\mathbf{x},\mathbf{x}'}(\mathcal{P}'_{\mathbf{x}}) < \varepsilon/16\big] + \frac{1}{2500} \leq \frac{32}{\varepsilon q} + \frac{1}{2500} \leq \frac{1}{2000}.$$

□

6.3 Excellent Pairs are Excellent for Most Cubes

In this section we prove Expander Fact 1 which was a critical element of the "bootstrapping" part of the proof of Lemma 1 from Section 4. Recall that $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ is *excellent* if $\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \frac{\varepsilon}{8}$ and if $\Pr_{(\mathsf{P},\mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}\big[\mathsf{AGR} \big| \mathsf{P}, \mathsf{P}' \in \mathcal{P}_{(\mathbf{x},\alpha)}\big] \geq 1 - \gamma$, where AGR is shrothand for the "agreement event" $\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} = \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}$. Similarly, $(\mathbf{x}, \alpha)$ is *excellent* for $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$ if $\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \frac{8}{9} \cdot \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})$ and if $\Pr_{\mathsf{P},\mathsf{P}' \sim \mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}\big[\mathsf{AGR}\big] \geq 1 - \gamma'$, where $\gamma' = 3000\gamma$.

Expansion Fact 1 (Restated). If $(\mathbf{x}, \alpha) \in \mathbb{F}^m \times \mathbb{F}$ is excellent, $\Pr_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[(\mathbf{x}, \alpha) \text{ excellent for } \mathsf{C}\big] \geq \frac{499}{500}$.

Proof. One way that $(\mathbf{x}, \alpha)$ could fail to be excellent for C is if $\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}) < \frac{8}{9} \cdot \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})$. But if $\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \frac{\varepsilon}{8}$ (which is the case when $(\mathbf{x}, \alpha)$ is excellent), then the second point of Claim 6 says that this occurs with probability at most

$$\Pr_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\left[\left|\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)}) - \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})\right| > \frac{\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})}{9}\right] \leq \frac{328}{\varepsilon q} \leq \frac{1}{1000}$$

The other way that $(\mathbf{x}, \alpha)$ could fail to be excellent for C is if $\Pr_{\mathsf{P},\mathsf{P}' \sim \mathcal{P}_{(\mathbf{x},\alpha),\mathsf{C}}}\big[\mathsf{AGR}\big] < 1 - \gamma'$. Let us say that $\mathsf{C} \in B_{(\mathbf{x},\alpha)}$ if this is the case *and* if $\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \frac{8}{9} \cdot \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})$. So $\mathsf{C} \in B_{(\mathbf{x},\alpha)}$ if $(\mathbf{x}, \alpha)$ fails to be excellent for C only because of the second reason. We will show that when $(\mathbf{x}, \alpha)$ is excellent, $\Pr_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mathsf{C} \in B_{(\mathbf{x},\alpha)}\big] \leq \frac{1}{1000}$, from which the result follows. We set some shorthand. For $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$, let $\mathsf{X}_{(\mathbf{x},\alpha)}(\mathsf{C}) := \Pr_{\mathsf{P},\mathsf{P}' \sim \mathcal{P}_{\mathbf{x},\mathsf{C}}}\big[\mathsf{AGR} \,\&\, \mathsf{P}, \mathsf{P}' \in \mathcal{P}_{(\mathbf{x},\alpha)}\big]$. Note that $\mathsf{C} \in B_{(\mathbf{x},\alpha)}$ exactly when 1) $\mathsf{X}_{(\mathbf{x},\alpha)}(\mathsf{C}) < (1-\gamma') \cdot \mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2$ and; 2) $\mu_{\mathbf{x},\mathsf{C}}(\mathsf{P}_{(\mathbf{x},\alpha)}) \geq \frac{8}{9} \cdot \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})$ both hold. We now give upper and lower bounds on the quantity $\mathbb{E} := \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mathsf{X}_{(\mathbf{x},\alpha)}(\mathsf{C})\big]$, from which the result will follow. When $(\mathbf{x}, \alpha)$ is excellent, we get a lower bound for $\mathbb{E}$ as follows:

$$\begin{aligned}\mathbb{E} &= \Pr_{\substack{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}} \\ \mathsf{P},\mathsf{P}' \sim \mathcal{P}_{\mathbf{x},\mathsf{C}}}}\big[\mathsf{AGR} \,\&\, \mathsf{P}, \mathsf{P}' \in \mathcal{P}_{(\mathbf{x},\alpha)}\big] = \Pr_{(\mathsf{P},\mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}\big[\mathsf{AGR} \,\&\, \mathsf{P}, \mathsf{P}' \in \mathcal{P}_{(\mathbf{x},\alpha)}\big] \\ &\geq (1-\gamma) \cdot \Pr_{(\mathsf{P},\mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}\big[\mathsf{P}, \mathsf{P}' \in \mathcal{P}_{(\mathbf{x},\alpha)}\big] = (1-\gamma) \cdot \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\big].\end{aligned}$$

On the other hand, we can upper bound $\mathbb{E}$ using the definition of $B_{(\mathbf{x},\alpha)}$ as follows:

$$\begin{aligned}\mathbb{E} &= \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mathbb{1}_{\mathsf{C} \in B_{(\mathbf{x},\alpha)}} \cdot \mathsf{X}_{(\mathbf{x},\alpha)}(\mathsf{C})\big] + \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mathbb{1}_{\mathsf{C} \notin B_{(\mathbf{x},\alpha)}} \cdot \mathsf{X}_{(\mathbf{x},\alpha)}(\mathsf{C})\big] \\ &< (1-\gamma') \cdot \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mathbb{1}_{\mathsf{C} \in B_{(\mathbf{x},\alpha)}} \cdot \mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\big] + \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mathbb{1}_{\mathsf{C} \notin B_{(\mathbf{x},\alpha)}} \cdot \mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\big] \\ &= \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\big] - \gamma' \cdot \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mathbb{1}_{\mathsf{C} \in B_{(\mathbf{x},\alpha)}} \cdot \mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\big] \\ &\leq \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\big] - \frac{64\gamma'}{81} \cdot \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2 \cdot \Pr_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mathsf{C} \in B_{(\mathbf{x},\alpha)}\big]\end{aligned}$$

