Electronic Colloquium on Computational Complexity, Report No. 315 (2026)

On derandomizing the line-point low-degree test

Prahladh Harsha* Swastik Kopparty† Mrinal Kumar* Ramprasad Saptharishi*
Madhu Sudan‡

Abstract

We investigate the derandomized version of the classical line-point low-degree test in the high-error regime in the bivariate setting and reveal some unexpected behavior. The classical line-point low-degree test takes an m-variate function f over a finite field $\mathbb{F}_q$, queries it along a random line and accepts if the restriction of the function to this line is a low-degree polynomial. The high-error version of (the analysis of) this test asserts that if f has at least ε expected local agreement with a degree-k univariate polynomial on a random line, then in fact f is non-trivially close to some degree-k m-variate polynomial even as ε approaches 0 (provided q is sufficiently large compared to k and $1/\varepsilon$). The derandomized version of the problem asks if the same holds when the line is not chosen uniformly over all possible lines but rather from a small set. Derandomized analyses of low-degree tests play a crucial role in obtaining near-linear sized PCPs. In this paper we explore the bivariate case ($m = 2$).

We show, somewhat surprisingly, that there exists a function $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ and a set of lines $\mathscr{L}$ in $\mathbb{F}_q^2$ of size nearly $q^{3/2}$ such that on every line in $\mathscr{L}$, f has agreement $\approx 1/2$ on average with some univariate polynomial of degree $k = \sqrt{q}/2$ and yet f is $1 - O(q^{-1/2})$ far from every polynomial of degree $O(k)$. On the positive side, we show that once the field size q is at least $k^2/\operatorname{poly}(\varepsilon)$ such examples disappear and we can get sets of lines of size $O(q/\varepsilon^{O(1)})$ on which the low-degree test has a high-error analysis.

On the way to our positive result, we show a new high-degree version of the classical two-direction Polishchuk–Spielman divisibility lemma. It deals with finding a low-degree global root $Z = U(X, Y)$ of a trivariate polynomial $Q(X, Y, Z)$, based on restrictions of Q to lines in $r > \deg_Z(Q)$ different directions (generalizing the original $r = 2$ and $\deg_Z(Q) = 1$ case). Specifically, it states that if Q has a low-degree root $Z = U_{a,b}(X)$ for all lines $Y = aX + b$ in each of those r directions, then Q has a low-degree global root $Z = U(X, Y)$. This high degree Polishchuk–Spielman lemma is proved by a new technique: using simultaneous Hensel lifting of *consistent* roots on many parallel lines.

Our negative result addresses one of the big challenges in analyzing low-degree tests, namely the rarity of interesting counterexamples that offer concrete barriers.

*Tata Institute of Fundamental Research, Mumbai, India. {prahladh, mrinal, ramprasad}@tifr.res.in. Research supported by the Department of Atomic Energy, Government of India, under project number RTI400112, and in part by research grants from Google and Premji Invest.

†Department of Computer Science and Department of Mathematics, University of Toronto, Canada. swastik@utoronto.ca.

‡School of Engineering and Applied Sciences, Harvard University, Cambridge, Massachusetts, USA.madhu@cs.harvard.edu. Supported in part by a Simons Investigator Award.

ISSN 1433-8092

Contents

1 Introduction **2**
- 1.1 Our results . . . 4

2 Overview of the proofs **7**

3 Notations and preliminaries **10**
- 3.1 Notations . . . 10
- 3.2 Preliminaries . . . 11
- 3.3 Hasse derivatives . . . 11
- 3.4 Resultant and discriminant . . . 13
- 3.5 Power series roots . . . 14
- 3.6 The Polishchuk–Spielman lemma . . . 14
- 3.7 Pruning to subgraph of high min degree . . . 15

4 Consistent roots on parallel lines to global rational roots **16**
- 4.1 The case of axis parallel lines . . . 16
- 4.2 From axis parallel to the general case . . . 18

5 Generalizations of the Polishchuk–Spielman lemma **19**
- 5.1 Preprocessing . . . 20
- 5.2 Finding two good directions . . . 21
- 5.3 Rational roots from $\mathscr{L}_{i_0}$ and $\mathscr{L}_{j_0}$ . . . 21
- 5.4 From a rational function to a polynomial . . . 23
- 5.5 A Z-root of Q . . . 23

6 The low-degree test **24**
- 6.1 Pruning to *good* lines, *good* points . . . 25
- 6.2 Interpolation . . . 25
- 6.3 Proof of Theorem 1.2 . . . 28

7 Counterexamples when $k \gg q^{1/2}$ **30**

1 Introduction

In this paper, we study the problem of "derandomizing" the "line-point" low-degree test in the "high-error" regime. We show a surprising limitation on how well this test can be derandomized over fields of size quadratic in the degree parameter, and complement this with an analysis of the derandomized line-point test over fields of at least quadratic size (in the degree parameter). We expand on these terms and results below.

Low-degree testing, one of the classical problems in property testing, checks if a given function, viewed as a table of values, is close to the evaluation of a polynomial of low total degree, by querying the function

only on a few points of the domain. More precisely, given a finite field $\mathbb{F}$ of size q, a dimension parameter m and a degree parameter k, the goal of low-degree testing is to check if the function $f\colon \mathbb{F}^m \to \mathbb{F}$ is close to the evaluation of some m-variate polynomial P of total degree at most k, i.e., $P \in \mathscr{P}_{k,m}$, where $\mathscr{P}_{k,m}$ denotes the space of all such polynomials, by querying the function f on very few points of $\mathbb{F}^m$. The most natural such test is the *line-point test* of Rubinfeld and Sudan [RS96]: pick a uniformly random line ℓ in $\mathbb{F}^m$, query f at all points of ℓ, and accept if the restriction $f|_\ell$ is the evaluation of a univariate polynomial of degree at most k (i.e., $f|_\ell \in \mathscr{P}_{k,1}$). Low-degree tests, and the line-point test in particular, are the algebraic core of the proof of the PCP theorem [AS98, ALMSS98], and improvements to their analyses have repeatedly translated into improvements in the parameters of PCPs.

The soundness of the line-point test is typically studied in two regimes. In the *low-error* (or unique-decoding) regime, where the test rejects with small constant probability δ, the early works [RS96, AS98, ALMSS98], culminating in those of Polishchuk and Spielman [PS94] and Friedl and Sudan [FS95], show that f is $O(\delta)$-close to a degree-k polynomial as soon as $q = \Omega(k)$. To state the results in the *high-error* (or list-decoding) regime, it is convenient to compare the expected local agreement of f with degree-k univariate polynomials, namely $\mathbb{E}_\ell[\mathrm{agree}(f|_\ell, \mathscr{P}_{k,1})]$, with the global agreement $\mathrm{agree}(f, \mathscr{P}_{k,m})$.[1] For the line-point test over fields of size $q \geq k^4/\operatorname{poly}(\varepsilon)$, Arora and Sudan [AS03] proved that $\mathbb{E}_\ell[\mathrm{agree}(f|_\ell, \mathscr{P}_{k,1})] \geq \varepsilon$ implies $\mathrm{agree}(f, \mathscr{P}_{k,m}) \geq \operatorname{poly}(\varepsilon)$. While this gave an analysis of the line-point test in the high-error regime, it worked only when the field size was at least quartic in the degree. In parallel and independent work, Raz and Safra [RS97] proved a similar result, this time over linear-sized fields (i.e., $q = \Omega(k)/\operatorname{poly}(\varepsilon)$), at the cost of replacing lines by planes (and hence $O(q)$ queries by $O(q^2)$ queries). In recent work [HKSS24], a subset of the authors of this paper gave a high-error analysis of the line-point test over fields of size $\Omega(k)/\operatorname{poly}(\varepsilon)$, thereby obtaining a common strengthening of the above two results. In this work, we ask if this improved analysis of the line-point test can be extended to a derandomized test.

Derandomized low-degree tests. A second, equally important, axis along which low-degree tests have been improved is their *randomness complexity*. The line-point test over $\mathbb{F}^m$ picks a random line, which requires roughly $(2m-2)\log q$ random bits, since there are about q^{2m-2} lines in $\mathbb{F}^m$. When a low-degree test is used inside a PCP, the randomness of the test essentially dictates the size of the resulting proof, and so reducing the number of lines (or planes) the test uses is the key step in constructing PCPs of nearly-linear size [GS06, PS94, BSVW03, BGHSV06, BGHSV05, MR08, MR10a, MR10b]. In fact, it follows from Goldreich and Sudan [GS06] that $|\mathbb{F}^m|^{1+o(1)}$ lines suffice (to be precise $|\mathbb{F}^m| \cdot \exp(\widetilde{O}(\sqrt{\log|\mathbb{F}^m|}))$ lines), however their proof does not yield an explicit set of such lines. The natural way to derandomize the test is to restrict the *directions* of the lines: instead of allowing every direction in $\mathbb{F}^m$, one allows only directions from a small, structured set—for instance, directions from a small-biased set [BSVW03] or directions in $\mathbb{H}^m$ for a subfield $\mathbb{H} \subseteq \mathbb{F}$ [MR08]. The latter reduces the number of lines from about q^{2m-2} to about $q^{m-1} \cdot |\mathbb{H}|^{m-1}$.

In the low-error regime, derandomized line-point tests are well understood. Already the Polishchuk–Spielman analysis [PS94] is a derandomized analysis: for bivariate functions it uses lines in only *two* directions (the axis-parallel lines), and it is this feature that made it useful for nearly-linear sized PCPs. Ben-Sasson, Sudan, Vadhan and Wigderson [BSVW03] extended this to the m-variate line-point test with directions drawn from a small-biased set. In the high-error regime, however, the only derandomized low-degree test

[1] Here, for functions f, g on a common domain, $\mathrm{agree}(f,g) := \Pr_z[f(z) = g(z)]$, where z is uniform over the domain, and for a family $\mathscr{F}$ of functions, $\mathrm{agree}(f,\mathscr{F}) := \max_{g\in\mathscr{F}} \mathrm{agree}(f,g)$.

is the derandomized *plane-point* test of Moshkovitz and Raz [MR08], which derandomizes the Raz–Safra test [RS97] and which works over fields of size $q = k/\operatorname{poly}(\varepsilon)$ as long as the subfield satisfies $|\mathbb{H}| \geq \operatorname{poly}(1/\varepsilon)$. This leaves open the following question.

Is there a high-error analysis of a derandomized line-point test?

The Raz–Safra and Moshkovitz–Raz analyses are coding-theoretic and use the fact that two planes typically intersect in a line, on which the restricted polynomials form a code of distance $1 - o(1)$; two lines intersect in at most one point, so this approach does not apply to line-point tests, which instead have a very algebraic analysis [AS03, HKSS24]. One could, nevertheless, ask if the Moshkovitz–Raz approach to derandomizing the plane-point test of Raz–Safra extends to the recent improved analysis of the line-point test [HKSS24]. The crucial observation of Moshkovitz–Raz is that besides the above coding-theoretic fact, the Raz–Safra analysis uses just the sampling properties of the planes-vs-points bipartite graph, which even the derandomized-planes-vs-points graph has, and hence the Raz–Safra analysis carries over. The algebraic analyses of the line-point test [AS03, HKSS24], on the other hand, crucially use lines in a large number of directions, a number that grows with the degree k, whereas a derandomized test with r directions offers only r of them, where r should ideally depend only on ε. This implies that a Moshkovitz–Raz-style transformation of the analysis of [HKSS24] is not feasible.

Nevertheless, in this work, we show that, with substantial modifications, the analysis of [HKSS24] can be adapted to the setting where r, the number of directions, is considerably smaller than the degree k.

1.1 Our results

In this subsection, we describe our three results: (1) the necessity of quadratically large fields for derandomizing the line-point low-degree test, (2) an analysis of a derandomized line-point test in which the number of directions satisfies $r \ll k$ provided $q \geq k^2/\operatorname{poly}(\varepsilon)$, and (3) a generalization of the Polishchuk–Spielman divisibility lemma. We state all these results in the bivariate setting, i.e., $m = 2$ and $f\colon \mathbb{F}^2 \to \mathbb{F}$, since this case already presents several challenges, as we will soon see. Unlike the analysis of the bivariate test in [HKSS24], we do not know if the analysis in Theorem 1.2 can be lifted from the bivariate to the multivariate case.

Derandomization is infeasible in subquadratic-sized fields. The current best analyses of the line-point test [HKSS24] as well as the analysis of the derandomized plane-point test [MR08] in the high-error regime work over fields of size $k/\operatorname{poly}(\varepsilon)$. However, a similar derandomized analysis of the line-point test has remained elusive. Our first result shows that such a derandomization using lines whose slopes come from a subfield is in fact infeasible as long as the field size is subquadratic in the degree parameter, at least for fields of small characteristic. This infeasibility result is especially interesting since counterexamples that offer concrete barriers are rare in the study of low-degree tests.

Theorem 1.1 (Necessity of large fields for LDT)**.** *For every prime p, $\varepsilon \in (0,1)$ of the form p^{-r} and $s \in \mathbb{N}$, the following holds: Let $\mathbb{F}$ be the finite field of size $q = p^{2rs} = (1/\varepsilon)^{2s}$, H be the subfield of $\mathbb{F}$ of size $p^{rs} = (1/\varepsilon)^s$ and $k = \varepsilon\sqrt{q} = p^{r(s-1)}$ the degree parameter. For any $a, b \in \mathbb{F}$, let $\ell_{a,b}\colon \mathbb{F} \to \mathbb{F}^2$ denote the line given by $\ell_{a,b}(t) = (t, at + b)$. Let $\mathscr{L} = \{\ell_{a,b} \mid a \in H, b \in \mathbb{F}\}$. Observe that $\mathscr{L}$ consists of all lines with slope in the subfield H.*

There exist a function $f\colon \mathbb{F}^2 \to \mathbb{F}$ and univariate polynomials P_ℓ of degree k, one for each $\ell \in \mathscr{L}$, such that $\mathbb{E}_{\ell\in\mathscr{L}}[\mathrm{agree}(f|_\ell, P_\ell)] \geq \varepsilon$ and yet $\mathrm{agree}(f, \mathscr{P}_{O(k),2}) \leq O(\varepsilon/\sqrt{q})$.

Furthermore, there exists a trivariate polynomial $Q(X,Y,Z)$ of Z-degree $1/\varepsilon$ and $(1,1,k)$-degree $\sqrt{q}+1$ such that for each $\ell \in \mathscr{L}$, P_ℓ is a Z-root of the restriction of Q to ℓ, yet Q has no polynomial Z-root.

This choice of directions is precisely the subfield-based derandomization of [MR08], thus ruling out a similar derandomization for the line-point test with comparable parameters.

The special case $\varepsilon = \frac{1}{2}$ (i.e., $p = 2$ and $r = 1$) shows that there exists a function f having expected local agreement with degree k univariate polynomials as large as $\frac{1}{2}$, but still f is $(1 - o(1))$-far from bivariate polynomials of degree at most $O(k)$.

An important caveat of these counterexamples is that the characteristic of the underlying field is small (in particular, $\mathrm{char}(\mathbb{F}) \leq 1/\varepsilon$), and it is a natural question to understand if these examples can be extended to finite fields of large characteristic.

A high-error derandomized line-point test. We now complement the above counterexample by showing that once the field size is quadratically large, any set of r directions for $r = \mathrm{poly}(1/\varepsilon)$ suffices.

Theorem 1.2 (Analysis of derandomized line-point test)**.** *There is a constant $c \in \mathbb{N}$ such that the following holds for every $\varepsilon > 0$, every finite field $\mathbb{F}$ of size q, and all natural numbers k, r satisfying $q \geq k^2/\varepsilon^c$ and $r \geq 1/\varepsilon^c$. Let U be a set of r distinct directions in $\mathbb{F}^2$, and let $\mathscr{L}$ be the set of* all *lines along these r directions (i.e., $|\mathscr{L}| = rq$). Then for any $f\colon \mathbb{F}^2 \to \mathbb{F}$, we have*

$$\mathop{\mathbb{E}}_{\ell\in\mathscr{L}}\big[\mathrm{agree}(f|_\ell, \mathscr{P}_{k,1})\big] \geq \varepsilon \implies \mathrm{agree}(f, \mathscr{P}_{2k,2}) \geq \varepsilon^c\,.$$

Three features of this statement deserve comment.

- First, the number of directions must grow with $1/\varepsilon$: if $g\colon \mathbb{F} \to \mathbb{F}$ is a random univariate function and $f(X,Y) := g(Y - mX)$, where the set of directions U includes the direction with slope m, then f is constant on every line with slope m, so the expected local agreement is at least $1/r$, and yet f has negligible agreement with every low-degree polynomial. Thus $r > 1/\varepsilon$ is necessary, and our theorem shows that $r = \mathrm{poly}(1/\varepsilon)$ suffices.

- Second, the conclusion shows agreement with a polynomial of degree $2k$ rather than k. Some loss of this kind is unavoidable once the directions are restricted: if the set U consists of the directions given by r distinct slopes $m_1, \ldots, m_r$ and $(r-1)$ divides k, the polynomial

  $$g(X,Y) := \prod_{i=1}^{r} (Y - m_i X)^{k/(r-1)}$$

  has degree at most k on every line with slope in U, but has total degree $rk/(r-1) > k$. Thus $f = g$ passes the test with probability 1, i.e., has perfect local agreement, but is far from every polynomial of degree k. In a companion paper, we show that the total degree of such polynomials is bounded above by $rk/(r-1)$. (The same phenomenon appears for $r = 2$ in the Polishchuk–Spielman analysis [PS94], which also concludes with a polynomial of degree $2k$.)

- Third, our requirement on the field size is quadratic in the degree k, unlike the derandomized plane-point test of Moshkovitz–Raz [MR08], which requires only a linear dependence. As observed in Theorem 1.1, such a quadratic dependence is necessary at least for low-characteristic fields. More precisely, for a field $\mathbb{F}_q$ with characteristic at most $1/\varepsilon$, we require $q \geq (k/\varepsilon)^2$ for derandomization to work with lines in even $\sqrt{q}$ directions, while the condition $q \geq k^2/\varepsilon^c$ in the above theorem shows that this is tight up to the value of the constant c and in this case, the number of directions can be made as low as $\mathrm{poly}(1/\varepsilon)$.

A Polishchuk–Spielman lemma for few directions and high Z-degree. At the heart of the Polishchuk–Spielman analysis [PS94] is a divisibility lemma, which can alternatively be stated (see [HKSS24, Lemma 1.3]) as follows. Let $Q(X, Y, Z) = A(X, Y)Z - B(X, Y)$ be a trivariate polynomial with Z-degree one. Suppose the restriction of Q to many axis-parallel lines has a Z-root that is a polynomial of degree at most k; in other words, for various restrictions of the form $X = a$ or $Y = b$, the restricted polynomial A divides the restricted polynomial B and the quotient has degree at most k. Then Q itself has a Z-root that is a bivariate polynomial of degree at most k in each variable; that is, A divides B and the quotient has degree at most k in each variable. Intuitively, the global root is what explains the roots on the various restrictions.

A natural question is whether this lemma generalizes to polynomials Q of Z-degree larger than one. Such a generalization was crucial to the analysis of the line-point test in the high-error regime in [HKSS24] (see [HKSS24, Lemma 1.4]). However, the generalization there required, as a hypothesis, that Q have a low-degree Z-root on its restrictions to lines in many directions (not just two, as in the original Polishchuk–Spielman setting). One could ask for the smallest number of directions for which such a generalization holds. If the number of directions equals the Z-degree, i.e., $r = \deg_Z(Q)$, then the statement is simply false: for distinct $m_1, \ldots, m_r$ and irreducible $g_1, \ldots, g_r$ of degree k, the polynomial

$$Q(X, Y, Z) := \prod_{i=1}^{r} \big((Y - m_i X)Z - g_i(X, Y)\big)$$

has a degree-k Z-root on every line $Y = m_i X + c$ with $c \neq 0$, but no polynomial Z-root. (The case $r = 2$ of this example appears in [HKSS24].)

Our third result shows that this example is essentially the only obstruction: as soon as the number of directions exceeds the Z-degree, the generalized lemma holds, provided the field is large enough.

Lemma 1.3 (Generalized Polishchuk–Spielman lemma)**.** *Let $Q(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ have $(1, 1, k)$-degree D, and suppose that the restriction of Q to every line in $r > \deg_Z(Q)$ directions has a Z-root that is a univariate polynomial of degree at most k. If $q \geq \mathrm{poly}(\deg_Z(Q)) \cdot Dk$, then Q has a Z-root $P(X, Y) \in \mathbb{F}[X, Y]$ of total degree at most $2k$. Moreover, there exist two directions (among the r directions) such that the restriction of P agrees with the given roots on all but $O(Dk)$ of the lines in these two directions.*

Compared to the corresponding statement in [HKSS24, Lemma 1.4], this result needs only $\deg_Z(Q) + 1$ directions, which is optimal by the example above, rather than a number of directions that grows with D. This comes at a cost, however: the field must be of size $\Omega(Dk)$ rather than $\Omega(D + k)$, and, as observed in Theorem 1.1, this large field size is unavoidable and the condition $q \geq \mathrm{poly}(\deg_Z(Q)) \cdot Dk$ cannot be weakened to $q = O(D + k)$.

Our proof of Theorem 1.2 does not directly use this lemma. Instead, both statements are proved from another, similar statement (see Lemma 2.1), which shows that consistent low-degree Z-roots on a family of parallel lines can be lifted to a global *rational* Z-root of Q. Lemma 1.3 follows from Lemma 2.1 by observing that if there are $\deg_Z(Q)+1$ sets of parallel lines, then there is a pair of directions such that the roots on the lines in these directions agree on a constant (depending on $\deg_Z(Q)$) fraction of points in $\mathbb{F}^2$. This agreement provides the necessary structure for us to apply Lemma 2.1 for lines in these two directions. This also allows us to conclude that the two rational roots obtained must in-fact be the same! We then use the standard Polischuk-Spielman lemma to conclude that these rational roots must be polynomials.

Given that our counterexamples only prove tightness of the above result when the characteristic is small (in particular when $\mathrm{char}(\mathbb{F}) \leq 1/\varepsilon$), it would be interesting to know whether the quantitative bounds in Theorem 1.2 and Lemma 1.3 can be improved over fields of sufficiently large characteristic.

Organization

In the next section, we provide an overview of our proofs. We set up the necessary notation and preliminaries in Section 3. We then prove Lemma 2.1 in Section 4. We use this lemma to complete the proof of Lemma 1.3 in Section 5 and the analysis of the derandomized low-degree test in Theorem 1.2 in Section 6. Finally, we prove Theorem 1.1 in Section 7.

AI use

All the technical content in the paper is due to its human authors. An AI assistant (Claude) was used to help write the introduction, and for typographical corrections and minor edits to the abstract and the proof overview.

2 Overview of the proofs

Our proofs of Theorem 1.2 and Lemma 1.3 follow the high-level outlines of similar results in [AS03] and [HKSS24]. However, the presence of lines in very few directions introduces some important technical challenges that the proof has to overcome. In this section, we discuss the high-level outline of the proofs of the main theorems.

Proof of Theorem 1.2: Let $f\colon \mathbb{F}^2 \to \mathbb{F}$ be a function that satisfies

$$\mathop{\mathbb{E}}_{\ell\in\mathscr{L}}[\mathrm{agree}(f|_\ell, \mathscr{P}_{k,1})] \geq \varepsilon\,,$$

where $\mathscr{L}$ refers to the set of all lines in r distinct directions. The proof starts by focusing on the set of lines in $\mathscr{L}$ and points in $\mathbb{F}^2$ that pass the test with probability $\Omega(\varepsilon)$. We call such points and lines *good* and focus on them for the analysis of the test. We show that there is a non-zero trivariate $Q(X,Y,Z)$ of *low* total degree and *constant* Z-degree such that for *all* good points $\mathbf{a}\in\mathbb{F}^2$, $Q(\mathbf{a}, f(\mathbf{a}))$ is zero. We also show that for all good lines ℓ, there is a univariate g_ℓ of degree k such that g_ℓ is a Z-root of the polynomial $Q((X,Y)_\ell, Z)$. By massaging Q to avoid some degenerate cases, we show that Q satisfies the hypothesis of a variant of a

generalization (Lemma 2.1) of the Polishchuk–Spielman lemma. We then rely on this lemma, together with bounds on the degree of Q to complete the proof of Theorem 1.2. The details can be found in Section 6.

We note that while the interpolation step is similar to that in [AS03, HKSS24], the details turn out to be substantially cleaner in the proof here. Instead of focussing on two good directions as is done in the earlier proofs, we start by sampling a small number of good lines ℓ and finding a non-zero low-degree Q such that $Q((X,Y)_\ell, g_\ell)$ is identically zero for these special lines. We then use the geometry of the space $\mathbb{F}^2$ to conclude that Q must satisfy a similar constraint for *all* good lines ℓ. A similar interpolation argument was also independently discovered in the recent work of Kominers, Thaler and Zheng [KTZ26] on an improved analysis of the (non-derandomized) line-point test.

The main technical highlight of this proof is a version of the Polishchuk–Spielman lemma in the high Z-degree setting. We now describe the lemma, the main ideas in its proof and the proof of Lemma 1.3 which improves on the corresponding lemma in [HKSS24] in the number of directions required: only one more than the Z-degree, which is the bare minimum.

Proof of Lemma 1.3: The following technical lemma is the key to both the proof of Theorem 1.2 and Lemma 1.3.

Lemma 2.1 (Lifting from consistent parallel lines)**.** *There is a constant $c > 0$ such that the following holds. Let $Q(X,Y,Z)$ be a non-zero trivariate polynomial of $(1,1,k)$-degree D. Let $\mathscr{L}$ be a set of parallel lines in $\mathbb{F}^2$ such that for every $L \in \mathscr{L}$, there exists a polynomial g_L of degree at most k that satisfies*

$$Q((X,Y)_L, g_L) \equiv 0.$$

Furthermore, let $\hat{L}$ be a line that is not parallel to the lines in $\mathscr{L}$, and let $\hat{h}$ be a degree k polynomial such that $Q((X,Y)_{\hat{L}}, \hat{h})$ is identically zero, $(\partial_Z Q)((X,Y)_{\hat{L}}, \hat{h})$ is non-zero, and for every $L \in \mathscr{L}$, $\hat{h}$ and g_L agree at the point $L \cap \hat{L}$.

If $|\mathscr{L}| > c \cdot (\deg_Z(Q) Dk)$, then there exists $U(X,Y) \in \mathbb{F}(X,Y)$ of total degree at most Dk such that

$$Q(X,Y,U(X,Y)) \equiv 0.$$

Moreover, for all but at most D choices of $L \in \mathscr{L}$, the restriction of U on L is well defined and equals g_L.

This lemma shows that consistent, low-degree Z-roots of $Q(X,Y,Z)$ on a set of parallel lines can be lifted to a common global rational root. Here, consistency of the roots on the parallel lines is asserted by their agreement with the Z-root on a separate anchor line $\hat{L}$ that intersects these parallel lines, and the fact that the multiplicity of the root on $\hat{L}$ is one. A similar lifting theorem, but from a non-degenerate point, is at the heart of the proof in [HKSS24]. We need to lift from an anchor line instead of an anchor point as in [HKSS24] as the number of lines passing through any point in the derandomized test is very small (in fact, $\ll k$). Lifting from an anchor point (α,β) involves division by $(\partial_Z Q)(\alpha,\beta,f(\alpha,\beta))$ and hence the only requirement is that this field element is non-zero. Lifting from an anchor line $\hat{L}$ involves division by the polynomial $(\partial_Z Q)((X,Y)_{\hat{L}}, \hat{h})$ and hence the requirement that this polynomial is non-zero. However, this causes several complications as we are dividing by a polynomial and not a field element. We need to ensure that the degrees of the numerator and denominator polynomials do not blow up and one has to carefully

count the degree growth. This is done using a corollary of a result of Furstenberg [Fur67, BKRRSS26] applied to Newton's iteration (see Theorem 3.16).

To prove the above lemma, we show that the root on the anchor line can be lifted via Newton iteration to obtain a global power series root. This power series root is then shown to be equal to the low-degree polynomial roots on (most of) the lines in $\mathscr{L}$ using the consistency of the anchor line with the lines in $\mathscr{L}$. We then work with an appropriate truncation of the power series root (which has rational coefficients) to show that if the number of lines in $\mathscr{L}$ is large enough, then this truncation gives us a rational global Z-root of Q. The details of the proof are discussed in Section 4.

To prove Lemma 1.3, we start by preprocessing Q to ensure some non-degeneracy properties (e.g. square-freeness and non-zero Z-derivative). We then use the fact that the Z-degree of Q is strictly smaller than the number of directions available to conclude that there is a pair of directions (among the r available directions), such that roots on many lines in these directions are consistent (i.e. their values on the intersection points agree) for at least $\Omega(q^2/\operatorname{poly}(\deg_Z(Q)))$ of the points in $\mathbb{F}^2$. For simplicity of notation, let us assume that the directions correspond to lines parallel to the X and Y-axes (i.e, horizontal and vertical lines). The high-level idea is to invoke Lemma 2.1 twice: once on a set of horizontal parallel lines with a vertical line as anchor, and once on a set of vertical parallel lines with a horizontal line as anchor. This gives us two global roots $U(X,Y), U'(X,Y)$ of $Q(X,Y,Z)$: $U(X,Y)$ lies in $\mathbb{F}(Y)[X]$ with X-degree at most k, and $U'(X,Y)$ lies in $\mathbb{F}(X)[Y]$ with Y-degree at most k. Moreover, these roots *explain* the given roots of Q on many horizontal lines and vertical lines respectively. Since we chose the two directions to be such that the given roots of Q on lines in these directions are often consistent, this implies that $U(X,Y)$ and $U'(X,Y)$ agree on many points. By the Schwartz-Zippel lemma, this means that the low-degree rational functions $U(X,Y)$ and $U'(X,Y)$ are identical, and in particular they lie in $\mathbb{F}(Y)[X] \cap \mathbb{F}(X)[Y] = \mathbb{F}[X,Y]$ and have degree at most k in both variables.

Filling in the details, e.g. handling degeneracy of Q, showing the existence of good anchors for the lifting outlined above and dealing with lines where the rational root does not equal the polynomial root on the line requires some care, and we discuss the details of the proof in Section 5.

Proof of Theorem 1.1 For the proof of Theorem 1.1, let us for the purpose of this overview restrict our attention to characteristic two fields (i.e., $p = 2$) and when $\varepsilon = 1/2$ (i.e., $r = 1$). In this case, we work over a field $\mathbb{F}_q$, where $q = 2^{2s}$. This field clearly contains the subfield $\mathbb{F}_{2^s}$ of size $\sqrt{q}$. We set the degree parameter k to $\sqrt{q}/2$. The lines considered for the line-point test in this construction are of the form $\ell_{a,b} = \{(t, at+b) : t \in \mathbb{F}_q\}$, where a is in $\mathbb{F}_{\sqrt{q}}$ and b is in $\mathbb{F}_q$. Thus, the set $\mathscr{L}$ of lines considered here has $q^{3/2}$ lines in it, q lines each in the $|\mathbb{F}_{2^s}| = \sqrt{q}$ directions. To construct the function $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$, we start by assigning univariate polynomials of degree k to each of the lines in $\mathscr{L}$. We show that over a uniformly random pair of lines chosen from $\mathscr{L}$, the line polynomials agree at the intersection of these lines with probability very close to half, and yet there is no degree $O(k)$ bivariate polynomial whose restriction to a constant fraction of the lines ℓ in $\mathscr{L}$ equals the line polynomial in ℓ. These properties are very closely built into the careful construction of the line polynomials, which are constructed using properties of the trace function (Tr) from $\mathbb{F}_q$ to $\mathbb{F}_2$. More precisely, the line polynomial associated to the line $\ell_{a,b}$ for $a \in \mathbb{F}_{\sqrt{q}}$ and

$b \in \mathbb{F}_q$, is the polynomial $\mathsf{HTr}(b^{\sqrt{q}}T)$, where the *half-trace* polynomial $\mathsf{HTr}(Z)$ is defined as

$$\mathsf{HTr}(Z) = Z + Z^2 + Z^4 + \cdots + Z^{2^{s-1}}.$$

Observe that HTr is the trace map $\mathsf{Tr}_{\mathbb{F}_{2^s}/\mathbb{F}_2}$ extended as a polynomial map to all of $\mathbb{F}_q = \mathbb{F}_{2^{2s}}$ and is related to Tr as $\mathsf{HTr}(z) + \mathsf{HTr}(z^{\sqrt{q}}) = \mathsf{Tr}(z)$ for every $z \in \mathbb{F}_q = \mathbb{F}_{2^{2s}}$.

On the way to the proof of Theorem 1.1, we also construct a polynomial $Q(X, Y, Z)$ defined as

$$Q(X, Y, Z) := Z^2 + Z + (XY^{\sqrt{q}} + YX^{\sqrt{q}}),$$

with Z-degree 2 and $(1, 1, k)$-degree $\sqrt{q}+1$. We show that on every line $\ell_{a,b} \in \mathscr{L}$, the polynomial $\mathsf{HTr}(b^{\sqrt{q}}T)$ is a Z-root of $Q((X, Y)_{\ell_{a,b}}, Z)$, and yet $Q(X, Y, Z)$ has no Z-root in the bivariate polynomial ring $\mathbb{F}[X, Y]$.