We can now complete the proof:

$$2\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2 \geq \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2 + \frac{1}{q}\cdot\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)}) \geq \Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\big[\mathsf{P},\mathsf{P}'\in\mathcal{P}_{(\mathbf{x},\alpha)}\big]$$
$$= \mathbb{E}_{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}}\big[\mu_{\mathbf{x},\mathsf{C}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\big] > \frac{64\cdot 3000}{81}\cdot\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\cdot\Pr_{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}}\big[\mathsf{C}\in B_{(\mathbf{x},\alpha)}\big],$$

which rearranges to give $\Pr_{\mathsf{C}\sim\mathcal{C}_{\mathbf{x}}}\big[\mathsf{C}\in B_{(\mathbf{x},\alpha)}\big] < \frac{1}{1000}$, as desired. The second inequality on the first line has used Claim 5, and the inequality on the second line comes from putting the upper and lower bounds for $\mathbb{E}$ together and rearranging (and using $\gamma' = 3000\gamma$). □

6.4 Intersection Distributions

In this section we prove the remaining three expansion facts, which all have to do with understanding the distribution of the line of intersection between two planes which are drawn from a subset. We begin by proving Expansion Fact 8 which addresses the trivariate case (*i.e.*, when $m = 3$).

Expansion Fact 8. *Let $\mu > 0$, $\mathbf{x}\in\mathbb{F}^3$ and let $\mathcal{P}'_{\mathbf{x}}\subset\mathcal{P}_{\mathbf{x}}$ be a subset of density μ. Then*

$$\left\{\mathbf{x}' : \begin{array}{c}\mathsf{P},\mathsf{P}'\sim\mathcal{P}'_{\mathbf{x}}\\ \mathbf{x}'\sim\mathsf{P}\cap\mathsf{P}'\end{array}\right\} \approx_{\frac{3}{\sqrt{\mu q}}} \mathsf{Unif}(\mathbb{F}^3).$$

First, however, we work out a useful calculation.

Claim 7. *Define $\mathsf{q}:\mathbb{F}^3\to\mathbb{R}$ via $\mathsf{q}(\mathbf{x}') := \Pr_{\mathsf{P}\sim\mathcal{P}'_{\mathbf{x}}}\big[\mathbf{x}'\in\mathsf{P}\big]$. Then we have*

$$\sum_{\mathbf{x}'\in\mathbb{F}^3}\mathsf{q}(\mathbf{x}') = q^2;\ \textit{and}\ \sum_{\mathbf{x}'\in\mathbb{F}^3}\mathsf{q}(\mathbf{x}')^2 \leq \mu^{-1}+q$$

Proof. Since $\mathsf{q}(\mathbf{x}') = \mathbb{E}_{\mathsf{P}\sim\mathcal{P}'_{\mathbf{x}}}\big[\mathbb{1}_{\mathbf{x}'\in\mathsf{P}}\big]$, we have $\sum_{\mathbf{x}'\in\mathbb{F}^3}\mathsf{q}(\mathbf{x}') = \mathbb{E}_{\mathsf{P}\sim\mathcal{P}'_{\mathbf{x}}}\big[|\mathsf{P}|\big] = q^2$ by linearity of expectation. For the other sum, we compute

$$\sum_{\mathbf{x}'\in\mathbb{F}^3}\mathsf{q}(\mathbf{x}')^2 = \mathbb{E}_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}'_{\mathbf{x}}}\big[|\mathsf{P}\cap\mathsf{P}'|\big] \leq \frac{q^2}{|\mathcal{P}'_{\mathbf{x}}|} + q \leq \mu^{-1}+q.$$

The first inequality holds because $\mathsf{P}=\mathsf{P}'$ occurs with probability $\frac{1}{|\mathcal{P}'_{\mathbf{x}}|}$ and results in $|\mathsf{P}\cap\mathsf{P}'| = q^2$, while whenever $\mathsf{P}\neq\mathsf{P}'$ then $|\mathsf{P}\cap\mathsf{P}'| = q$ (since we are in 3-space). The final inequality holds because $|\mathcal{P}'_{\mathbf{x}}| = \mu\cdot|\mathcal{P}_{\mathbf{x}}| \geq \mu\cdot q^2$, as there are q^2+q+1 planes through any point in 3-space. □

Proof of Expansion Fact 8. Let $\mathcal{D}'$ be the distribution which draws $\mathsf{P}\sim\mathcal{P}_{\mathbf{x}}$ and $\mathbf{x}'\sim\mathsf{P}$ and outputs $\mathbf{x}'$. By Claim 4, we have $\Delta\big(\mathcal{D}',\mathsf{Unif}(\mathbb{F}^3)\big)\leq\frac{1}{\sqrt{\mu q}}$, since the bipartite graph with $A=\mathbb{F}^3$ and $B=\mathcal{P}_{\mathbf{x}}$ is a $q^{-1/2}$-expander. Thus, it suffices to show that $\Delta(\mathcal{D},\mathcal{D}')\leq\frac{2}{\sqrt{\mu q}}$, where $\mathcal{D}$ is the distribution from Expansion Fact 8. Note, for all $\mathbf{x}'\in\mathbb{F}^3$,

$$\Pr\big[\mathcal{D}=\mathbf{x}'\big] = \Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}'_{\mathbf{x}}}\big[\mathbf{x}'\in\mathsf{P}\cap\mathsf{P}'\ \&\ \mathsf{P}\neq\mathsf{P}'\big]\cdot q^{-1} + \Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}'_{\mathbf{x}}}\big[\mathbf{x}'\in\mathsf{P}\cap\mathsf{P}'\ \&\ \mathsf{P}=\mathsf{P}'\big]\cdot q^{-2}$$
$$= \Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}'_{\mathbf{x}}}\big[\mathbf{x}'\in\mathsf{P}\cap\mathsf{P}'\big]\cdot q^{-1} - \Pr_{\mathsf{P},\mathsf{P}'\sim\mathcal{P}'_{\mathbf{x}}}\big[\mathbf{x}'\in\mathsf{P}\cap\mathsf{P}'\ \&\ \mathsf{P}=\mathsf{P}'\big]\cdot\big(q^{-1}-q^{-2}\big)$$
$$= \mathsf{q}(\mathbf{x}')^2\cdot\frac{1}{q} - \frac{1}{|\mathcal{P}'_{\mathbf{x}}|}\cdot\mathsf{q}(\mathbf{x}')\cdot\frac{q-1}{q^2},$$

while $\Pr\left[\mathcal{D}' = \mathbf{x}'\right] = \mathsf{q}(\mathbf{x}') \cdot \frac{1}{q^2}$. Therefore,

$$\Delta(\mathcal{D}, \mathcal{D}') \leq \frac{1}{q} \cdot \sum_{\mathbf{x}' \in \mathbb{F}^3} \mathsf{q}(\mathbf{x}') \cdot \left|\mathsf{q}(\mathbf{x}') - q^{-1}\right| + \frac{1}{q|\mathcal{P}'_{\mathbf{x}}|} \cdot \sum_{\mathbf{x}' \in \mathbb{F}^3} \mathsf{q}(\mathbf{x}').$$

The second term is at most $\frac{1}{\mu q}$ using Claim 7 and $|\mathcal{P}'_{\mathbf{x}}| \geq \mu q^2$. By Cauchy-Schwarz, the first term is at most

$$\sqrt{\frac{1}{q} \cdot \sum_{\mathbf{x}' \in \mathbb{F}^3} \mathsf{q}(\mathbf{x}')^2} \cdot \sqrt{\frac{1}{q} \cdot \sum_{\mathbf{x}' \in \mathbb{F}^3} \left(\mathsf{q}(\mathbf{x}') - q^{-1}\right)^2} \leq \sqrt{\frac{1}{q\mu} + 1} \cdot \sqrt{\frac{1}{\mu q}} \leq \frac{\sqrt{2}}{\sqrt{\mu q}},$$

using Claim 7. The result follows. □

Our final two expansion facts will follow relatively easily from an m-variate version of Expansion Fact 8 which we now state.

Claim 8. *Let $\mu > 0$, $\mathbf{x} \in \mathbb{F}^m$ and let $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density μ. Then*

$$\left\{\mathbf{x}' : \begin{array}{c} (\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}|\mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}' \end{array}\right\} \approx_{\frac{8}{\sqrt{\mu q}}} \mathsf{Unif}(\mathbb{F}^m),$$

where $\mathbb{G}_{\mathbf{x}}|\mathcal{P}'_{\mathbf{x}}$ is the distribution which draws $(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}$ conditioned on $\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}}$.

Expansion Fact 9. *Let $\mu > 0$, $\mathbf{x} \in \mathbb{F}^m$ and let $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density μ. Then*

$$\left\{(\mathsf{P}, \mathsf{P}') : \begin{array}{c} \mathbf{x}' \sim \mathbb{F}^m \\ \mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x},\mathbf{x}'} \end{array}\right\} \approx_{\frac{8}{\sqrt{\mu q}}} \mathbb{G}_{\mathbf{x}}|\mathcal{P}'_{\mathbf{x}}.$$

Proof. Consider the following procedures to generate a pair $(\mathsf{P}, \mathsf{P}')$:

$$\left\{\begin{array}{c} \mathbf{x}' \sim \mathbb{F}^m \\ \mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x},\mathbf{x}'} \end{array}\right\} \approx_{\frac{8}{\sqrt{\mu q}}} \left\{\begin{array}{c} (\hat{\mathsf{P}}, \hat{\mathsf{P}}') \sim \mathbb{G}_{\mathbf{x}}|\mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \hat{\mathsf{P}} \cap \hat{\mathsf{P}}' \\ \mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x},\mathbf{x}'} \end{array}\right\} \equiv \left\{\begin{array}{c} (\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}|\mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}' \\ \hat{\mathsf{P}}, \hat{\mathsf{P}}' \sim \mathcal{P}'_{\mathbf{x},\mathbf{x}'} \end{array}\right\}.$$

The first two procedures are within statistical distance $\frac{8}{\sqrt{\mu q}}$ of each other by Claim 8, the next two are identical since the marginal distributions on $(\mathsf{P}, \mathsf{P}')$ and $(\hat{\mathsf{P}}, \hat{\mathsf{P}}')$ are the same. But this final distribution is just $\mathbb{G}_{\mathbf{x}}|\mathcal{P}'_{\mathbf{x}}$ since the $\mathbf{x}'$ and $(\hat{\mathsf{P}}, \hat{\mathsf{P}}')$ which are generated after $(\mathsf{P}, \mathsf{P}')$ is chosen do not affect the output. □

Expansion Fact 10. *Let $\mu > 0$, $\mathbf{x} \in \mathbb{F}^m$ and $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density μ. Then*

$$\left\{(\mathsf{P}, \mathbf{x}') : \begin{array}{c} (\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}|\mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}' \end{array}\right\} \approx_{\frac{9}{\sqrt{\mu q}}} \left\{(\mathsf{P}, \mathbf{x}') : \begin{array}{c} \mathsf{P} \sim \mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P} \end{array}\right\}.$$