Note that we are considering lines in $\sqrt{q}$ directions here, and yet the Z-degree of Q is just 2! This is in stark contrast to the setting of Lemma 1.3, where over a field of sufficiently large (and yet quadratic) size, existence of low-degree polynomial Z-roots on all lines in any set of $(\deg_Z(Q) + 1)$ directions is sufficient to guarantee the existence of a low-degree polynomial Z-root globally.

This overview focuses on the case when $p = 2$ and $r = 1$ (and hence $\varepsilon = 1/2$). Our results work for all characteristics and all ε provided the characteristic is at most $1/\varepsilon$. We discuss the details of these constructions in Section 7.

3 Notations and preliminaries

3.1 Notations

- $\mathbb{F}$ denotes a (usually) finite field.
- The support of a polynomial is the set of non-zero monomials in it.
- $\mathbb{F}[X]_{<d}$ denotes the linear space of univariate polynomials of degree less than d with coefficients in $\mathbb{F}$, and can naturally be identified with the space $\mathbb{F}^d$.
- The $(1, 1, k)$-weighted degree (or simply the $(1, 1, k)$-degree) of a monomial $X^i Y^j Z^\ell$ is defined to be equal to $(i + j + k\ell)$. The $(1, 1, k)$-degree of a polynomial $Q(X, Y, Z)$ is defined to be the maximum of the $(1, 1, k)$-degrees of any monomial in the support of Q.
- The degree of a rational function $R(X)$ is defined to be equal to the maximum of the degrees of the numerator of R and the denominator of R.
- For $\ell \in \mathbb{N}$ and polynomial $Q(Y, Z) \in \mathbb{K}[Y, Z]$, the expression $[Z^\ell]\{Q(Y, Z)\}$ denotes the coefficient Z^ℓ in the polynomial $Q(Y, Z)$, when it is viewed as a univariate in Z with coefficients in $\mathbb{F}[Y]$.
- For a trivariate polynomial $Q(X, Y, Z)$ and a line $L \in \mathbb{F}^2$, the polynomial $Q((X, Y)_L, Z)$ denotes a bivariate polynomial obtained by restricting the variables (X, Y) to the line L. For instance, if the line L is parameterized as $(T, mT + c)$ for slope m and intercept c, $Q((X, Y)_L, Z)$ denotes the bivariate polynomial $Q(T, mT + c, Z)$.

- For a line L and a trivariate $Q(X, Y, Z)$, we say that Q has a Z-root of degree k on the line L if there is a polynomial $h(T)$ of degree at most k such that $Q(T, mT + c, h(T))$ is identically zero, where $L = \{(t, mt + c) : t \in \mathbb{F}\}$.

  We note that the existence of a degree k Z-root on a line L is independent of the precise parameterization of the line L and is a property of the polynomial Q. Thus, we often just say that a polynomial h is a Z-root of Q on the line L, indicated by $Q((X, Y)_L, h) \equiv 0$, without specifying the precise parameterization.

3.2 Preliminaries

Lemma 3.1 (Chernoff bound)**.** *Let $X_1, X_2, \ldots, X_n$ be independent random variables taking values in $\{0, 1\}$, let X denote their sum, and μ be the expected value of X. Then,*

$$\Pr\left[|X - \mu| \geq \delta\mu\right] \leq 2 \cdot \exp(-\delta^2\mu/3),$$

for every $\delta \in [0, 1]$.

Lemma 3.2 (Claims A.4, A.5, A.6 in [HKSS24])**.** *For all $p, k, D \in \mathbb{N}$ such that $D > 20k$ and $p \geq 2$.*

Then, the number of monomials $X^iY^jZ^\ell$ of $(1, 1, k)$-degree at most D is greater than $D^3/6k$, and the number of monomials $X^iY^jZ^\ell$ of $(1, 1, k)$-degree at most D, where ℓ is either zero or is not divisible by p is greater than $D^3/12k$.

Lemma 3.3 (Schwartz-Zippel lemma)**.** *Let $\mathbb{F}$ be any field and A be a subset of $\mathbb{F}$. If $P(\mathbf{x})$ is a non-zero polynomial on n variables with coefficients in $\mathbb{F}$, then the number of zeroes of P on the product set A^n is at most $(\deg(P) \cdot |A|^n)$.*

Lemma 3.4. *Let $\mathbb{F}$ be any field and $f(X, Y) \in \mathbb{F}[X, Y]$ be a non-zero polynomial of total degree at most D. Then, the number of lines L in $\mathbb{F}^2$ such that the restriction of $f(X, Y)$ on L is identically zero is at most D.*

Proof. Each distinct line on which f restricts to 0 gives a distinct linear factor of $f(X, Y)$. □

Definition 3.5. *Let $f \in \mathbb{F}[\mathbf{X}]$ be a polynomial that factorizes as $f = \prod_i f_i(\mathbf{X})^{e_i}$, for irreducible polynomials f_i such that $\gcd(f_i, f_j) = 1$ for $i \neq j$, and natural numbers $e_i \geq 1$. Then, the squarefree part of f is defined as $\prod_i f_i$.* ◊

3.3 Hasse derivatives

Definition 3.6. *The Hasse derivative of order t of a polynomial $f(X) \in \mathbb{F}[X]$, denoted by $\partial_{X^t}(f)$, is defined as the coefficient of Z^t in the polynomial $f(X + Z)$, when $f(X + Z)$ is viewed as a univariate in Z with coefficients in the ring $\mathbb{F}[X]$.* ◊

Lemma 3.7 (Properties of Hasse derivatives)**.** *Let $\mathbb{F}$ be a field of characteristic p. Then, the following properties hold.*

- *Let $f(X) \in \mathbb{F}[X]$ be a non-zero polynomial of degree at least one. The first order Hasse derivative of f is identically zero, if and only if there exists a polynomial $g(X) \in \mathbb{F}[X]$ such that $g(X^p) = f(X)$.*

- *For any two polynomials f, g, $\partial_X(fg) = g \cdot \partial_X(f) + f \cdot \partial_X(g)$. By induction, this implies that for every $n \in \mathbb{N}$, $\partial_X(f^n) = nf^{n-1}\partial_X(f)$.*

A consequence of the above lemma is the following corollary.

Corollary 3.8. *Let $\mathbb{F}$ be any field, $n \in \mathbb{N}$ be a natural number and $f, g \in \mathbb{F}[Z]$ be non-zero polynomials such that $f = g^n$.*

If n is not divisible by the characteristic of the field and $\partial_Z(f)$ is non-zero, then $\partial_Z(g)$ is non-zero.

Proof. This immediately follows from the fact that $\partial_Z(f) = ng^{n-1}\partial_Z(g)$ in Lemma 3.7. □

In the next lemma, we try to understand the following issue: we have a bivariate $f(X, Y) \in \mathbb{F}[X, Y]$ over a field of characteristic p that is *not* the pth power of a polynomial. The goal of the lemma is to understand the number of lines L such that the restriction of f on the line L is the pth power of a polynomial.

Lemma 3.9. *Let $\mathbb{F}$ be any field of characteristic p and $f(X, Y) \in \mathbb{F}[X, Y]$ be a non-zero polynomial of total degree at most D such that there* does not exist *a polynomial $g(X, Y) \in \mathbb{F}[X, Y]$ satisfying $f(X, Y) = g(X, Y)^p$.*

Then, there is at most one direction $\Delta \in \mathbb{F}^2$ such that for all directions $\Delta' \neq \Delta$, the following is true: the number of lines L in the direction Δ' for which the restriction of f on L is pth power of a polynomial is at most D.

Proof. Let $f = \sum_{i,j} f_{i,j} X^i Y^j$ for non-negative integers i, j such that $i + j \leq D$, and $f_{i,j} \in \mathbb{F}$. Since f is not the pth power of a polynomial, there exists an $f_{i,j}$ that is non-zero, such that p does not divide at least one of i and j. Thus, from Lemma 3.7, we get that at least one of the first order Hasse derivatives $\partial_X(f)$ or $\partial_Y(f)$ is not identically zero. Without loss of generality, we assume that $\partial_Y(f)$ is non-zero.

Lines parallel to Y-axis: Since $\partial_Y(f)$ is non-zero, there is at least one non-zero monomial f_{i_0,j_0} in f such that p does not divide j_0. Let $f_{j_0}(X)$ be the coefficient of Y^{j_0} in f, when it is viewed as a univariate in Y with coefficients in $\mathbb{F}[X]$. Clearly, for an $a \in \mathbb{F}$, $f(a, Y)$ is the pth power of a univariate in $\mathbb{F}[Y]$ only if $f_{j_0}(a)$ is zero. But there are at most $\deg_X(f) \leq D$ many such a.

Lines of the form $(Y = mX + c)$ for $m \in \mathbb{F}$: Since $\partial_Y(f)$ is non-zero, there is at most one $m_0 \in \mathbb{F}$ such that the polynomial $\partial_X(f)(X, Y) + m_0\partial_Y(f)(X, Y)$ is identically zero. We now argue that for every $m \neq m_0$, the set of lines L of slope m such that the restriction f_L is a pth power has size at most D.

From Lemma 3.7 and the definition of Hasse derivatives, we get that

$$\partial_X(f(X, mX + c)) = \partial_X(f)(X, mX + c) + m\partial_Y(f)(X, mX + c)\,.$$

Furthermore, for $f_L = f(X, mX + c)$ to be a pth power, it must be the case that the Hasse derivative $\partial_X(f(X, mX + c))$ is identically zero, or in other words, c is a zero of the polynomial $\partial_X(f)(X, mX + Z) + m\partial_Y(f)(X, mX + Z) \in (\mathbb{F}[X])[Z]$. But this polynomial has Z-degree at most D, and is non-zero; indeed $m \neq m_0$ ensures that $\partial_X(f)(X, Z) + m\partial_Y(f)(X, Z)$ is non-zero, and shifting Z to $Z + mX$ retains this non-zeroness. Thus, there at most D choices of c for which f_L is a pth power. □

3.4 Resultant and discriminant

Definition 3.10 (Sylvester Matrix, Resultant and Discriminant)**.** *The Sylvester matrix of two univariates $f(X), g(X)$ over a field $\mathbb{F}$ of degree $d_1 \geq 1, d_2 \geq 1$ is a $(d_1 + d_2) \times (d_1 + d_2)$ matrix corresponding to the linear transformation*

$$\Gamma_{f,g} : \mathbb{F}^{d_2} \times \mathbb{F}^{d_1} \to \mathbb{F}^{d_1+d_2},$$

defined as

$$\Gamma_{f,g}(A, B) = Af + Bg\,,$$

where $A, B \in \mathbb{F}[X]$ are polynomials of degree at most $d_2 - 1$ and $d_1 - 1$ respectively.

The determinant of the Sylvester matrix of f, g is referred to as the Resultant of f, g and is denoted by $\mathsf{Res}(f, g)$. The resultant of f and its first order Hasse derivative $f^{(1)}$ is referred to as the Discriminant of f and is denoted by $\mathsf{Disc}(f)$. ◊

The utility of the resultant and discriminant stem from the following fundamental facts.

Theorem 3.11. *For every field $\mathbb{F}$ and polynomials $f, g \in \mathbb{F}[X]$ of degree at least one, the $\mathsf{Res}(f, g)$ is non-zero if and only if f, g have* gcd 1.

Corollary 3.12. *Let $\mathbb{F}$ be a finite field or a field of characteristic zero and $f \in \mathbb{F}[X]$ be a polynomial of degree at least two. Then, f is squarefree if and only if $\mathsf{Disc}(f)$ is non-zero.*

In the course of our proofs, we would also have to work with multivariates that we view as univariates in one of the variables with coefficients in the field of rational functions. For such fields, we have the following weaker variant of Corollary 3.12.

Corollary 3.13. *Let $\mathbb{F}$ be any field and $f \in \mathbb{F}[X]$ be a polynomial of degree at least two such that the Hasse derivative $\partial(f)$ is non-zero and has degree at least one. Then, f is squarefree if and only if $\mathsf{Disc}(f)$ is non-zero.*

On many occasions in this paper, we work with polynomials with larger number of variables and view them as univariates with respect to one of the variables and coefficients coming from the field of rational functions in the other variables. In such settings, we use $\mathsf{Res}_Z(f, g)$ and $\mathsf{Disc}_Z(f)$ to denote the resultant and discriminants respectively, with the subscript indicating that we are viewing the multivariates as univariates in Z.

Another simple, but useful structural property of the resultant (and discriminant) for multivariate polynomials that we rely on is the following.

Observation 3.14. *Let $f(X, Y, Z), g(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ be trivariates with Z-degree at least one, and let $\mathbf{a} \in \mathbb{F}^2$ be such that $\deg_Z(f(X, Y, Z)) = \deg_Z(f(\mathbf{a}, Z))$ and $\deg_Z(g(X, Y, Z)) = \deg_Z(g(\mathbf{a}, Z))$.*

Then, $\mathsf{Res}_Z(f(X, Y, Z), g(X, Y, Z)) \in \mathbb{F}[X, Y]$ when evaluated at $\mathbf{a}$ equals the $\mathsf{Res}_Z(f(\mathbf{a}, Z), g(\mathbf{a}, Z))$.

Proof. The proof follows from the fact that the Z-degree preserving property of $\mathbf{a}$ ensures that the Sylvester matrix of $f(X, Y, Z), g(X, Y, Z)$ (while viewing these as a univariate in Z) when evaluated at $\mathbf{a}$ equals the Sylvester matrix of $f(\mathbf{a}, Z), g(\mathbf{a}, Z)$. □

3.5 Power series roots

Theorem 3.15 (Newton iteration)**.** *Let $\mathbb{F}$ be any field and $\mathbb{K}$ be any extension of $\mathbb{F}$, and let $P(Y,Z) \in \mathbb{F}[Y,Z]$ be a bivariate polynomial with coefficients in $\mathbb{F}$. Let $a \in \mathbb{K}$ be such that $P(0,a) = 0$ and $\partial_Z(P)(0,a) \neq 0$. Let $\Phi_0 := a$, and for every $k \geq 1$, $\Phi_k(Y) \in \mathbb{K}[Y]$ be defined as*

$$\Phi_k(Y) := \left(\Phi_{k-1}(Y) - \frac{P(Y, \Phi_{k-1}(Y))}{\partial_Z(P)(0,a)}\right) \bmod Y^{k+1}.$$

Then, for every $k \geq 1$, $\Phi_k(Y)$ is the unique *polynomial that satisfies the following conditions.*

$$\begin{aligned} &P(Y, \Phi_k(Y)) \equiv 0 \bmod Y^{k+1}, \\ &\Phi(Y) \equiv a \bmod Y, \qquad \textit{and} \\ &\deg(\Phi_k(Y)) \leq k. \end{aligned}$$

The following theorem gives an explicit non-iterative expression for the approximate root $\Phi_k(Y)$ defined above. This is a corollary of a theorem of Furstenberg [Fur67] and the precise expression here is implicit in Corollary 3.3 and Theorem 4.1 in [BKRRSS26].

Theorem 3.16 (Explicit Newton iteration [Fur67, BKRRSS26])**.** *Let $\mathbb{F}$ be any field and $\mathbb{K}$ be any extension of $\mathbb{F}$, and let $P(Y,Z) \in \mathbb{F}[Y,Z]$ be a bivariate polynomial with coefficients in $\mathbb{F}$. Let $a \in \mathbb{K}$ be such that $P(0,a) = 0$ and $\partial_Z(P)(0,a) \neq 0$. Let $\Phi_0 := a$, and for every $k \geq 1$, $\Phi_k(Y) \in \mathbb{K}[Y]$ be defined as*

$$\Phi_k(Y) := \left(\Phi_{k-1}(Y) - \frac{P(Y, \Phi_{k-1}(Y))}{\partial_Z(P)(0,a)}\right) \bmod Y^{k+1}.$$

Then, $\Phi_k(Y)$ equals the polynomial

$$\left(\sum_{m=1}^{2k} \frac{1}{\alpha^{m+1}} [Z^{m-1}]\{\partial_Z(P(Y, Z+a))\dot{(}\alpha Z - P(Y, Z+a))^m\}\right) \bmod Y^{k+1},$$

where α equals $\partial_Z(P)(0,a)$.