Proof. Consider the following procedures to generate a pair $(\mathsf{P}, \mathbf{x}')$:

$$\left\{\begin{array}{c} (\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}|\mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}' \end{array}\right\} \approx_{\frac{8}{\sqrt{\mu q}}} \left\{\begin{array}{c} \hat{\mathbf{x}}' \sim \mathbb{F}^m \\ \mathsf{P}, \mathsf{P}' \sim \mathcal{P}_{\mathbf{x},\hat{\mathbf{x}}'} \\ \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}' \end{array}\right\} \equiv \left\{\begin{array}{c} \mathbf{x}' \sim \mathbb{F}^m \\ \mathsf{P}, \mathsf{P}' \sim \mathcal{P}_{\mathbf{x},\mathbf{x}'} \\ \hat{\mathbf{x}}' \sim \mathsf{P} \cap \mathsf{P}' \end{array}\right\} \approx_{\frac{1}{\sqrt{\mu q}}} \left\{\begin{array}{c} \mathsf{P} \sim \mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P} \\ \mathsf{P}' \sim \mathcal{P}_{\mathbf{x},\mathbf{x}'} \\ \hat{\mathbf{x}}' \sim \mathsf{P} \cap \mathsf{P}' \end{array}\right\}.$$

The first two procedures are within statistical distance $\frac{8}{\sqrt{\mu q}}$ of each other by Expansion Fact 9. The next two are identical because $\mathbf{x}'$ and $\hat{\mathbf{x}}'$ are identically distributed. The final two are within statistical distance $\frac{1}{\sqrt{\mu q}}$ by Claim 4 using the bipartite graph $A = \mathbb{F}^m$, $B = \mathcal{P}_{\mathbf{x}}$ which is a $q^{-1/2}$-expander. □

We now prove Claim 8, making use of the following additional claim which we will prove below.

Claim 9. *Let $\mu > 0$, $\mathbf{x} \in \mathbb{F}^m$ and let $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ be a subset of density μ. Then $\Delta\big(\mathcal{D}, \mathsf{Unif}(\mathcal{C}_{\mathbf{x}})\big) \leq \frac{3}{\sqrt{\mu q}}$, where $\mathcal{D}$ is the distribution which draws $(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}$ conditioned on $\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}}$, and then outputs the unique cube $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$ which contains both P and P'.*

Proof of Claim 8. For starters, consider the following three procedures for generating $\mathbf{x}' \in \mathbb{F}^m$:

$$\left\{ \begin{array}{c} (\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}} | \mathcal{P}'_{\mathbf{x}} \\ \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}' \end{array} \right\} \equiv \left\{ \begin{array}{c} (\hat{\mathsf{P}}, \hat{\mathsf{P}}') \sim \mathbb{G}_{\mathbf{x}} | \mathcal{P}'_{\mathbf{x}} \\ \Rightarrow \mathsf{C} \in \mathcal{C}_{\hat{\mathsf{P}}, \hat{\mathsf{P}}'} \\ \mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x}, \mathsf{C}} \\ \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}' \end{array} \right\} \approx_{\frac{3}{\sqrt{\mu q}}} \left\{ \begin{array}{c} \mathsf{C} \sim \mathcal{C}_{\mathbf{x}} \\ \mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x}, \mathsf{C}} \\ \mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}' \end{array} \right\}.$$

The first two are identical because $(\hat{\mathsf{P}}, \hat{\mathsf{P}}')$ and $(\mathsf{P}, \mathsf{P}')$ are identically distributed in the second distribution, and the third is within standard deviation $\frac{3}{\sqrt{\mu q}}$ of the second by Claim 9. However, consider the third distribution. By Claim 6 (second bullet), the probability that C is such that $\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}}) \leq \mu/2$ is at most $\frac{4}{\mu q}$. Moreover, whenever $\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}}) \geq \mu/2$ holds, by Expansion Fact 8, we have that the distribution which draws $\mathsf{P}, \mathsf{P}' \sim \mathcal{P}'_{\mathbf{x}, \mathsf{C}}$ and $\mathbf{x}' \sim \mathsf{P} \cap \mathsf{P}'$ and outputs $\mathbf{x}'$ is within statistical distance $\frac{3\sqrt{2}}{\sqrt{\mu q}}$ of $\mathsf{Unif}(\mathsf{C})$. Thus, the third distribution above is within statistical distance $\frac{4}{\mu q} + \frac{3\sqrt{2}}{\sqrt{\mu q}} \leq \frac{5}{\sqrt{\mu q}}$ of the distribution which draws $\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}$ and then outputs $\mathbf{x}' \sim \mathsf{C}$, *i.e.*, $\mathsf{Unif}(\mathbb{F}^m)$. □

Proof of Claim 9. Let $\mathcal{D}$ be the probability which draws $(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}} | \mathcal{P}'_{\mathbf{x}}$ and outputs the unique $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$ which contains P and P'. For any $\mathsf{C} \in \mathcal{C}_{\mathbf{x}}$, we have

$$\Pr\big[\mathcal{D} = \mathsf{C}\big] = \Pr_{(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}\big[\mathsf{P}, \mathsf{P}' \in \mathcal{P}_{\mathbf{x}, \mathsf{C}} \big| \mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}}\big] = \frac{1}{|\mathcal{C}_{\mathbf{x}}|} \cdot \frac{\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}})^2}{\Pr_{(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}[\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}}]},$$

by using Bayes' law to switch the probabilities. It follows that

$$\begin{aligned} \Delta\big(\mathcal{D}, \mathsf{Unif}(\mathcal{C}_{\mathbf{x}})\big) &= \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\left[\left| \frac{\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}})^2 - \Pr_{(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}[\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}}]}{\Pr_{(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}[\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}}]} \right|\right] \\ &\leq \mu^{-2} \cdot \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\Big[\big|\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}})^2 - \mu^2\big|\Big] + \mu^{-2} \cdot \frac{\mu}{q}, \end{aligned}$$

where the inequality follows from Claim 5 and $\Pr_{(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}\big[\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}}\big] \geq \mu^2$, which is Jensen:

$$\mu^2 = \mathbb{E}_{\mathbf{x}' \sim \mathbb{F}^m}\Big[\Pr_{\mathsf{P} \sim \mathcal{P}_{\mathbf{x}, \mathbf{x}'}}\big[\mathsf{P} \in \mathcal{P}'_{\mathbf{x}}\big]\Big]^2 \leq \mathbb{E}_{\mathbf{x}' \sim \mathbb{F}^m}\Big[\Pr_{\mathsf{P} \sim \mathcal{P}_{\mathbf{x}, \mathbf{x}'}}\big[\mathsf{P} \in \mathcal{P}'_{\mathbf{x}}\big]^2\Big] = \Pr_{(\mathsf{P}, \mathsf{P}') \sim \mathbb{G}_{\mathbf{x}}}\big[\mathsf{P}, \mathsf{P}' \in \mathcal{P}'_{\mathbf{x}}\big].$$

Finally, using Cauchy-Schwarz, we get

$$\begin{aligned} \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\Big[\big|\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}})^2 - \mu^2\big|\Big] &= \mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\Big[\big|\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}}) - \mu\big| \cdot \big(\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}}) + \mu\big)\Big] \\ &\leq \sqrt{\mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\Big[\big(\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}}) - \mu\big)^2\Big]} \cdot \sqrt{\mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\Big[\big(\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}}) + \mu\big)^2\Big]} \\ &= \sqrt{\Big[\mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}})^2)\big] - \mu^2\Big]} \cdot \sqrt{\Big[\mathbb{E}_{\mathsf{C} \sim \mathcal{C}_{\mathbf{x}}}\big[\mu_{\mathbf{x}, \mathsf{C}}(\mathcal{P}'_{\mathbf{x}})^2)\big] + 3\mu^2\Big]} \\ &\leq \sqrt{\frac{\mu}{q}} \cdot \sqrt{4\mu^2 + \frac{\mu}{q}} \leq \frac{\sqrt{5}\mu^2}{\sqrt{\mu q}}, \end{aligned}$$

where the final inequality has used Claim 5. Putting everything together gives

$$\Delta\big(\mathcal{D}, \mathsf{Unif}(\mathcal{C}_{\mathbf{x}})\big) \leq \frac{\sqrt{5}}{\sqrt{\mu q}} + \frac{1}{\mu q} \leq \frac{3}{\sqrt{\mu q}}.$$

□

References

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM (JACM)*, 45(3):501–555, 1998.

[AS98] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM (JACM)*, 45(1):70–122, 1998.

[AS03] Sanjeev Arora and Madhu Sudan. Improved low-degree testing and its applications. *Comb.*, 23(3):365–426, 2003.

[BDN17] Amey Bhangale, Irit Dinur, and Inbal Livni Navon. Cube vs. cube low degree test. In Christos H. Papadimitriou, editor, *8th Innovations in Theoretical Computer Science Conference, ITCS 2017, January 9-11, 2017, Berkeley, CA, USA*, volume 67 of *LIPIcs*, pages 40:1–40:31. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

[FGL+96] Uriel Feige, Shafi Goldwasser, Laszlo Lovász, Shmuel Safra, and Mario Szegedy. Interactive proofs and the hardness of approximating cliques. *Journal of the ACM (JACM)*, 43(2):268–292, 1996.

[FS95] Katalin Friedl and Madhu Sudan. Some improvements to total degree tests. In *Third Israel Symposium on Theory of Computing and Systems, ISTCS 1995, Tel Aviv, Israel, January 4-6, 1995, Proceedings*, pages 190–198. IEEE Computer Society, 1995.

[GLR+91] Peter Gemmell, Richard J. Lipton, Ronitt Rubinfeld, Madhu Sudan, and Avi Wigderson. Self-testing/correcting for polynomials and for approximate functions. In Cris Koutsougeras and Jeffrey Scott Vitter, editors, *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 32–42. ACM, 1991.

[HKSS24] Prahladh Harsha, Mrinal Kumar, Ramprasad Saptharishi, and Madhu Sudan. An improved line-point low-degree test. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*, pages 1883–1892. IEEE, 2024.

[IKW12] Russell Impagliazzo, Valentine Kabanets, and Avi Wigderson. New direct-product testers and 2-query PCPs. *SIAM Journal on Computing*, 41(6):1722–1768, 2012.

[MR08] Dana Moshkovitz and Ran Raz. Sub-constant error low degree test of almost-linear size. *SIAM J. Computing*, 38(1):140–180, 2008.

[MZ23] Dor Minzer and Kai Zheng. Approaching the soundness barrier: A near optimal analysis of the cube versus cube test. In Nikhil Bansal and Viswanath Nagarajan, editors, *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22-25, 2023*, pages 2761–2776. SIAM, 2023.

[RS92] Ronitt Rubinfeld and Madhu Sudan. Self-testing polynomial functions efficiently and over rational domains. In *Proceedings of the Third Annual ACM/SIGACT-SIAM Symposium on Discrete Algorithms, 27-29 January 1992, Orlando, Florida.*, pages 23–32, 1992.

[RS96] Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. Comput.*, 25(2):252–271, 1996.

[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 *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 475–484. ACM, 1997.

A Omitted Proofs

In this section we prove the claims which were omitted from the body of the paper.

A.1 Claims Used to Show that Excellent Points Come in Bunches

In this section we prove the claims which we used in the proof of Lemma 2. For convenience, recall that a pair $(\mathbf{x},\alpha)\in\mathbb{F}^m\times\mathbb{F}$ is *excellent* if $\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})\geq\frac{\varepsilon}{8}$ and if

$$\Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\Big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'}=\mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}\Big|\mathsf{P},\mathsf{P}'\in\mathcal{P}_{(\mathbf{x},\alpha)}\Big]\geq 1-\gamma.$$

Claim 2 (Restated). $\Pr_{\Pi}\big[\mathsf{AGR}\ \&\ (\mathbf{x},\alpha)\text{ not excellent}\big]<\frac{\varepsilon}{7}$.