3.6 The Polishchuk–Spielman lemma

Lemma 3.17 ([PS94])**.** *Let $\mathbb{F}$ be any field and $A(X,Y), B(X,Y) \in \mathbb{F}[X,Y]$ be polynomials with X,Y-degrees at most D. Let there be n-values $x \in \mathbb{F}$ such that $A(x,Y)$ divides $B(x,Y)$ in the ring $\mathbb{F}[Y]$ and the quotient $C_x(Y)$ has degree at most k, and let there be n-values $y \in \mathbb{F}$ such that $A(X,y)$ divides $B(X,y)$ in the ring $\mathbb{F}[X]$ and the quotient $R_y(X)$ has degree at most k.*

There exists constants $c, c' > 0$ with $c > c'$ such that if $n > cD$, then there is a bivariate $Q(X,Y)$ of degree at most k in each variable such that

$$B(X,Y) = Q(X,Y) \cdot A(X,Y).$$

Furthermore, for all but $c'D$ choices of the substitutions x, y, $Q(x,Y) = C_x(Y)$ and $Q(X,y) = R_y(X)$.

3.7 Pruning to subgraph of high min degree

Lemma 3.18. *Let $G = (U, V, E)$ be a bipartite graph, such that the maximum degree of a vertex $u \in U$ is at most ℓ, the maximum degree of a vertex $v \in V$ is at most r. Let ε, δ be parameters such that the average degree of a vertex in U is $\varepsilon\ell$ and the average degree of a vertex in V is δr.*

Then, there exists a subgraph $G' = (U', V', E')$ of the graph G such that

- $|U'| \geq \frac{4\varepsilon}{5}|U|$, $|V'| \geq \frac{4\delta}{5}|V|$.
- *The degree of every vertex in U' in the graph G' is at least $\varepsilon\ell/10$ and the degree of every vertex in R' in the graph G' is at least $\delta r/10$.*

Proof. To prove the lemma, we iteratively start deleting low-degree vertices from the graph G as long as there is such a vertex. We argue that this procedure stops at some point, and when it stops, the remaining graph has the desired properties.

Algorithm Prune

- Set flag ϕ to 1.
- If $\deg(u) \geq \frac{\varepsilon\ell}{10}$ for every $u \in U$, $\deg(v) \geq \frac{\delta r}{10}$ for every $v \in V$, set ϕ to 0 and stop.
- While ϕ is 1:
  1. For $u \in U$:
     - if $\deg(u) < \frac{\varepsilon\ell}{10}$, delete u and update $U \leftarrow U \setminus \{u\}$.
  2. For $v \in V$:
     - if $\deg(v) < \frac{\delta r}{10}$, delete v and update $V \leftarrow V \setminus \{v\}$.
  3. If $\deg(u) \geq \frac{\varepsilon\ell}{10}$ for every $u \in U$, $\deg(v) \geq \frac{\delta r}{10}$ for every $v \in V$, set ϕ to 0 and stop.

Here, by the degree of a vertex, we mean the degree in the subgraph of G alive at that moment, after any deletions that might have occurred in the algorithm.

If ϕ equals one at the beginning of the *While* loop, then at least one vertex is deleted from the graph in that run of the loop, and hence this process will terminate in finitely many steps. Note that at any step of the algorithm, a vertex in U is deleted if its degree in the current graph is less than $\frac{\varepsilon\ell}{10}$, and hence its deletion results in the deletion of at most $\frac{\varepsilon\ell}{10}$ edges from the graph. Similarly, the deletion of any right vertex in the second for loop results in the deletion of at most $\frac{\delta r}{10}$ edges from the graph.

Thus, the maximum number of edges that could have been deleted during the run of the algorithm is at most $\left(|U| \cdot \frac{\varepsilon\ell}{10} + |V| \cdot \frac{\delta r}{10}\right)$, which is at most $\left(\frac{|E|}{5}\right)$, since $\varepsilon\ell|U| = \delta r|V| = |E|$. So at least $\left(\frac{4|E|}{5}\right)$ edges must have survived the pruning process.

Hence, the graph G' obtained at the end of the process is non-empty. Clearly, the minimum degree condition on the vertices will be satisfied at this point. The lower bound on the number of surviving left and right vertices now follows from the number of surviving edges and the bounds on the maximum degrees.

□

4 Consistent roots on parallel lines to global rational roots

In this section, we state and prove the following technical lemma that is crucial for the proof of the generalization of the Polishchuk–Spielman lemma in Lemma 1.3 as well as to the proof of Theorem 1.2.

Lemma 2.1 (Lifting from consistent parallel lines)**.** *There is a constant $c > 0$ such that the following holds. Let $Q(X, Y, Z)$ be a non-zero trivariate polynomial of $(1, 1, k)$-degree D. Let $\mathscr{L}$ be a set of parallel lines in $\mathbb{F}^2$ such that for every $L \in \mathscr{L}$, there exists a polynomial g_L of degree at most k that satisfies*

$$Q((X, Y)_L, g_L) \equiv 0.$$

Furthermore, let $\hat{L}$ be a line that is not parallel to the lines in $\mathscr{L}$, and let $\hat{h}$ be a degree k polynomial such that $Q((X, Y)_{\hat{L}}, \hat{h})$ is identically zero, $(\partial_Z Q)((X, Y)_{\hat{L}}, \hat{h})$ is non-zero, and for every $L \in \mathscr{L}$, $\hat{h}$ and g_L agree at the point $L \cap \hat{L}$.

If $|\mathscr{L}| > c \cdot (\deg_Z(Q)Dk)$, then there exists $U(X, Y) \in \mathbb{F}(X, Y)$ of total degree at most Dk such that

$$Q(X, Y, U(X, Y)) \equiv 0.$$

Moreover, for all but at most D choices of $L \in \mathscr{L}$, the restriction of U on L is well defined and equals g_L.

For the proof of the lemma, we first do an affine change of basis and reduce to the setting where the lines in $\mathscr{L}$ are parallel to the Y-axis and the line $\hat{L}$ is the X-axis. This helps simplify the notation in the proof while conveying most of the main technical ideas.

4.1 The case of axis parallel lines

Lemma 4.1. *Let $Q(X, Y, Z)$ be a non-zero trivariate polynomial of $(1, 1, k)$-degree D. Let $S \subseteq \mathbb{F}$ be a set of field elements such that for every $a \in S$, there exists a polynomial $g_a(Y)$ of degree at most k that satisfies*

$$Q(a, Y, g_a(Y)) \equiv 0.$$

Furthermore, let $h(X)$ be a degree k polynomial such that $Q(X, 0, h(X))$ is identically zero, $\partial_Z(Q(X, 0, h(X)))$ is non-zero, and for every $a \in S$, $h(a) = g_a(0)$.

If $(|S| > 2D + d_Z(Q)D(2k + 1))$, then there exists $U(X, Y) \in \mathbb{F}(X)[Y]$ such that $\deg_Y(U) \leq k$, $\deg_X(U) \leq Dk$ and

$$Q(X, Y, U(X, Y)) \equiv 0.$$

Moreover, for all but at most D choices of $a \in S$, $U(a, Y) = g_a(Y)$.

Proof. From the bound on the weighted degree of Q, we have that the degree of $\partial_Z(Q(X, 0, h(X)))$ is also at most D. Moreover, since $\partial_Z(Q(X, 0, h(X)))$ is a non-zero polynomial of degree at most D, it can have no more than D zeroes in the set $S \subseteq \mathbb{F}$. Let $\hat{S}$ be the subset of S defined as

$$\hat{S} = \{a : a \in S \text{ and } \partial_Z(Q(a, 0, h(a))) \neq 0\}.$$

Thus, we have that

$$|\hat{S}| \geq |S| - D.$$

We now view Q as a bivariate in Y, Z, with coefficients over the field $\mathbb{F}(X)$. From the hypothesis of the lemma, we have that

$$Q(X, Y, h(X)) = 0 \bmod Y, \quad \text{and}$$
$$\partial_Z(Q(X, Y, h(X))) \neq 0 \bmod Y.$$

Thus, from Theorem 3.15, we have that there is a unique power series $\Phi(X, Y)$ in Y, with coefficients from the field $\mathbb{F}(X)$ such that

$$Q(X, Y, \Phi(X, Y)) \equiv 0 \quad \text{and}$$
$$\Phi(X, Y) \equiv h(X) \bmod Y.$$

Let $U(X, Y)$ be defined as the truncation of $\Phi(X, Y)$ modulo Y^{k+1}. Thus, $U(X, Y)$ is a univariate in Y of degree k with coefficients in the field $\mathbb{F}(X)$ of rational functions in X, and is the unique such element that satisfies

$$Q(X, Y, U(X, Y)) \equiv 0 \bmod Y^{k+1} \quad \text{and}$$
$$U(X, Y) \equiv h(X) \bmod Y.$$

To complete the proof of the lemma, we need the following two claims. We first complete the proof of the lemma using the claims and then discuss the proofs of the claims.

Claim 4.2. *For every $a \in \hat{S}$, the denominator of $U(a, Y)$ is non-zero and $U(a, Y) = g_a(Y)$. In particular,*

$$Q(a, Y, U(a, Y)) \equiv 0.$$

Claim 4.3. $\deg_X(U) \leq D(2k + 1)$.

To prove the theorem, we consider the formal rational function $R(X, Y) := Q(X, Y, U(X, Y))$. Clearly, R is a polynomial in Y and a rational function in X. Moreover, R can be written as

$$R = \sum_{i=0}^{d_Z(Q)} Q_i(X, Y) U(X, Y)^i,$$

where each Q_i is a polynomial of total degree at most D (in fact, at most $(D - d_z k)$). Thus, $\deg_X(R)$ is at most $D' := (D + d_z \cdot \deg_X(U))$. In particular, let us focus on the numerator of the R, whose degree is at most D'. From Claim 4.2, we have that for every $a \in \hat{S}$, $R(a, Y)$ is well defined (its denominator does not vanish), and its numerator evaluates to zero. Thus, if

$$|\hat{S}| > D',$$

we get that $R(X,Y)$ is identically zero, and $U(X,Y)$ is a Z-root of Q. Moreover, from Claim 4.2, we get that for every $a \in \hat{S}$, $U(a,Y)$ equals $g_a(Y)$.

But the inequality needed on the size of $\hat{S}$ immediately follows from $|\hat{S}| \geq (|S| - D)$, the upper bound on $\deg_X(U)$ in Claim 4.3. □

Proof of technical claims

Proof of Claim 4.2. From Theorem 3.16, we have that the denominator of $U(X,Y) \in \mathbb{F}(X)[Y]$ is a power of $\partial_Z(Q(X,0,h(X)))$. Thus, from the definition of $\hat{S}$, we get that for every $a \in \hat{S}$, this denominator is non-zero.

Since $Q(X,Y,U(X,Y))$ is zero modulo Y^{k+1}, we get that for every $a \in \hat{S}$, $U(a,Y)$ is well defined, and

$$Q(a,Y,U(a,Y)) \equiv 0 \bmod Y^{k+1}.$$

Moreover, the degree of $U(a,Y)$ is at most $(k+1)$ and the constant term $U(a,0)$ of $U(a,Y)$ equals $h(a)$. From the hypothesis of the lemma, this equals $g_a(0)$.

Thus, $U(a,Y)$ and $g_a(Y)$ are both degree k polynomials in Y that are the *lifts* of the root $h(a)$ of $Q(a,0,Z)$, which additionally satisfies $\partial_Z(Q)(a,0,h(a)) \neq 0$. By the uniqueness part of Theorem 3.15, we get that $U(a,Y)$ must equal $g_a(Y)$, and thus, $Q(a,Y,U(a,Y))$ must be identically zero. □

Proof of Claim 4.3. The claim immediately follows from the expression for approximate Z-roots of the bivariate $Q(X,Y,Z) \in \mathbb{F}(X)[Y,Z]$ in Theorem 3.16, when invoked with initial conditions $Q(X,0,h(X))$ is zero and $\partial_Z(Q(X,0,h(X)))$ is non-zero.

□

4.2 From axis parallel to the general case

We now complete the proof of Lemma 2.1.

Proof of Lemma 2.1. For the ease of notation, we assume that neither the line L nor the lines in $\mathscr{L}$ are parallel to the Y-axis. The argument below can be easily extended to this case by a different parameterization of the lines.

Let L_0 be the line $L_0 := \{(x, mx) : x \in \mathbb{F}\}$ with slope $m \in \mathbb{F}$ that is parallel to the lines in $\mathscr{L}$. Similarly, let $\hat{L}$ be the line $\hat{L} := \{(x, \hat{m}x + \hat{u}) : x \in \mathbb{F}\}$ for some $\hat{m}, \hat{u}$ in $\mathbb{F}$. We also know that $\hat{m} \neq m$. Let V, W be new formal variables and let us consider the system of linear constraints

$$Y - mX = V \tag{4.4}$$

$$Y - \hat{m}X = W + \hat{u}\,. \tag{4.5}$$

Since $m \neq \hat{m}$, this system has a unique solution and gives us a way to write X and Y as affine linear combinations of V, W, namely $X = \frac{(V-W-\hat{u})}{(\hat{m}-m)}$ and $Y = \frac{(\hat{m}V - m(W+\hat{u}))}{(\hat{m}-m)}$.

Let $P(V,W,Z) \in \mathbb{F}[V,W,Z]$ be a trivariate polynomial defined as

$$P(V,W,Z) := Q\left(\frac{(V-W-\hat{u})}{(\hat{m}-m)}, \frac{(\hat{m}V - m(W+\hat{u}))}{(\hat{m}-m)}, Z\right).$$

Clearly, $P(Y - mX, Y - \hat{m}X - \hat{u}, Z)$ equals $Q(X, Y, Z)$.

Now, for any line L that is parallel to L_0, parameterized as $L := \{(x, mx + u) : x \in \mathbb{F}\}$ and polynomial $g_L(X)$,

$$Q(X, mX + u, g_L(X)) = P(u, X(m - \hat{m}) + (u - \hat{u}), g_L(X)).$$

Furthermore, by setting $W := (m - \hat{m})X + (u - \hat{u})$, we get a polynomial $\tilde{g}_L$ with degree at most the degree of g_L such that if $Q(X, mX + u, g_L(X))$ is identically zero, then $P(u, W, \tilde{g}_L(W))$ is also identically zero.

Similarly, the degree-k Z-root $\hat{h}$ of $Q((X, Y)_{\hat{L}}, Z)$ implies that $P(V, 0, \tilde{h}(V))$ is identically zero for a polynomial $\tilde{h}$ of degree at most k.

Thus, the polynomial P satisfies the hypothesis of Lemma 4.1. From the conclusion of the lemma, we get a rational function $U(V, W) \in \mathbb{F}(V, W)$ with numerator and denominators of degree at most Dk such that U is a Z-root of P. Now, writing V, W as linear combinations of X, Y as in equation Equation 4.4, we get a rational function $\tilde{U}(X, Y)$ of degree at most Dk that is a Z-root of Q. Note that this transformation between X, Y and V, W is invertible, so the non-zero denominator of U cannot vanish under this transformation.

The moreover part also follows immediately from the basis change and the guarantees on the restrictions of U in Lemma 4.1. □

5 Generalizations of the Polishchuk–Spielman lemma

We now state and prove the generalization of Lemma 3.17 that drives the analysis of our low-degree test.

Theorem 5.1. *There exists a constant $c > 1$ such that for all $D, k, q, p, r \in \mathbb{N}$ where q is a prime power, $\mathbb{F}$ is the finite field of size q and $Q(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ is a polynomial with $(1, 1, k)$-degree D the following is true.*

Let $\mathscr{L}_1, \ldots, \mathscr{L}_r$ be subsets of lines in $\mathbb{F}^2$ such that for every $i \in [r]$, $\mathscr{L}_i$ is the set of all q parallel lines in a certain direction, the lines in $\mathscr{L}_i$ and $\mathscr{L}_j$ are intersecting for $i \neq j$. Furthermore, for every $i \in [r]$ and line $L \in \mathscr{L}_i$, there is a polynomial g_L of degree at most k that is a Z-root of $Q((X, Y)_L, Z)$.

If $r > d_Z(Q)$, and $q > c \operatorname{poly}(\deg_Z(Q))Dk$, then there is a bivariate polynomial $P(X, Y)$ of total degree at most $2k$ so that $Q(X, Y, P(X, Y))$ is identically zero and there are distinct indices $i_0, j_0 \in [r]$ such that the restriction of P on any line L equals g_L for all but $O(Dk)$ choices of lines L in $\mathscr{L}_{i_0} \cup \mathscr{L}_{j_0}$.

In the rest of this section, we prove this theorem.

Proof of Theorem 5.1

The rest of this section is devoted to the proof of Theorem 5.1. The proof is in divided into various stages. We first start by preprocessing Q in a way that ensures additional structure on the problem instance without loss of generality. We then zero-in on two of the r-directions that are *good* in some formal sense. Using the lines in these two directions, we conclude that Q must have a Z-root that is a rational function in X, Y. This is the step that involves the use of the generalization of the Polishchuk–Spielman lemma in Lemma 2.1. Finally, we conclude that the root obtained in the previous step is not just a rational function; it is a polynomial of the appropriate degree, and concludes the proof of Theorem 5.1.