Proof. Let $\mathsf{q}:=\Pr_{\Pi}\big[\mathsf{AGR}\ \&\ (\mathbf{x},\alpha)\text{ not excellent}\big]$ be the probability that we are trying to bound. Using Claim 5, we get

$$\begin{aligned}\mathsf{q}&\leq\mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha:(\mathbf{x},\alpha)\text{ not exc}}\Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\big[\mathsf{P},\mathsf{P}'\in\mathcal{P}_{(\mathbf{x},\alpha)}\big]\right]\\&\leq\mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha:(\mathbf{x},\alpha)\text{ not exc}}\Big(\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2+\frac{1}{q}\cdot\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})\Big)\right]=\frac{1}{q}+\mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha:(\mathbf{x},\alpha)\text{ not exc}}\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\right].\end{aligned}$$

There are two ways $(\mathbf{x},\alpha)$ could fail to be excellent. The first is if $\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})<\varepsilon/8$; note that

$$\mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha:\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})<\varepsilon/8}\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\right]<\frac{\varepsilon}{8}\cdot\mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha\in\mathbb{F}}\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})\right]=\frac{\varepsilon}{8}.$$

The second way that $(\mathbf{x},\alpha)$ could fail to be excellent is if

$$\gamma\cdot\Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\big[\mathsf{P},\mathsf{P}'\in\mathcal{P}_{(\mathbf{x},\alpha)}\big]<\Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\Big[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'}\neq\mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}\ \&\ \mathcal{T}(\mathsf{P})|_{\mathbf{x}}=\mathcal{T}(\mathsf{P}')|_{\mathbf{x}}=\alpha\Big]$$

holds. Say $(\mathbf{x},\alpha) \in B$ in this case. We have

$$\begin{aligned}
\mathbb{E}_B &:= \mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha:(\mathbf{x},\alpha)\in B} \mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\right] \le \mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha:(\mathbf{x},\alpha)\in B} \Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\left[\mathsf{P},\mathsf{P}'\in\mathcal{P}_{(\mathbf{x},\alpha)}\right]\right] \\
&< \frac{1}{\gamma}\cdot\mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha\in\mathbb{F}} \Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\left[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} \neq \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'} \;\&\; \mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}} = \alpha\right]\right] \\
&= \frac{1}{\gamma}\cdot\Pr_{\substack{\mathbf{x}\sim\mathbb{F}^m \\ (\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}}\left[\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'} \neq \mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'} \;\&\; \mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}}\right] \\
&\le \frac{1}{\gamma}\cdot\mathbb{E}_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}}\left[\mathbb{1}_{\mathcal{T}(\mathsf{P})|_{\mathsf{P}\cap\mathsf{P}'}\neq\mathcal{T}(\mathsf{P}')|_{\mathsf{P}\cap\mathsf{P}'}}\cdot\Pr_{\mathbf{x}\sim\mathsf{P}\cap\mathsf{P}'}\left[\mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}}\right]\right] \le \frac{d}{\gamma q}.
\end{aligned}$$

The last inequality is Schwartz-Zippel; the first inequality is Jensen. Putting everything together proves the claim: $\mathsf{q} \le \frac{1}{q} + \frac{\varepsilon}{8} + \frac{d}{\gamma q} \le \frac{\varepsilon}{7}$. □

Claim 3 (Restated). $\Pr_{\Pi}\left[\mathsf{AGR} \;\&\; (\mathbf{x},\alpha) \text{ excellent} \;\&\; \mathcal{T}(\mathsf{P}) \neq f_{(\mathbf{x},\alpha)}|_{\mathsf{P}}\right] < \frac{11\varepsilon}{100}$.

Proof. Let $\mathsf{q} := \Pr_{\Pi}\left[\mathsf{AGR} \;\&\; (\mathbf{x},\alpha) \text{ excellent} \;\&\; \mathcal{T}(\mathsf{P}) \neq f_{(\mathbf{x},\alpha)}|_{\mathsf{P}}\right]$ be the probability we are trying to bound, and for an excellent $(\mathbf{x},\alpha) \in \mathbb{F}^m \times \mathbb{F}$, let $\mathcal{P}'_{(\mathbf{x},\alpha)} := \left\{\mathsf{P} \in \mathcal{P}_{(\mathbf{x},\alpha)} : \mathcal{T}(\mathsf{P}) \neq f_{(\mathbf{x},\alpha)}|_{\mathsf{P}}\right\}$. We have

$$\begin{aligned}
\mathsf{q} &\le \mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha:(\mathbf{x},\alpha)\text{ exc}} \Pr_{(\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}\left[\mathsf{P}\in\mathcal{P}'_{(\mathbf{x},\alpha)} \;\&\; \mathsf{P}'\in\mathcal{P}_{(\mathbf{x},\alpha)}\right]\right] \\
&\le \mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha:(\mathbf{x},\alpha)\text{ exc}} \frac{1}{10}\cdot\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2 + \frac{1}{q}\cdot\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})\right] \le \frac{1}{10}\cdot\mathbb{E}_{\mathbf{x}\sim\mathbb{F}^m}\left[\sum_{\alpha\in\mathbb{F}}\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})^2\right] + \frac{1}{q} \\
&\le \frac{1}{10}\cdot\Pr_{\substack{\mathbf{x}\sim\mathbb{F}^m \\ (\mathsf{P},\mathsf{P}')\sim\mathbb{G}_{\mathbf{x}}}}\left[\mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \mathcal{T}(\mathsf{P}')|_{\mathbf{x}}\right] + \frac{1}{q} \le \frac{1}{10}\cdot\left(\varepsilon + d/q\right) + \frac{1}{q} \le \frac{11\varepsilon}{100},
\end{aligned}$$

and the claim follows. The first inequality on the second line follows from Claim 5, plugging in $\mu_{\mathbf{x}}(\mathcal{P}'_{(\mathbf{x},\alpha)}) \le \frac{1}{10}\cdot\mu_{\mathbf{x}}(\mathcal{P}_{(\mathbf{x},\alpha)})$, which holds by Lemma 1. The first and second inequalities on the third line are Jensen, and Schwartz-Zippel, respectively. □

A.2 The Interpolation Lemma

Let $\mathbb{F}$ be a finite field of size $|\mathbb{F}| = q$, let $\mathcal{P}$ denote the set of 2-planes in $\mathbb{F}^3$, let $d \in \mathbb{N}$ with $d < q$ be a degree parameter, and let $\mathcal{T}$ be a planes table which assigns to each $\mathsf{P} \in \mathcal{P}$ a bivariate degree d polynomial. Let $r, D \in \mathbb{N}$ be additional integer parameters such that $d|D$, we write $s = D/d \in \mathbb{N}$.

Lemma 5 (Restated). *Assume $D \ge 5$, $s \ge 10$, and $r < Ds/60$. For any $S \subset \mathcal{P}$ of size $|S| = r$, there exists a non-zero 4-variate $A(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ of $(1,1,1,d)$-degree at most D, such that $\mathsf{Disc}_Z(A) \not\equiv 0$, and $A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0$ for all $\mathsf{P} \in S$.*

The idea of the proof is to show that the number of degrees of freedom available to a 4-variate polynomial of $(1,1,1,d)$-degree at most D is large enough to ensure that a non-zero solution exists to the linear constraints imposed by requiring that the polynomial vanish at every $\mathsf{P} \in S$. A complication is introduced by demanding also that the polynomial has non-vanishing discriminant. The following

lemma from [HKSS24] allows incorporating this extra requirement into the dimension counting proof framework. Let $\Gamma_S \subset \mathbb{F}[\mathbf{X}, Z]$ be the set of 4-variate polynomials $A(\mathbf{X}, Z)$ of $(1,1,1,d)$-degree at most D such that $A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0$ for all $\mathsf{P} \in S$.

Lemma 10 ([HKSS24], Lemma 2.9). *If there exists $A \in \Gamma_S$ such that $\partial_Z(A) \not\equiv 0$, then there exists a (possibly different) $A' \in \Gamma_S$ such that $\mathsf{Disc}_Z(A') \not\equiv 0$. Here $\partial_Z(A)$ denotes the formal partial derivative of A with respect to Z (also known as the Hasse derivative).*

Proof of Lemma 5. Let $p \in \mathbb{N}$ be the characteristic of $\mathbb{F}$, and let

$$T_{d,D,p} := {}^{\#}\Big\{(i_1,i_2,i_3,j) \in \mathbb{Z}^4_{\geq 0} : i_1 + i_2 + i_3 + dj \leq D \;\&\; j \not\equiv 0 \bmod p\Big\}$$

be the number of 4-variate monomials in $\mathbb{F}[\mathbf{X}, Z]$ of $(1,1,1,d)$-degree at most D whose Z-partial derivative does not vanish. Any non-zero polynomial in the $T_{d,D,p}$-dimensional vector space spanned by these monomials has $(1,1,1,d)$-degree at most D and has non-vanishing Z-partial derivative. Note that, for each $\mathsf{P} \in S$, the requirement that $A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0$ imposes at most $\binom{D+2}{2}$ linear constraints on the coefficients of A. Therefore, the following claim, which says that $T_{d,D,p} - r \cdot \binom{D+2}{2} > 0$, implies that there exists a polynomial in Γ_S whose Z-partial derivative does not vanish. By Lemma 10, there exists a (possibly different) polynomial in Γ_S whose discriminant does not vanish. The lemma follows. □

Claim 10. *Continuing under the assumptions that $p \geq 2$, $D \geq 5$, and $s \geq 10$, we have*

$$T_{d,D,p} \geq \frac{Ds}{60} \cdot \binom{D+2}{2}.$$

Proof. For $k \in \{0, \ldots, s\}$, let

$$X_{d,D,k} := {}^{\#}\Big\{(i_1,i_2,i_3) \in \mathbb{Z}^3_{\geq 0} : i_1 + i_2 + i_3 \leq D - dk\Big\}.$$

Since $X_{d,D,k}$ decreases as k increases,

$$T_{d,D,p} = \sum_{k=1}^{s} \mathbb{1}_{p \nmid k} \cdot X_{d,D,k} \geq \left(1 - \frac{1}{p}\right) \cdot \sum_{k=1}^{s} X_{d,D,k} \geq \frac{1}{2} \cdot \sum_{k=1}^{s} X_{d,D,k},$$

using $p \geq 2$. Since $X_{d,D,k} = \binom{D-dk+3}{3}$,

$$\begin{aligned} T_{d,D,p} \Big/ \binom{D+2}{2} &\geq \frac{1}{2} \cdot \sum_{k=1}^{s} X_{d,D,k} \Big/ \binom{D+2}{2} = \frac{1}{2} \cdot \sum_{k=1}^{s} \binom{D-dk+3}{3} \Big/ \binom{D+2}{2} \\ &\geq \frac{1}{6} \cdot \sum_{k=1}^{s} \frac{(D-dk)^3}{(D+2)^2} \geq \frac{1}{6} \cdot \frac{d^3}{2D^2} \cdot \sum_{k=1}^{s} (s-k)^3 = \frac{d^3}{12D^2} \cdot \sum_{k=0}^{s-1} k^3 \\ &= \frac{d^3}{12D^2} \cdot \frac{s^2(s-1)^2}{4} \geq \frac{d^3}{12D^2} \cdot \frac{s^4}{5} = \frac{Ds}{60}, \end{aligned}$$

as desired. We have used $(D+2)^2 \leq 2D^2$ which holds because $D \geq 5$; we have used the formula $\sum_{k=0}^{s-1} k^3 = \frac{s^2(s-1)^2}{4}$; and we have used $\frac{(s-1)^2}{4} \geq \frac{s^2}{5}$, which holds because $s \geq 10$. □

A.3 Low-Degree Roots on Restrictions to Global Low-Degree Roots

In this section, we prove Lemma 9 following the argument from [HKSS24].