5.1 Preprocessing

We start with the preprocessing step here.

The square-free part

Let $Q_1(X, Y, Z)$ be the square-free part of Q (Definition 3.5). Then, clearly, Q_1 also satisfies the hypothesis of the theorem. Furthermore, if the conclusion is true for Q_1, then it is also true for Q. So, we work with Q_1 henceforth.

Z-degree at least one

The hypothesis of the theorem may be true on some of the lines L because $Q_1((X, Y)_L, Z)$ is identically zero. From Lemma 3.4, we know that the total number of such lines is at most the total degree of Q_1, which is at most D. In fact, a stronger conclusion is true here: for all but at most D lines L, the Z-degree of $Q_1((X, Y)_L, Z)$ equals the Z-degree of Q_1. We discard the $O(D)$ *bad lines* (note that the number of lines q in each direction is large enough compared to D for us to be able to tolerate this loss), and for the rest of the proof assume that $Q_1((X, Y)_L, Z)$ is non-zero and equals the Z-degree of $Q_1(X, Y, Z)$ for all lines L under consideration. In particular, this ensures that the Z-degree of Q_1 is at least one for the hypothesis to hold.

Furthermore, we will assume without loss of generality that for at least one of the line polynomials g_L, the degree equals k, else we can replace k everywhere by $(k-1)$. This also implies that $k \leq D$, since otherwise a degree k polynomial $(Z - g_L)$ cannot be a factor of the polynomial $Q_1((X, Y)_L, Z)$ of total degree at most D.

Ensuring a non-zero Z-derivative

This step of pre-processing can be skipped if the underlying field $\mathbb{F}$ has characteristic either zero or larger than the Z-degree of Q_1, since over such fields $\deg_Z(Q_1) \geq 1$ implies that $\partial_Z(Q_1)$ is a non-zero polynomial. Some of the details are simpler in this setting, and we encourage the reader to read the proof with this setting in mind for the first time.

Over fields $\mathbb{F}$ of small positive characteristic, it may be the case that $\deg_Z(Q_1) \geq 1$ and yet $\partial_Z(Q_1)$ is identically zero. From Lemma 3.7, we know that this happens if and only if Q_1 is a polynomial in Z^p for some $s \geq 1$. Let $s \in \mathbb{N}$ be such that Q_1 is a polynomial in Z^{p^s} and not in $Z^{p^{s+1}}$. From Lemma 3.7, we get that there exists a polynomial $\hat{Q}(X, Y, Z)$ and a natural number $s \geq 1$ such that $\partial_Z(\hat{Q})$ is non-zero, and $Q_1(X, Y, Z) = \hat{Q}(X, Y, Z^{p^s})$. For the next few steps of the proof, we work with $\hat{Q}$. We eventually return to Q_1 towards the end.

To proceed further, we first discuss the properties of $\hat{Q}$ that follow from the properties of Q_1. Since the $(1, 1, k)$-degree of Q_1 is at most D, we get that the $(1, 1, p^s k)$-degree of $\hat{Q}$ is at most D. Furthermore, for any line $L \in \mathbb{F}^2$, if g_L is a degree k polynomial such that $Q_1((X, Y)_L, g_L)$ is identically zero, then we get

$$Q_1((X, Y)_L, g_L) = \hat{Q}((X, Y)_L, g_L^{p^s}) \equiv 0\,.$$

Thus, ${g_L}^{p^s}$ is a Z-root of $\hat{Q}((X, Y)_L, Z)$ for any line L where g_L is the Z-root of $Q_1((X, Y)_L, Z)$. So, the

property of having Z-roots on lines is preserved, although the degree of each of the Z-roots on lines is now bounded above by $p^s k$. We also record the following simple observation that follows from the definitions so far.

Observation 5.2. *$\hat{Q}$ is square-free, $\partial_Z(\hat{Q})$ is non-zero. If line L is such that*

$$\deg_Z(Q_1(X,Y,Z)) = \deg_Z(Q_1((X,Y)_L, Z)),$$

then,

$$\deg_Z(\hat{Q}(X,Y,Z)) = \deg_Z(\hat{Q}((X,Y)_L, Z)).$$

Going forward, we work with $\hat{Q}$, whose $(1,1,kp^s)$-degree is at most D, and has Z-roots of degree at most $\hat{k} = kp^s$ on many lines. Furthermore, each of these roots is the p^s-th power of a polynomial of degree at most k.

5.2 Finding two good directions

In this phase, we use the fact that the number of directions r is strictly greater than the $d_Z := \deg_Z(Q) \geq \deg_Z(\hat{Q})$ (and hence $\deg_Z(\hat{Q})$) to conclude that there is a pair of directions $i, j \in [r]$ such that the line polynomials for lines in $\mathscr{L}_i$ and $\mathscr{L}_j$ have non-trivial consistency. This is formalized in the following lemma.

Lemma 5.3. *There exist $i_0, j_0 \in [r]$ such that $i_0 \neq j_0$ and there is a set $\mathcal{P}$ of points in $\mathbb{F}^2$ of size at least $\Omega(q^2/d_Z^2)$ such that for every point $\mathbf{a} \in \mathcal{P}$ and lines $L \in \mathscr{L}_{i_0}$ and $L' \in \mathscr{L}_{j_0}$ incident on $\mathbf{a}$, the corresponding* line polynomials *g_L and $g_{L'}$ agree on $\mathbf{a}$.*

Proof. Let $\mathbf{a} \in \mathbb{F}^2$ be any point and let $L_1, L_2, \ldots, L_r$ be the lines incident on a such that $L_i \in \mathscr{L}_i$. Let g_{L_i} be the corresponding line polynomials such that $\hat{Q}((X,Y)_{L_i}, g_{L_i})$ is identically zero. Since each of the lines L_i is incident to $\mathbf{a}$, we get that $\hat{Q}(\mathbf{a}, g_{L_i}(\mathbf{a}))$ equals zero, or equivalently, $g_{L_i}(\mathbf{a})$ is a zero of the univariate $\hat{Q}(\mathbf{a}, Z)$. But $\hat{Q}(\mathbf{a}, Z)$ has degree at most d_Z, and $r > d_Z$ so there is a subset of size at least $\lceil r/d_Z \rceil \geq 2$ of these lines such that the corresponding line polynomials agree on $\mathbf{a}$.

Thus, by Pigeonhole principle, there is a pair of directions $i_0, j_0 \in [r]$ such that the line polynomials in these directions agree on at least $\frac{\binom{\lceil r/d_Z \rceil}{2}}{\binom{r}{2}}$ fraction of all points $\mathbf{a}$. For $r > \deg_Z(Q) \geq 1$, this fraction is at least $\frac{1}{2d_Z^2}$.

Finally, we note that we can only do the above arguments on points in $\mathbb{F}^2$ that have a line from each of the r sets $\mathscr{L}_1, \ldots, \mathscr{L}_r$ incident on it. In particular, we need to exclude all points in $\mathbb{F}^2$ that may be incident to any of the $O(D)$ bad lines excluded in Section 5.1. Thus, the size of the set $\mathcal{P}$ of points where lines in $\mathscr{L}_{i_0}, \mathscr{L}_{j_0}$ are consistent with each other is at least $\frac{q(q-O(Dd_Z^2))}{2d_Z^2}$, which, for $D < q/(cd_Z^2)$ (for a sufficiently large constant c) is $\Omega(q^2/d_Z^2)$. □

5.3 Rational roots from $\mathscr{L}_{i_0}$ and $\mathscr{L}_{j_0}$

For brevity of notation, we assume that $i_0 = 1$ and $j_0 = 2$. From Lemma 5.3, we know that line polynomials on lines in $\mathscr{L}_1$ and $\mathscr{L}_2$ are consistent on at least $\alpha q^2/d_Z^2$ points in $\mathbb{F}^2$ for some absolute constant $\alpha > 0$. Let

G be a bipartite graph with vertices $\mathscr{L}_1, \mathscr{L}_2$ with there being an edge between lines $L \in \mathscr{L}_1, L' \in \mathscr{L}_2$ if the corresponding line polynomials g_L and $g_{L'}$ are consistent, i.e. they agree on the point $L \cap L'$. Clearly, both sets of vertices in the bipartition have size at most q, the maximum degree of any vertex is q and there are at least $\alpha q^2/d_Z^2$ edges in the graph.

From Lemma 3.18, we get that there is a subgraph G' of G with vertex sets $\mathscr{H}_1 \subseteq \mathscr{L}_1$ and $\mathscr{H}_2 \subseteq \mathscr{L}_2$ of size at least $\frac{4\alpha}{5} q/d_Z^2$ each and minimum degree at least $\frac{\alpha}{10} q/d_Z^2$.

We focus on lines in this subgraph G' now, and refer to the lines in $\mathscr{H}_1, \mathscr{H}_2$ as *heavy* lines.

Setting up an anchor

We now prove the following crucial technical claim.

Claim 5.4. *For all but $O(d_Z D)$ lines L in $\mathscr{H}_1 \cup \mathscr{H}_2$, $\partial_Z(\hat{Q}((X,Y)_L, g_L))$ is non-zero.*

Proof. Recall that $\hat{Q}$ has the property that $\partial_Z(\hat{Q})$ is a non-zero polynomial. Furthermore, $\hat{Q}$ is square-free. We know from Lemma 3.4 that there are at most $\deg(\partial_Z(\hat{Q})) \leq D$ lines L in total such that $\deg(\partial_Z(\hat{Q})((X,Y)_L, Z))$ is strictly smaller than $\deg(\partial_Z(\hat{Q})(X,Y,Z)$ or $\partial_Z(\hat{Q})((X,Y)_L, Z)$ is identically zero. Let B_1 be the subset of all such $O(D)$ lines.

Furthermore, $D < \frac{q}{ck\,\mathrm{poly}(d_Z)}$ for some $c > 1$, so, there exist lines in $\mathscr{H}_1$ and in $\mathscr{H}_2$ that are not in B_1.

If the Z-degree of $\partial_Z(\hat{Q})$ is zero, we get that for any such L not in B_1, $\partial_Z(\hat{Q}((X,Y)_{L_i}, g_{L_i}))$ is non-zero and we are done.

Else, the Z-degree of $\partial_Z(\hat{Q})$ is at least one. Since $\hat{Q}$ is square-free, we get from Corollary 3.13 that $\mathsf{Disc}_Z(\hat{Q})$ is a non-zero bivariate polynomial, and has degree at most $2d_Z D$. Thus, from Lemma 3.4, there are at most $2d_Z D$ lines L such that $\mathsf{Disc}_Z(\hat{Q})$ vanishes identically when restricted to these lines. Let B_2 be the set of such lines. Clearly, $|B_2| \leq 2d_Z D$.

From Observation 3.14, we get that for any line L that is not in $B_1 \cup B_2$, the polynomials $\hat{Q}((X,Y)_L, Z)$ and $\partial_Z(\hat{Q}((X,Y)_L, Z))$ do not share a common Z-root, and if the polynomial g_L is a root of $\hat{Q}((X,Y)_L, Z)$, then it cannot be a root of $\partial_Z(\hat{Q}((X,Y)_L, Z))$.

The claim now follows from the upper bound on the sizes of B_1 and B_2. □

Existence of a rational root

Let $L_1 \in \mathscr{H}_1$ be a line not excluded in Claim 5.4. Since L_1 is heavy, the line polynomial on L_1 is consistent with at least $\Omega(q/d_Z^2)$ of the line polynomials for lines in $\mathscr{H}_2$. Let S_1 be the subset of $\mathscr{H}_2$ of these lines. We also know from Claim 5.4 that $\partial_Z(\hat{Q}((X,Y)_{L_1}, g_{L_1}))$ is non-zero and $\hat{Q}((X,Y)_{L_1}, g_{L_1})$ is identically zero. Recall that the $(1,1,\hat{k})$-degree of $\hat{Q}$ is at most D and each of the line polynomials has degree at most $\hat{k}$, where $\hat{k} \leq kp^s$. So, a stronger bound on $\deg_Z(\hat{Q})$ is that $\deg_Z(\hat{Q}) \leq \deg_Z(Q)/p^s \leq D/\hat{k} = D/(kp^s)$.

From the setting of parameters, we have that $|S_1| \geq \Omega(\mathrm{poly}(\deg_Z(Q))Dk)$, for $q > c\,\mathrm{poly}(d_Z)Dk$ for a sufficiently large constant c. This implies that

$$|S_1| \geq \Omega(\deg_Z(\hat{Q})D\hat{k}).$$

Thus, from Lemma 2.1, we get that there is a rational function $U_1(X,Y)$ of degree at most $D\hat{k}$ such that

$$\hat{Q}(X, Y, U_1(X,Y)) \equiv 0,$$

and for all but D choices of lines $L \in S_1$, $U_1((X,Y)_L) = g_L$.

Let S_1' be the set of lines L in S_1 such that $U_1((X,Y)_L) = g_L$. We have that $|S_1'| \geq |S_1| \geq \Omega(q/\deg_Z(\hat{Q})^2)$ since $D < \frac{q}{ck\,\mathrm{poly}(\deg_Z(Q))} \leq \frac{q}{c\hat{k}\,\mathrm{poly}(\deg_Z(\hat{Q}))}$. Let us consider the induced subgraph of G' on vertices $S_1' \cup \mathscr{H}_1$.

The degree of vertex in S_1' in this graph is at least $\frac{\alpha q}{10\deg_Z(\hat{Q})^2}$ and hence the number of edges is at least $\frac{\beta q^2}{\mathrm{poly}(\deg_Z(\hat{Q}))}$ for some constant $\beta > 0$. Once again, by an application of Lemma 3.18, we get that this graph has an induced subgraph $G'' = (\mathscr{H}_1', S_1'', E'')$ where the size of the left and right side of the bipartition as well as the minimum degree are at least $\Omega\left(\frac{q}{\mathrm{poly}(\deg_Z(\hat{Q}))}\right)$.

We now repeat the argument applied to the graph G' over the last two sections to this new graph G'': we pick a line L_2 in S_1'' as the anchor (using Claim 5.4 again), and pick its neighbors in G'' as in the set S_2 and invoke Lemma 2.1 to obtain a rational function $U_2(X,Y)$ of degree at most Dk whose restriction on all but D lines L in $\mathscr{H}_1'$ equals the corresponding line polynomial g_L. Let $\mathscr{H}_1''$ be the subset of $\mathscr{H}_1'$ whose line polynomials are consistent with U_2. Note that the number of edges in G'' with both end points in $S_1'' \cup \mathscr{H}_1''$ is at least $\Omega(q^2/\mathrm{poly}(\deg_Z(\hat{Q})))$, where once again we use the fact that Dk (and hence D) is much smaller than q.

Recall that $S_1'' \subseteq S_1'$ and hence, for every line L in S_1'', $U_1((X,Y)_L) = g_L$. This means that for every $L' \in \mathscr{H}_1''$ and $L \in S_1''$, if L' and L are adjacent in G'', then U_1 and U_2 agree on the point $L \cap L'$. Thus, U_1 and U_2 are rational functions of degree $D\hat{k}$ and agree on at least $\Omega(q^2/\mathrm{poly}(\deg_Z(\hat{Q})))$ many points in $\mathbb{F}^2$. Since $D\hat{k} < q/\mathrm{poly}(\deg_Z(\hat{Q}))$, this means, from Lemma 3.3, that U_1 and U_2 must be the same rational function.

5.4 From a rational function to a polynomial

Let U denote the rational function in simplest form that equals U_1, U_2 constructed in the previous subsection. From the construction above, we know that its degree is at most $D\hat{k}$, and it equals a degree $\hat{k}$ polynomial when restricted to $\Omega(q/\mathrm{poly}(\deg_Z(\hat{Q})))$ many lines in two distinct directions. Since $D\hat{k}$ is much smaller than the number of lines in each direction, we apply the classical Polishchuk–Spielman lemma (Lemma 3.17) on the numerator and the denominator of U to conclude that there is a bivariate polynomial $P(X,Y)$ of degree at most $2\hat{k}$ that equals U on all but $O(D)$ of the $\Omega(q/\mathrm{poly}(\deg_Z(\hat{Q})))$ lines in consideration in the two directions.

5.5 A Z-root of Q

If the characteristic p of the underlying field $\mathbb{F}$ exceeds $\deg_Z(Q)$, then the polynomial $\hat{Q}$ is equal to Q_1, and hence $P(X,Y)$ is a Z-root of Q_1, and hence of Q, and this completes the proof of the theorem.