Lemma 9 (Restated). *Let $d, D \in \mathbb{N}$ be degree parameters. Fix a pair $(\mathbf{x}, \alpha) \in \mathbb{F}^3 \times \mathbb{F}$, a subset $\mathcal{P}'_{\mathbf{x}} \subset \mathcal{P}_{\mathbf{x}}$ of size $|\mathcal{P}'_{\mathbf{x}}| > D$, such that $\mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \alpha$ for all $\mathsf{P} \in \mathcal{P}'_{\mathbf{x}}$, and a 4-variate polynomial $A(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ of $(1,1,1,d)$-degree at most D, such that α is a simple zero of the univariate polynomial $A(\mathbf{x}, Z) \in \mathbb{F}[Z]$. If $A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0$ for all $\mathsf{P} \in \mathcal{P}'_{\mathbf{x}}$, then there exists a trivariate, degree d polynomial $f(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ such that $A\big(\mathbf{X}, f(\mathbf{X})\big) \equiv 0$ and such that $f|_{\mathsf{P}} = \mathcal{T}(\mathsf{P})$ for all $\mathsf{P} \in \mathcal{P}'_{\mathbf{x}}$.*

The global root is built using the following procedure based on Newton's method.

Claim 11 (Newton Iteration). *Let $m \in \mathbb{N}$ be a dimension parameter. Let $(\hat{\mathbf{x}}, \hat{\alpha}) \in \mathbb{F}^m \times \mathbb{F}$. Suppose $\hat{A}(\mathbf{X}, Z) \in \mathbb{F}[\mathbf{X}, Z]$ is an $(m+1)$-variate polynomial such that the univariate $\hat{A}(\hat{\mathbf{x}}, Z) \in \mathbb{F}[Z]$ has a simple zero at $\hat{\alpha}$. Then there exists a unique family of m-variate polynomials $\{\Phi_k(\mathbf{X})\}_{k \in \mathbb{N}}$ such that for all $k \in \mathbb{N}$, the following all hold:*

$$(1)\ \deg(\Phi_k) \leq k; \quad (2)\ \Phi_k(\hat{\mathbf{x}}) = \hat{\alpha}; \quad (3)\ \hat{A}\big(\mathbf{X}, \Phi_k(\mathbf{X})\big) \equiv 0 \bmod (\mathbf{X})^{k+1}.$$

Proof of Lemma 9. Invoke Claim 11 on the polynomial $A(\mathbf{X}, Z)$ and point $(\mathbf{x}, \alpha) \in \mathbb{F}^3 \times \mathbb{F}$ to get a family $\{\Phi_k(\mathbf{X})\}_{k \in \mathbb{N}}$ of trivariate polynomials such that for all $k \in \mathbb{N}$: $\deg(\Phi_k) \leq k$, $\Phi_k(\mathbf{x}) = \alpha$, and $A\big(\mathbf{X}, \Phi_k(\mathbf{X})\big) \equiv 0 \bmod (\mathbf{X})^{k+1}$ all hold. Additionally, consider for some $\mathsf{P} \in \mathcal{P}'_{\mathbf{x}}$, the trivariate polynomial A_{P} which is the restriction of A to P. Specifically, $A_{\mathsf{P}}(\mathbf{Y}, Z) \in \mathbb{F}[\mathbf{Y}, Z]$ uses the two-variables in $\mathbf{Y}$ to parametrize P and obtain an assignment to the three-variables of $\mathbf{X}$ via the embedding $\mathsf{P} \hookrightarrow \mathbb{F}^3$. If $\mathbf{y} \in \mathbb{F}^2$ is the point which parametrizes $\mathbf{x} \in \mathsf{P}$, then note that the univariate polynomial $A_{\mathsf{P}}(\mathbf{y}, Z)$ is precisely $A(\mathbf{x}, Z)$, and so has a simple zero at α. We invoke Claim 11 on $A_{\mathsf{P}}(\mathbf{y}, Z)$ to obtain another batch of (this time bivariate) polynomials $\{\Psi_{\mathsf{P},k}\}_{k \in \mathbb{N}}$ such that for all $k \in \mathbb{N}$, $\deg(\Psi_{\mathsf{P},k}) \leq k$, $\Psi_{\mathsf{P},k}(\mathbf{y}) = \alpha$, and $A_{\mathsf{P}}\big(\mathbf{Y}, \Psi_{\mathsf{P},k}(\mathbf{Y})\big) \equiv 0 \bmod (\mathbf{Y})^{k+1}$.

Now, consider the three bivariate polynomials $\Psi_{\mathsf{P},d}$, $\Phi_d|_{\mathsf{P}}$, and $\mathcal{T}(\mathsf{P})$, all defined on P. They all have degree at most d; they satisfy $\Psi_{\mathsf{P},d}(\mathbf{y}) = \Phi_d(\mathbf{x}) = \mathcal{T}(\mathsf{P})|_{\mathbf{x}} = \alpha$; and finally,

$$A\big(\mathbf{Y}, \Psi_{\mathsf{P},d}(\mathbf{Y})\big) \equiv A\big(\mathsf{P}, \Phi_d|_{\mathsf{P}}\big) \equiv A\big(\mathsf{P}, \mathcal{T}(\mathsf{P})\big) \equiv 0 \bmod (\mathbf{Y})^{d+1}.$$

By the uniqueness of the polynomials guaranteed by Claim 11, it must be that $\Psi_{\mathsf{P},d} \equiv \Phi_d|_{\mathsf{P}} \equiv \mathcal{T}(\mathsf{P})$, so in particular, $\Phi_d|_{\mathsf{P}} \equiv \mathcal{T}(\mathsf{P})$ holds for all $\mathsf{P} \in \mathcal{P}'_{\mathbf{x}}$. Finally, consider the trivariate polynomial $A\big(\mathbf{X}, \Phi_d(\mathbf{X})\big)$. It has degree at most D, but vanishes on every $\mathsf{P} \in \mathcal{P}'_{\mathbf{x}}$. Since $|\mathcal{P}'_{\mathbf{x}}| > D$, Schwartz-Zippel implies that $A\big(\mathbf{X}, \Phi_d(\mathbf{X})\big) \equiv 0$. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il