Over fields of (small, positive) characteristic p, we have that $Q_1(X,Y,Z) = \hat{Q}(X,Y,Z^{p^s})$ for some positive integer s. From the discussion so far, we know that $P(X,Y)$ is a Z-root of $\hat{Q}$ of in other words, $(Z - P(X,Y))$ divides $\hat{Q}(X,Y,Z)$. Substituting Z by Z^{p^s}, we get that $(Z^{p^s} - P(X,Y))$ divides $\hat{Q}(X,Y,Z^{p^s})$, and hence $Q_1(X,Y,Z)$ and therefore the original polynomial $Q(X,Y,Z)$. To complete the proof of the theorem, it suffices to show that $P(X,Y)$ equals $\hat{P}(X,Y)^{p^s}$ for some polynomial $\hat{P} \in \mathbb{F}[X,Y]$.

To see this, we recall that P has the property that there exist two distinct directions in $\mathbb{F}^2$ such that the restriction of P on at least $\Omega(q/\mathrm{poly}(\deg_Z(\hat{Q})))$ lines in these directions equals the line polynomial g_L. But from the relationship between $\hat{Q}$ and Q_1, we know that $g_L = \tilde{g}_L^{p^s}$, where $\tilde{g}_L$ is the Z-root of $Q_1((X,Y)_L, Z)$.

Let $s' \leq s$ be the largest integer such that there is a polynomial $\hat{P}$ satisfying $P = \hat{P}^{p^{s'}}$, and $\hat{P}$ is not the pth power of any polynomial in $\mathbb{F}[X,Y]$. Now, if $s' < s$, then $\hat{P}$ must be the pth power of every line polynomial g_L for which $g_L^{p^s} = P_L$. But, we have this property for more than $\deg(P)$ lines in two different directions, and hence by Lemma 3.9, we get that $\hat{P}$ is also a pth power, which is a contradiction. Thus, s' must equal s and $\hat{P}$ and P satisfy $P = \hat{P}^{p^s}$.

So, we get that $(Z^{p^s} - \hat{P}^{p^s}) = (Z - \hat{P})^{p^s}$ divides Q_1 and hence Q. This completes the proof of Theorem 5.1.

6 The low-degree test

In this section, we analyze the derandomized version of the line-point low-degree test in the high-error regime. We start by recalling the set up.

Setup: Let $\mathcal{U} = \{u_1, u_2, \ldots, u_r\} \subseteq \mathbb{F}^2$ be *directions* of interest to us. $u_i's$ represent distinct directions and hence, u_i and u_j are not scalar multiples of each other for any $i \neq j$. Let $\mathscr{L}_1, \ldots, \mathscr{L}_r$ be subsets of lines in $\mathbb{F}^2$ such that for every i, $\mathscr{L}_i$ is the set of *all* lines in the direction u_i in $\mathbb{F}^2$. Clearly, $|\mathscr{L}_i| = |\mathbb{F}| = q$. Clearly, for every point $\mathbf{a} \in \mathbb{F}^2$, and for every $i \in [t]$, there is a unique line $L_{i,v}$[2] in $\mathscr{L}_i$ that is incident to $\mathbf{a}$. Let $\mathscr{L}$ denote the union of $\mathscr{L}_i$.

We now restate the theorem we wish to prove. We recall the main theorem.

Theorem 1.2 (Analysis of derandomized line-point test)**.** *There is a constant $c \in \mathbb{N}$ such that the following holds for every $\varepsilon > 0$, every finite field $\mathbb{F}$ of size q, and all natural numbers k, r satisfying $q \geq k^2/\varepsilon^c$ and $r \geq 1/\varepsilon^c$. Let U be a set of r distinct directions in $\mathbb{F}^2$, and let $\mathscr{L}$ be the set of* all *lines along these r directions (i.e., $|\mathscr{L}| = rq$). Then for any $f \colon \mathbb{F}^2 \to \mathbb{F}$, we have*

$$\mathop{\mathbb{E}}_{\ell \in \mathscr{L}}\big[\mathrm{agree}(f|_\ell, \mathscr{P}_{k,1})\big] \geq \varepsilon \implies \mathrm{agree}(f, \mathscr{P}_{2k,2}) \geq \varepsilon^c\,.$$

Before we proceed it will be convenient to understand the hypothesis of the above theorem, namely

$$\mathop{\mathbb{E}}_{\ell \in \mathscr{L}}[\mathrm{agree}(f|_\ell, \mathscr{P}_{k,1})] \geq \varepsilon\,.$$

It will be convenient to interpret this statement in terms of a subgraph of the points-vs-line incidence graph. The points-vs-line incidence graph is the graph between the set $\mathcal{P}$ of all points in $\mathbb{F}^2$ and set $\mathscr{L}$ of allowed lines where a point $\mathbf{a} \in \mathcal{P}$ is adjacent to a line $\ell in \mathscr{L}$ if $\mathbf{a} \in \ell$. Let E^* be the set of edges of this incidence graph. We label the points $\mathcal{P} = \mathbb{F}^2$ with the function $f \colon \mathbb{F}^2 \to \mathbb{F}$, more precisely $\mathbf{a} \in \mathbb{F}^2$ is labeled with $f(\mathbf{a})$. We label the lines with univariate polynomials of degree k that have the best agreement with the restriction of the function f on that line. More precisely, for each $\ell \in \mathscr{L}$, we consider the restricted function $f|_\ell$ and find the univariate polynomial P_ℓ of degree at most k that has the best agreement with $f|_\ell$ (if there exists more than one best-fit, we break ties arbitrarily). We now consider the subgraph $(\mathcal{P}, \mathscr{L}, E)$ of the points-vs-line incidence graph where $E \subseteq E^*$ is defined as follows:

$$E = \{(\mathbf{a}, \ell) \in \mathcal{P} \times \mathscr{L} \mid \mathbf{a} \in \mathscr{L}, P_\ell(\mathbf{a}) = f(\mathbf{a})\}\,.$$

[2]note that the same line can be indexed in many different ways

In other words, $(\mathbf{a}, \ell)$ is an edge in E iff the line polynomial P_ℓ agrees with the points table f at the point $\mathbf{a}$. It immediately follows from the definition of this graph that $\mathbb{E}_{\ell \in \mathscr{L}}[\text{agree}(f|_\ell, \mathscr{P}_{k,1})] \geq \varepsilon$ iff $|E| \geq \varepsilon |E^*|$.

6.1 Pruning to *good* lines, *good* points

Consider the bipartite lines-vs-points incidence graph $G_f = (\mathcal{P}, \mathscr{L}, E)$ for the function f defined as follows. The set $\mathcal{P}$ is the set of all points in $\mathbb{F}^2$ and the set $\mathscr{L}$ is the union of all lines in $\cup_{i \in [r]} \mathscr{L}_i$. For a point $\mathbf{a} \in \mathcal{P}$ and a line L in $\mathscr{L}$, (v, L) is an edge in G_f iff the line L is incident to $\mathbf{a}$ and the line-point test for the function f passes on the line-point pair $(L, \mathbf{a})$.

Clearly, the number of points is q^2, the number of lines is qr and the maximum degree of any line in the graph G_f is at most the field size, i.e. q and the maximum degree of any point is r. Furthermore, if the test passes with probability ε, then the graph G_f has $\varepsilon q^2 r$ edges. Thus, the average degree of a line vertex in G is εq and the average degree of a point vertex is εr.

Applying Lemma 3.18 to the graph G_f gives us the following corollary.

Corollary 6.1. *Let $f : \mathbb{F}^2 \to \mathbb{F}$ be a function such that $\mathbb{E}_{\ell \in \mathscr{L}}[\text{agree}(f|_\ell, \mathscr{P}_{k,1})]$. Then, there exists a subgraph $G'_f = (\mathcal{P}', \mathscr{L}', E')$ of the graph G_f such that*

- $|\mathcal{P}'| \geq \frac{4\varepsilon}{5} q^2$, $|\mathscr{L}'| \geq \frac{4\varepsilon}{5} qr$.
- *The degree of every vertex in $\mathcal{P}'$ is at least $\varepsilon r/10$ and the degree of every vertex in $\mathscr{L}'$ is at least $\varepsilon q/10$.*

For the rest of this proof, we focus our attention on the lines and points in the graph G'_f. We refer to them as *good* lines and *good* points respectively. For the ease of notation, we also drop the subscript f and simply refer to G'_f as G'.

6.2 Interpolation

From this section onwards, we will use $\hat{k}$ to denote the maximum of k and $\log^2 q$. We think of $\hat{k}$ as a proxy for the degree parameter k.

In this section, we show that there is a non-zero trivariate polynomial $Q(X, Y, Z)$ of sufficiently low degree that in some sense succinctly *captures* the fact that the low-degree test passes with probability at least ε. This step is similar in spirit to the interpolation step in prior works, most notably in the low-degree test of Arora-Sudan [AS03], and was subsequently used in the work of Harsha, Kumar, Saptharishi and Sudan [HKSS24]. However, in our opinion, the details of the interpolation here are substantially simpler than those in these prior works. Furthermore, the quantitative guarantees are also somewhat stronger, and in particular the interpolated polynomial Q *explains* the passing of the test on *all* good lines and points and not just a subset of them as given by the analogous interpolation steps in [AS03, HKSS24]. This argument for interpolation was also discovered in an independent work of Kominers, Thaler and Zheng [KTZ26] where the goal was to obtain improved soundness guarantees for the (non-derandomized) line-point test.

We now prove the following lemma.

Lemma 6.2. *Let $\mathbb{F}$ be any field of size q and let p denote its characteristic.*

There exists a non-zero polynomial $Q(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ with $(1, 1, \hat{k})$-degree D at most $O\left(\frac{\hat{k}}{\varepsilon^2}\right)$ such that for every good *line L, and the corresponding line polynomial g_L of degree $k \leq \hat{k}$, the univariate polynomial $Q((X, Y)_L, g_L)$ is identically zero and $Q(\mathbf{a}, f(\mathbf{a}))$ is zero for every* good *point $\mathbf{a}$.*

We first set the parameters needed for the lemma.

Setting parameters: The parameter D is set to be equal to $\left(\frac{12\cdot 3\cdot 4\cdot 400}{2}\frac{\hat{k}}{\varepsilon^2}\right)$ and the parameter ρ is set to $\frac{12\cdot 3\cdot 1600\cdot 1600}{5}\cdot\frac{\hat{k}}{\varepsilon^4 rq}$. Recall that in the context of the results in this paper, the parameter $\varepsilon \in (0,1]$ is an arbitrary constant, $r = (1/\varepsilon)^c$ for a large enough c, and $k \leq \hat{k} = o(q)$. We have the following simple claim summarizing some of the inequalities satisfied for our setting of parameters.

Claim 6.3. *Let $\hat{k}, \rho, D$ be parameters as defined earlier in this section. Then, for all sufficiently large q,*

- $1 < \varepsilon r/20 < \frac{1}{2\rho}$
- $D > 20\hat{k} \geq 20k$
- $\rho qr = \Theta(\hat{k})$
- $\exp(-\frac{\varepsilon\rho qr}{100}) < 1/q^{100}$

We are now ready to proceed with the proof.

Proof of Lemma 6.2. The proof of existence of Q will be via the probabilistic method. We will probabilistically pick a small subset S of all good lines, and find a polynomial Q with low $(1,1,k)$-degree such that for every line L in S, $Q((X,Y)_L, g_L)$ is identically zero via the polynomial method. We will then use the geometry of the set up to show that with high probability, any such Q also satisfies the conclusion of the lemma. We now discuss the details.

Constructing S: The set S is constructed by starting with an empty set and including every good line L in S independently with probability ρ. Thus, the expected size of the set S equals $\rho \cdot |\text{Good Lines}|$. We also know that the number of good lines is at least $\frac{\varepsilon qr}{10} \geq \frac{4\varepsilon qr}{5}$, and at most qr. Thus,

$$\frac{\varepsilon\rho qr}{10} \leq \mathbb{E}[|S|] \leq \rho rq\,.$$

By Chernoff bound (Lemma 3.1), we also get that with probability at least $\left(1-\exp\left(-\frac{\varepsilon\rho qr}{100}\right)\right)$,

$$\frac{1}{2}\,\mathbb{E}[|S|] \leq |S| \leq \frac{3}{2}\,\mathbb{E}[|S|]\,.$$

For the rest of the proof, we assume that the above tail bound holds.

Constructing Q: For this step, we proceed via the polynomial method. Let $Q(X,Y,Z)$ be a polynomial with $(1,1,\hat{k})$-degree D such that its coefficients are formal variables. The goal is to show that there is a non-zero specialization of these formal variables (for coefficients) such that the Q satisfies $Q((X,Y)_L, g_L) \equiv 0$ for every L in the set S. Let the line L be defined as

$$L = \{(x_0,y_0) + \tau\cdot(u_0,u_1) : \tau \in \mathbb{F}\}\,.$$

Thus, the univariate $Q((X,Y)_L, g_L)$ can be explicitly written as $R_L(T) := Q\left(x_0 + Tu_0, y_0 + Tu_1, g_L(T)\right)$. The coefficients of $R_L(T)$ are clearly homogeneous linear forms in the coefficients of Q, and the degree of R_L

is at most the $(1, 1, \hat{k})$-degree of Q, which is at most D. Thus, setting $R_L(T)$ to be identically zero imposes at most $(D+1)$ homogeneous linear constraints on the coefficients of Q. If the number of such constraints is strictly less than the number of variables in the linear system, we must have a non-zero solution. Thus, from Lemma 3.2, we have that there is a non-zero solution if

$$\frac{D^3}{12\hat{k}} \geq (D+1)|S|.$$

Since D is a natural number, $D+1 \leq 2D$ and $|S|$ is at most $\frac{3}{2}\mathbb{E}[|S|]$, which in turn is at most $\frac{3}{2}\rho r q$, it suffices to have D such that $D^2 > 36\hat{k}\rho q r$, which is an inequality satisfied by our choice of D, ρ. We note that this step is completely deterministic once the random bits in the choice of the set S are fixed.

Behavior of Q on other good lines: We now argue that with high probability (over the choice of S), any polynomial Q constructed in the previous step satisfies $Q((X,Y)_L, g_L) \equiv 0$ for every good line L.

Let L be an arbitrary good line that is not in the set S. By definition, L has at least $\varepsilon q/10$ good points on it, and through each of these good points, there are at least $\varepsilon r/10$ lines that are also good and consistent with the value of f at the point. Let $\mathbf{a}$ be any good point on the line L and let $R_L(T)$ be the polynomial $Q((X,Y)_L, g_L)$. The goal in this step is to show that the polynomial $R_L(T)$ is identically zero with high probability over the randomness in the choice of S. By a union bound over the set of all good lines, this will complete the proof of the lemma. To this end, we proceed by showing that $R_L(T)$ has *too* many zeroes, or in other words, the polynomial $Q((X,Y)_L, g_L)$ vanishes at many points on L, and hence must be identically zero.

The key observation for this is that for any point $\mathbf{a}$, if L and L' are both neighbors of $\mathbf{a}$ in the graph G', i.e. the test passes for both the line-point pairs $(L', \mathbf{a})$ and $(L, \mathbf{a})$, then the line polynomials g_L and $g_{L'}$ agree on $\mathbf{a}$. Moreover, if the line L' is in S, then, by construction of Q, $Q((X,Y)_{L'}, g_{L'})$ is identically zero. From the above two properties, we have that R_L also has a zero at $\mathbf{a}$. We state the following simple claims and use them to complete the proof of the lemma, but we need a definition first.

We say that a good point $\mathbf{a}$ on L is *fortunate* if there is a line $L' \neq L$ through $\mathbf{a}$ such that L' is a neighbor of v in the graph G' and L' is contained in S. A point that is not fortunate is said to be *unfortunate*.

Claim 6.4. *$\mathbf{a}$ is unfortunate with probability at most $(1-\rho)^{\left(\frac{\varepsilon r}{10}-1\right)}$, which, from our choice of parameters is at most $\left(1-\frac{\varepsilon\rho r}{40}\right)$.*

Claim 6.5. *Let $\mathbf{a}, \mathbf{a}'$ be two distinct good points that are neighbors of L in the graph G'. Then, the events that $\mathbf{a}$ and $\mathbf{a}'$ are fortunate are independent of each other.*

Since L is a good line, it has at least $\varepsilon q/10$ good points as neighbors in G' and from Claim 6.4, we have that the expected number of fortunate points on the line L is at least $\frac{\varepsilon^2\rho q r}{400}$, which from the choice of our parameters is $\Theta(\hat{k}/\varepsilon^2)$, and from our choice of constants, this is at least $10D$. Furthermore, from Claim 6.5, the number of fortunate points on L is a sum of independent random variables, and hence via Lemma 3.1, we get that with probability at least $\left(1-\exp\left(-\Omega\left(\hat{k}/\varepsilon^2\right)\right)\right)$, L contains at least $(D+1)$ fortunate points. This implies that the univariate polynomial $R_L = Q((X,Y)_L, g_L)$ that has degree at most D has at least $D+1$ distinct zeroes, and hence must be identically zero.

From a union bound over the at most $qr < q^2$ good lines, we get that with high probability Q satisfies

$$Q((X,Y)_{\hat{L}}, g_{\hat{L}}) \equiv 0$$

for every good line $\hat{L}$.

We now note that the above condition also implies that Q must satisfy $Q(\mathbf{a}, f(\mathbf{a})) = 0$ for every good point $\mathbf{a}$, since every good point is incident to many good lines L (all of its neighbors in the graph G') such that for each of these lines f and g_L agree at $\mathbf{a}$. This condition lets us conclude that $\deg_Z(Q)$ is at least one: if this was not the case, Q is a bivariate of total degree at most D that vanishes on at least $4\varepsilon/5q^2$ points (namely, all the good points) in $\mathbb{F}^2$. But, $D = o(q)$, so this implies that Q must be identically zero, which is a contradiction. Finally, since Q depends on Z and yet does not contain any monomial with its Z-degree divisible by p, we get from the definition of Hasse derivatives that $\partial_Z(Q)$ must be non-zero.

This completes the proof of Lemma 6.2.

□

Proof of technical claims

Proof of Claim 6.4. Every good line incident to $\mathbf{a}$ is included in the set S independently with probability ρ and $\mathbf{a}$ being a good point is a neighbor of at least $\varepsilon r/10$ such good lines in G', including L itself. So, the probability that none of the good lines incident to v, which are not equal to L, is contained in S is at most $(1-\rho)^{\left(\frac{\varepsilon r}{10}-1\right)}$. The rest of the argument is just a sequence of inequalities using the fact that $1 < \varepsilon r/20 < \frac{1}{2\rho}$.

$$\begin{aligned}
(1-\rho)^{\left(\frac{\varepsilon r}{10}-1\right)} &\leq (1-\rho)^{\left(\frac{\varepsilon r}{20}\right)} \\
&\leq 1 - \rho\frac{\varepsilon r}{20} + \frac{1}{2}\left(\rho\frac{\varepsilon r}{20}\right)^2 \cdot \left(1 + \sum_{i=1}^{\infty}\left(\rho\frac{\varepsilon r}{20}\right)^i\right) \\
&\leq 1 - \rho\frac{\varepsilon r}{20} + \frac{1}{2}\left(\rho\frac{\varepsilon r}{20}\right)^2 \left(1 + \sum_{i=1}^{\infty} 1/2^i\right) \\
&\leq 1 - \rho\frac{\varepsilon r}{20} + \left(\rho\frac{\varepsilon r}{20}\right)^2 \\
&\leq 1 - \rho\frac{\varepsilon r}{40}
\end{aligned}$$

□

Proof of Claim 6.5. The independence of the events at $\mathbf{a}, \mathbf{a}'$ immediately follows from the fact that every line is included in S independently with probability ρ and the events at $\mathbf{a}, \mathbf{a}'$ do not have any line in common apart from L itself, which does not play a role in these points being fortunate. □

6.3 Proof of Theorem 1.2

We are now ready to complete the analysis of the low-degree test.

Proof of Theorem 1.2. Since the function f passes the test with probability ε, we get from Lemma 6.2 that there is a $Q(X,Y,Z)$ with $(1,1,\hat{k})$-degree at most $O\left(\frac{\hat{k}}{\varepsilon^2}\right)$ such that for every good line L, and the corresponding line polynomial g_L of degree k, the univariate polynomial $Q((X,Y)_L, g_L)$ is identically zero.

Note that Q must depend on the variable Z, else, it has degree at most D and vanishes at all good points, and there are much more than Dq of them for our choice of parameters. Thus, if Q does not depend on Z, then by Lemma 3.3, it must be identically zero.

Reducing to the non-degenerate case: As in the proof of Theorem 5.1, we work with the square-free part of Q. Let Q_1 be the square-free part of Q. Let $s \in \mathbb{N}$ be the largest integer such that there exists a polynomial $\hat{Q}(X, Y, Z)$ for which $Q_1(X, Y, Z) = \hat{Q}(X, Y, Z^{p^s})$.

This implies that $\partial_Z(\hat{Q})$ is a non-zero polynomial. We now note that $\hat{Q}$ also satisfies the interpolation constraints on all good lines and good points, i.e. $\hat{Q}((X, Y)_L, \hat{g}_L) \equiv 0$ for all good lines L and line polynomials $\hat{g}_L := g_L^{p^s}$ and $\hat{Q}(\mathbf{a}, \hat{f}(\mathbf{a}))$ is zero for all good points $\mathbf{a}$, where $\hat{f}(\mathbf{a}) := f(\mathbf{a})^{p^s}$. Furthermore, the $(1, 1, p^s\hat{k})$-degree of $\hat{Q}$ is at most D. Notice that $p^s < \deg_Z(Q_1)$.

Now, if $\deg_Z(\partial_Z(\hat{Q}))$ is zero, i.e. it is a non-zero polynomial of degree at most D in $\mathbb{F}[X, Y]$, then, it follows from Lemma 3.3 that there must exist a good point $\mathbf{a}$ such that $\partial_Z(\hat{Q})$ is non-zero for $\mathbf{a}$. We now argue that a similar conclusion holds even when $\deg_Z(\partial_Z(\hat{Q}))$ is at least one. To see this, we consider the discriminant of $\hat{Q}$ with respect to Z. From Corollary 3.13, and the properties of $\hat{Q}$ discussed so far, we get that $\mathsf{Disc}_Z(\hat{Q})$ is a non-zero bivariate of degree at most $O(\deg_Z(Q)D)$. Multiplying $\mathsf{Disc}_Z(\hat{Q})$ with the leading coefficients of $\hat{Q}$ and $\partial_Z(\hat{Q})$, while viewing these as a univariate in Z, we get a non-zero polynomial of degree at most $O(\deg_Z(\hat{Q})D)$. Since q is large enough compared to $\mathrm{poly}(\deg_Z(Q)D\hat{k})$, we get from Lemma 3.3 that there is a good point $\mathbf{a}$ for which this product polynomial is non-zero. From Observation 3.14 and Corollary 3.12, we get that for any such $\mathbf{a}$, the univariates $\hat{Q}(\mathbf{a}, Z)$ and $\partial_Z(\hat{Q})(\mathbf{a}, Z)$ do not have a common-zero. In particular, since $\hat{f}(\mathbf{a})$ is a zero of $\hat{Q}(\mathbf{a}, Z)$ (from the interpolation constraints), we get that $\partial_Z(\hat{Q})(\mathbf{a}, \hat{f}(\mathbf{a}))$ must be non-zero. For the rest of the proof, we work with this good point $\mathbf{a}$.

Setting up for lifting from parallel lines: We now proceed with the proof of the theorem. Let $\hat{\mathscr{L}}$ be the neighbors of the point $\mathbf{a}$ in the graph G'. Since $\partial_Z(\hat{Q}(\mathbf{a}, \hat{f}(\mathbf{a}))) \neq 0$ and for every $L \in \hat{\mathscr{L}}$, $\hat{g}_L$ and $\hat{f}$ must agree on $\mathbf{a}$, we get that the polynomial $\partial_Z(\hat{Q}((X, Y)_L, Z))$ is non-zero at $Z = \hat{g}_L$. Let us fix one such line L in $\hat{\mathscr{L}}$, and consider the set $\mathscr{L}'$ of lines L' such that L and L' have a common neighbor in G'. From the properties of G', L is adjacent to $\varepsilon q/10$ points and each of these points is incident to at least $\varepsilon r/10$ lines. Thus, $|\mathscr{L}'|$ is at least $\varepsilon^2 qr/100$. Since there are at most q lines in any direction, we get that there is a set $S \subseteq [r]$ of size at least $\varepsilon^2 r/200$, such that for every $i \in S$, $|\mathscr{L}_i \cap \mathscr{L}'|$ is at least $\varepsilon^2 q/200$. We focus on these directions.

We now note that for every $i \in S$, the set of parallel lines $\mathscr{L}_i \cap \mathscr{L}'$ together with the line L satisfies the hypothesis of Lemma 2.1, with the degree of the root on the line polynomials being at most $k' = p^s k$. Thus, it follows that if $\varepsilon^2 q/200 > \Omega(\deg_Z(Q)Dk')$, (which is an inequality that holds in our setting) then for each such i, we have a rational function $U_i(X, Y)$ of degree at most $Dk' = p^s Dk$ that is a Z-root of $\hat{Q}(X, Y, Z)$ and furthermore, the restriction of U_i on L equals $\hat{g}_L$ for all but $O(Dk')$ lines in $\mathscr{L}_i \cap \mathscr{L}'$.

From rational roots to polynomial roots: In our setting of parameters, $\varepsilon^2 r/200$ is greater than the Z-degree of $\hat{Q}$ (if the constant c in Theorem 1.2 is chosen to be large enough). So, there must exist distinct $i, j \in S$ such that $U_i(X, Y) = U_j(X, Y)$. This rational function, that we now refer to as U, has degree at most Dk' and for at least $\varepsilon^2 q/200 - O(Dk') = \Omega(\mathrm{poly}(\varepsilon)q)$ many parallel lines in two different directions, the restriction of U to these lines is a polynomial of degree at most kp^s. In other words, for each of these lines,

the restriction of the denominator of U to this line divides the restriction of the numerator of U on this line, and yields a quotient of degree at most kp^s. Thus, from Lemma 3.17, we get that if $q > \text{poly}(1/\varepsilon)D\hat{k}$, then when reduced to its simplest form, the rational function U is actually a polynomial of degree at most $2kp^s$. Moreover, the restriction of U on at least $\text{poly}(\varepsilon)(q - D\hat{k}) = \text{poly}(\varepsilon)q$ of these lines $L \in \mathscr{L}_i \cup \mathscr{L}_j$ equals the corresponding line polynomial $\hat{g}_L$. Since each of these lines is incident to at least $\Omega(\varepsilon q)$ points in the graph G' and the line polynomials $\hat{g}_L$ are consistent with the function values of $\hat{f}$ at these points, we get that U equals the function $\hat{f}$ on $\text{poly}(\varepsilon)q^2$ points.

We also know that the polynomial U is a p^s power when restricted to $\text{poly}(\varepsilon)q$ lines in two different directions. Thus, by (an iterative application of) Lemma 3.9, we get that there exists a polynomial $\tilde{U}(X, Y)$ of degree at most $2k$ such that $U := (\tilde{U})^{p^s}$. Furthermore, since pth roots of a field element in $\mathbb{F}$ are unique, and $\hat{f}(\mathbf{a}) = f(\mathbf{a})^{p^s}$ by definition, we get that if U agrees with $\hat{f}$ on the point $\mathbf{a}$, then $\tilde{U}$ must agree with f on $\mathbf{a}$. Furthermore, the degree of $\tilde{U}$ is at most $\deg(U)/p^s \leq 2k$.

This completes the proof of the theorem. □

7 Counterexamples when $k \gg q^{1/2}$

In this section, we show some limitations of derandomized tests when $q \leq (k/\varepsilon)^2$. The main result of this section is the following theorem which immediately implies Theorem 1.1.

Theorem 7.1. *For every $r, s \in N$ and prime p, the following holds.*

Let the local agreement parameter $\varepsilon := p^{-r}$. Let $\mathbb{F} = \mathbb{F}_q$ be the finite field of size $q := p^{2rs}$ and the degree parameter $k := p^{r(s-1)} = \varepsilon\sqrt{q}$.

Let $\mathscr{L}$ be the set of all lines in $\mathbb{F}_q^2$ whose slope lies in the subfield $\mathbb{F}_{p^{rs}}$. Then there exists a collection of functions $(f_\ell : \ell \to \mathbb{F}_q)_{\ell \in \mathscr{L}}$ such that:

1. *For each $\ell \in \mathscr{L}$, f_ℓ agrees with a univariate polynomial P_ℓ of degree at most k on ℓ.*
2. *If we pick the two lines $\ell, \ell' \in \mathscr{L}$ independently and uniformly at random from the set of all lines in $\mathscr{L}$, and let $\mathbf{a}$ be their point of intersection (undefined if the lines are parallel), we have:*

$$\Pr[f_\ell(\mathbf{a}) = f_{\ell'}(\mathbf{a})] \geq \varepsilon - O\left(\frac{1}{\sqrt{q}}\right).$$

3. *There exists a trivariate polynomial $Q(X, Y, Z)$ of Z-degree $1/\varepsilon$ and $(1, 1, k)$-degree at most $\sqrt{q}+1$ such that for each $\ell \in \mathscr{L}$, P_ℓ is a Z-root of the restriction of Q to ℓ, yet Q has no polynomial Z-root.*
4. *For any bivariate polynomial $g(X, Y)$ of total degree at most Ck for some $C < \sqrt{q}$, if we choose a line $\ell \in \mathscr{L}$ uniformly at random, then we have:*

$$\Pr[g|_\ell = f_\ell] \leq {}^{C}/_{q}$$
$$\mathbb{E}[\text{agree}(g|_\ell, f_\ell)] \leq {}^{2C\varepsilon}/_{\sqrt{q}}.$$

5. *There exists a function* $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ *satisfying*

$$\mathop{\mathbb{E}}_{\ell\in\mathscr{L}}[\text{agree}(f|_\ell, f_\ell)] \geq \varepsilon,$$

and yet $\text{agree}(f,g) \leq {}^{C}/_{\sqrt{q}}$ *for every bivariate polynomial* $g(X,Y)$ *of total degree at most* $C\sqrt{q}/\varepsilon$*-degree where* $C > 1$.

First for some notation and helper claims that will help us prove this theorem. Given a prime p and $r, s \in \mathbb{N}$, consider the field extensions: $E := \mathbb{F}_{p^r} \subseteq H := \mathbb{F}_{p^{rs}} \subseteq \mathbb{F} := \mathbb{F}_{p^{2rs}}$. It will be convenient to use the following notation: $e := p^r, h := |H| = e^s$ and $q := |\mathbb{F}| = e^{2s} = h^2$. To understand the counterexample, it is instructive to think of the case when $p = 2$ and $r = 1$.

We will use Tr to denote the usual trace polynomial from $\mathbb{F} = \mathbb{F}_q$ to $E = \mathbb{F}_e$,

$$\mathsf{Tr}(z) = \mathsf{Tr}_{\mathbb{F}/E}(z) = \sum_{i=0}^{2s-1} z^{e^i}\,.$$

Our construction will also use the *half-trace* function, denoted by HTr, which refers to trace polynomial from $H = \mathbb{F}_h$ to $E = \mathbb{F}_e$, but extended as a polynomial to all of $\mathbb{F}$.

$$\mathsf{HTr}(z) := \mathsf{Tr}_{H/E}(z) = \sum_{i=0}^{s-1} z^{e^i}\,.$$

Evaluated on $\mathbb{F}$ it is an E-linear map, and evaluated on H it is the field trace map to E.

For $a \in H$ and $b \in \mathbb{F}$, let $\ell_{a,b}\colon \mathbb{F}_q \to \mathbb{F}_q^2$ denote the line

$$\ell_{a,b}(T) := (T, aT + b)\,,$$

Note that

$$\mathscr{L} = \{\ell_{a,b} \mid (a,b) \in H \times \mathbb{F}\}\,. \tag{7.2}$$

For each $a \in H$ and $b \in \mathbb{F}$, define the polynomial $P_{a,b}(T) \in \mathbb{F}[T]$ of degree e^{s-1} by

$$P_{a,b}(T) := \mathsf{HTr}(b^h T)\,.$$

For the line $\ell = \ell_{a,b}$, we use $P_{a,b}$ to define the function $f_\ell\colon \ell \to \mathbb{F}$ as follows:

$$f_\ell(t, at+b) = P_{a,b}(t)\,. \tag{7.3}$$

First, we see that these line polynomials are mostly consistent. The lines $\ell_{a,b}$ and $\ell_{a',b'}$ intersect at $\left({}^{(b'-b)}/_{(a-a')}, {}^{(ab'-a'b)}/_{(a-a')}\right)$.

Claim 7.4.

$$\Pr_{\substack{a,a'\in H\\ b,b'\in\mathbb{F}}}\left[P_{a,b}\left(\frac{b'-b}{a-a'}\right) = P_{a',b'}\left(\frac{b'-b}{a-a'}\right)\right] \geq \frac{1}{e} - O\left(\frac{1}{h}\right)\,.$$

Proof. The relevant expressions are only defined if $a \neq a'$. Condition on $a \neq a'$; this only changes the claimed probability by $O(1/h)$.

Let t be the random variable $\frac{b'-b}{a-a'} \in \mathbb{F}_p$. We have:

$$\begin{aligned} P_{a,b}(t) - P_{a',b'}(t) &= \mathsf{HTr}(b^h t) - \mathsf{HTr}((b')^h t) \\ &= \mathsf{HTr}((b^h - (b')^h)t) \\ &= \mathsf{HTr}\left((b-b')^h \cdot \frac{b-b'}{a'-a}\right) \\ &= \mathsf{HTr}\left(\frac{(b-b')^{h+1}}{a'-a}\right). \end{aligned}$$

Now observe that when b, b' are picked uniformly from $\mathbb{F}$, then $b-b'$ is a uniform element of $\mathbb{F}$, and $(b-b')^{h+1} = \mathrm{Norm}_{\mathbb{F}/H}(b-b')$ is essentially (upto error $\frac{1}{q}$) a uniform nonzero element of H. We also have that $a'-a$ is essentially (upto error $\frac{1}{h}$) a uniform element of H.

Thus the probability in question is, upto error $O(\frac{1}{h})$ the probability that HTr of a uniform nonzero element c of H has $\mathsf{HTr}(c) = 0$. But for $c \in H$, we have that $\mathsf{HTr}(c) = \mathsf{Tr}_{H/E}(c)$, and the probability that $\mathsf{HTr}(c)$ equals 0 equals $1/e$.

Thus the probability in question is at least $1/e - O(1/h)$. □

Next we see that there is no bivariate polynomial $U(X,Y)$ that has high agreement with these line polynomials in a very strong sense.

Claim 7.5. *For any $C < h$ and for all $U(X,Y)$ of degree at most Ch/e,*

$$\Pr_{\ell \in \mathscr{L}}[U|_\ell = f_\ell] \leq \frac{C}{q}.$$

Proof. Let B, Q be polynomials defined as follows.

$$\begin{aligned} B(X,Y) &:= XY^h - X^h Y, \\ Q(X,Y,Z) &:= Z^e - Z + B(X,Y). \end{aligned}$$

We would need the following two technical claims for the proof.

Subclaim 7.6. *For any polynomial $U(X,Y)$, the polynomial $H(X,Y) := Q(X,Y,U(X,Y))$ is not identically zero.*

Subclaim 7.7. *For every $a \in H, b \in \mathbb{F}$, the polynomial $P_{a,b}(T)$ is a Z-root of $Q(\ell_{a,b}(T), Z)$.*

Given the sub claims, the proof of the claim is fairly straightforward. Let U is a bivariate polynomial of degree $d \leq Ch$. Define

$$R(X,Y) := Q(X,Y,U(X,Y)).$$

By Subclaim 7.6, R is a non-zero bivariate polynomial of degree at most $\max(ed, h+1)$ and its individual degree in both X, Y is upper bounded by $\max(ed, h)$, where $d \leq Ch/e$ is the total degree of U. Since

$Q(\ell_{a,b}(T), P_{a,b}(T))$ is identically zero for every $a \in H, b \in \mathbb{F}$, and $f_\ell(t) = P_{a,b}(t)$ for every line ℓ parameterized as $(t, at+b)$, we get that $U|_\ell = f_\ell$ implies that $R|_\ell(T) = Q(T, aT+b, U(T, aT+b))$ is identically zero. Here we use that fact that $\deg_T(R|_\ell) \le \max(ed, h+1) \le \max(Ch, h+1) \le h^2$ since $C < h$. So, the equality of U_ℓ and f_ℓ as functions on ℓ implies that they are equal as formal polynomials and since $f_\ell = P_{a,b}$ is a formal Z root of $Q((X,Y)_\ell, Z)$, so must U_ℓ. Thus, every such line ℓ for which $U|_\ell = f_\ell$ gives us a *distinct* factor of $R(X,Y)$ of the form $(Y - aX - b)$. So, the number of such lines is at most the Y degree of R, which is at most $\max(ed, h) \le Ch = C\sqrt{q}$. Finally, observing that $\mathscr{L}$ has exactly $hq = q^{3/2}$ lines completes the proof of the claim. □

We now prove the subclaims.

Proof of Subclaim 7.6. Consider the infinite power series $\psi := B + B^e + B^{e^2} + B^{e^3} + \cdots + \infty$. Observe that $Q(X, Y, \alpha + \psi)$ is identically zero for every $\alpha \in E$. Thus, $\{a + \psi \mid a \in E\}$ are Z-roots of Q in the ring of power formal series in X, Y over $\mathbb{F}$. Furthermore, observe that these roots are truly power series (and cannot be polynomials) since B is homogeneous and each term B^{e^i} contributes non-zero monomials of degree exactly $e^i(h+1)$ that can never be canceled out. Since the Z-degree of Q equals $e = |E|$, it cannot have any more roots in this ring (and hence the polynomial ring). □

Proof of Subclaim 7.7. Follows immediately by plugging in and checking that $Q(\ell_{a,b}(T), P_{a,b}(T))$ is identically zero for all $a \in H$ and $b \in \mathbb{F}$.

$$
\begin{aligned}
Q(\ell_{a,b}(T), P_{a,b}(T)) &= (P_{a,b}(T))^e - P_{a,b}(T) + T(aT+b)^h - T^h(aT+b) \\
&= \left(\mathsf{HTr}(b^h T)\right)^e - \mathsf{HTr}(b^h T) + T^{h+1}(a - a^h) + (Tb^h - T^h b) \\
&= \left(\sum_{i=0}^{s-1} (b^h T)^{e^i}\right)^e - \left(\sum_{i=0}^{s-1} (b^h T)^{e^i}\right) + (Tb^h - T^h b) && \text{[since } a^h = h \text{ as } a \in H\text{]} \\
&= \left(\sum_{i=1}^{s} (b^h T)^{e^i}\right) - \left(\sum_{i=0}^{s-1} (b^h T)^{e^i}\right) + (Tb^h - T^h b) \\
&= (b^h T)^{e^s} - (b^h T) + (Tb^h - T^h b) \\
&= b^{h^2} T^h - b^h T + (Tb^h - T^h b) && \text{[since } e^s = h\text{]} \\
&= T^h(b^{h^2} - b) = 0 && \text{[since } b^q = b \text{ as } b \in \mathbb{F}_{h^2} = \mathbb{F}_q\text{]}
\end{aligned}
$$

Note that we crucially use that $a^h = a$ and $b^q = b$. □

We are now ready to prove Theorem 7.1.

Proof of Theorem 7.1. Let p be a prime and $r, s \in \mathbb{N}$. Consider the field extensions: $E := \mathbb{F}_{p^r} \subseteq H := \mathbb{F}_{p^{rs}} \subseteq \mathbb{F} := \mathbb{F}_{p^{2rs}}$. Note, the local agreement parameter $\varepsilon = p^{-r} = 1/e$ and the degree parameter $k = \varepsilon\sqrt{q} = h/e = p^{r(s-1)}$.

The set $\mathscr{L}$ of all lines whose slopes lie in the subfield $H = \mathbb{F}_{p^{rs}}$ is given by (7.2) and the collection of functions $(f_\ell)_{\ell \in \mathscr{L}}$ be as in (7.3).

Item 1 follows from the definition of polynomial $P_{a,b}$ which has degree at most $e^{s-1} = p^{r(s-1)}$ while Item 2 follows from Claim 7.4 and Item 3 follows from Subclaim 7.6 and Subclaim 7.7.

We now use Claim 7.5 to prove Item 4. Let g be a bivariate polynomial of total degree at most $Ck = Ch/e$ for some $C < h$. By Claim 7.5, we have the first subitem that $\Pr_{L\in\mathscr{L}}[g|_\ell = f_\ell] \leq C/q$. Now, to prove the second subitem, we note that $g|_\ell, f_\ell$ are both univariates polynomial on ℓ of degree at most Ck. Thus, if they are not equal, then they agree on at most Ck/q points on ℓ. So, using Claim 7.5, we get

$$\begin{aligned}
\mathop{\mathbb{E}}_{\ell\in\mathscr{L}}[\text{agree}(g|_\ell, f_\ell)] &\leq \Pr_{L\in\mathscr{L}}[g|_\ell = f_\ell]\cdot 1 + \Pr_{\ell\in\mathscr{L}}[g|_\ell \neq f_\ell]\cdot\frac{Ck}{q} \\
&\leq \frac{C}{q} + \left(1-\frac{C}{q}\right)\frac{Ch}{eq} \leq \frac{C}{q} + \frac{C}{e\sqrt{q}} \\
&\leq \frac{2C\varepsilon}{\sqrt{q}}.
\end{aligned}$$

Finally, we are left with proving Item 5. We now define the points table $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ as follows. For every point $\mathbf{a}\in\mathbb{F}^2$, let $\mathscr{L}_\mathbf{a}$ be the subset of $|H| = \sqrt{q}$ lines in $\mathscr{L}$ that are incident to $\mathbf{a}$. From Subclaim 7.7, and the form of the polynomial Q there, we get that for every $\mathbf{a}\in\mathbb{F}^2$ and $\ell\in\mathscr{L}_\mathbf{a}$, $Q(\mathbf{a}, Z)$ has Z-degree exactly $e = 1/\varepsilon$ and f_ℓ is a Z-root of $Q((X,Y)_\ell, Z)$. Thus, for every $\ell\in\mathscr{L}_\mathbf{a}$, $f_\ell(\mathbf{a})$ equals one of the e roots of $Q(\mathbf{a}, Z)$. We set $f(\mathbf{a})$ to be the most popular value taken by $h_\ell(\mathbf{a})$ as we range over the $|H|$ lines $\ell\in\mathscr{L}_\mathbf{a}$.

We now argue that this f has at least ε-expected local agreement with polynomials of degree at most k. Now, for every $\mathbf{a}$, we have that $\Pr_{\ell\in\mathscr{L}_\mathbf{a}}[f(\mathbf{a}) = h_\ell(\mathbf{a})]$ is at least $1/e = \varepsilon$. Hence,

$$\begin{aligned}
\mathop{\mathbb{E}}_{\ell\in\mathscr{L}}[\text{agree}(f|_\ell, f_\ell)] &= \Pr_{\ell\in\mathscr{L},\mathbf{a}\in\ell}[f(\mathbf{a}) = f_\ell(\mathbf{a})] \\
&= \Pr_{\mathbf{a}\in\mathbb{F}^2,\ell\in\mathscr{L}_\mathbf{a}}[f(\mathbf{a}) = f_\ell(\mathbf{a})] \\
&= \frac{1}{q^2}\sum_{\mathbf{a}\in\mathbb{F}^2}\Pr_{\ell\in\mathscr{L}_\mathbf{a}}[f(\mathbf{a}) = f_\ell(\mathbf{a})] \\
&\geq \frac{1}{q^2}\sum_{\mathbf{a}\in\mathbb{F}^2}\varepsilon \\
&\geq \varepsilon
\end{aligned}$$

Finally, we have to argue that f has low agreement with every $g(X,Y)\in\mathbb{F}[X,Y]$ of degree at most $O(\sqrt{q})$. To see this, recall from the definition of f that for every $\mathbf{a}\in\mathbb{F}^2$, $Q(\mathbf{a}, f(\mathbf{a})) = 0$. Furthermore, from Subclaim 7.6 that for every *polynomial* $g(X,Y)\in\mathbb{F}[X,Y]$, $Q(X,Y,g(X,Y))$ is a non-zero polynomial, and its degree is at most $\max(\sqrt{q}+1, e\cdot\deg(g))$. Thus, if $f(\mathbf{a})$ equals $g(\mathbf{a})$ for some $\mathbf{a}\in\mathbb{F}^2$, then $Q(X,Y,g(X,Y))$ must vanish at $\mathbf{a}$. But from Lemma 3.3, this can happen on at most $\frac{\max(\sqrt{q}+1, e\cdot\deg(g))}{q}$ fraction of points in $\mathbb{F}^2$. If $\deg(g) \leq C\sqrt{q}/\varepsilon$ for some $C\geq 1$, then this bound is at most $C/\sqrt{q}$.

This completes the proof of Theorem 7.1. □

References

[ALMSS98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. *Proof verification and the hardness of approximation problems*. J. ACM, 45(3):501–555, May 1998. (Preliminary version in *33rd FOCS*, 1992). eccc:1998/008. 3

[AS98] Sanjeev Arora and Shmuel Safra. *Probabilistic checking of proofs: A new characterization of NP*. J. ACM, 45(1):70–122, January 1998. (Preliminary version in *33rd FOCS*, 1992). 3

[AS03] Sanjeev Arora and Madhu Sudan. *Improved low-degree testing and its applications*. Combinatorica, 23(3):365–426, 2003. (Preliminary version in *29th STOC*, 1997). eccc:1997/003. 3, 4, 7, 8, 25

[BGHSV05] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. *Short PCPs verifiable in polylogarithmic time*. In Luca Trevisan, ed., *Proc. 20th IEEE Conf. on Comput. Complexity*, pages 120–134. 2005. Full version available at http://www.tcs.tifr.res.in/~prahladh/papers/BGHSV2/BGHSV2005.pdf. 3

[BGHSV06] ———. *Robust PCPs of proximity, shorter PCPs and applications to coding*. SIAM J. Comput., 36(4):889–974, 2006. (Preliminary version in *36th STOC*, 2004). eccc:2004/021. 3

[BKRRSS26] Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. *Closure under factorization from a result of Furstenberg*. In Aditya Bhaskara and Artur Czumaj, eds., *Proc. 58th ACM Symp. on Theory of Computing (STOC)*, pages 174–185. 2026. arXiv:2506.23214, eccc:2025/084. 9, 14

[BSVW03] Eli Ben-Sasson, Madhu Sudan, Salil Vadhan, and Avi Wigderson. *Randomness-efficient low degree tests and short PCPs via epsilon-biased sets*. In Lawrence L. Larmore and Michel X. Goemans, eds., *Proc. 35th ACM Symp. on Theory of Computing (STOC)*, pages 612–621. 2003. 3

[FS95] Katalin Friedl and Madhu Sudan. *Some improvements to total degree tests*. In *Proc. 3rd Israel Symp. on Theoretical and Computing Systems*, pages 190–198. 1995. (See arXiv for corrected version). arXiv:1307.3975. 3

[Fur67] Harry Furstenberg. *Algebraic functions over finite fields*. Journal of Algebra, 7(2):271–277, 1967. 9, 14

[GS06] Oded Goldreich and Madhu Sudan. *Locally testable codes and PCPs of almost linear length*. J. ACM, 53(4):558–655, 2006. (Preliminary version in *43rd FOCS*, 2002). eccc:2002/050. 3

[HKSS24] Prahladh Harsha, Mrinal Kumar, Ramprasad Saptharishi, and Madhu Sudan. *An improved line-point low-degree test*. In Santosh Vempala, ed., *Proc. 65th IEEE Symp. on Foundations of Comp. Science (FOCS)*, pages 1883–1892. 2024. arXiv:2311.12752, eccc:2023/182. 3, 4, 6, 7, 8, 11, 25

[KTZ26] Scott Duke Kominers, Justin Thaler, and Kai Zhe Zheng. *Improved soundness for the line-versus-point test*, 2026. (manuscript). eccc:2026/147. 8, 25

[MR08] Dana Moshkovitz and Ran Raz. *Sub-constant error low degree test of almost-linear size*. SIAM J. Comput., 38(1):140–180, 2008. (Preliminary version in *38th STOC*, 2006). eccc:2005/086. 3, 4, 5, 6

[MR10a] ———. *Sub-constant error probabilistically checkable proof of almost-linear size*. Comput. Complexity, 19(3):367–422, 2010. eccc:2007/026. 3

[MR10b] ———. *Two-query PCP with subconstant error*. J. ACM, 57(5), 2010. (Preliminary version in *49th FOCS*, 2008). eccc:2008/071. 3

[PS94] Alexander Polishchuk and Daniel A. Spielman. *Nearly-linear size holographic proofs*. In Frank Thomson Leighton and Michael T. Goodrich, eds., *Proc. 26th ACM Symp. on Theory of Computing (STOC)*, pages 194–203. 1994. 3, 5, 6, 14

[RS96] Ronitt Rubinfeld and Madhu Sudan. *Robust characterizations of polynomials with applications to program testing*. SIAM J. Comput., 25(2):252–271, April 1996. (Preliminary version in *23rd STOC*, 1991 and *3rd SODA*, 1992). 3

[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 Frank Thomson Leighton and Peter W. Shor, eds., *Proc. 29th ACM Symp. on Theory of Computing (STOC)*, pages 475–484. 1997. 3, 4

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il