Electronic Colloquium on Computational Complexity, Report No. 204 (2016)

Robust Multiplication-based Tests for Reed-Muller Codes*

Prahladh Harsha† Srikanth Srinivasan‡

December 20, 2016

Abstract

We consider the following multiplication-based tests to check if a given function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is the evaluation of a degree-d polynomial over $\mathbb{F}_q$ for q prime.

- $\text{Test}_{e,k}$: Pick $P_1, \ldots, P_k$ independent random degree-e polynomials and accept iff the function $fP_1 \cdots P_k$ is the evaluation of a degree-$(d + ek)$ polynomial.

We prove the robust soundness of the above tests for large values of e, answering a question of Dinur and Guruswami (FOCS 2013). Previous soundness analyses of these tests were known only for the case when either $e = 1$ or $k = 1$. Even for the case $k = 1$ and $e > 1$, earlier soundness analyses were not robust.

We also analyze a derandomized version of this test, where (for example) the polynomials $P_1, \ldots, P_k$ can be the *same* random polynomial P. This generalizes a result of Guruswami *et al.* (STOC 2014).

One of the key ingredients that go into the proof of this robust soundness is an extension of the standard Schwartz-Zippel lemma over general finite fields $\mathbb{F}_q$, which may be of independent interest.

1 Introduction

We consider the problem of testing if a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is close to a degree-d multivariate polynomial (over $\mathbb{F}_q$, the finite field of q elements). This problem, in its local testing version, was first studied by Alon, Kaufman, Krivilevich, Litsyn and Ron [AKK+05], who proposed and analyzed a natural 2^{d+1}-query test for this problem for the case when $q = 2$. Subsequent to this work, improved analyses and generalizations to larger fields were discovered [KR06, BKS+10, HSS13]. These tests and their analyses led to several applications, especially in hardness of approximation, which in turn spurred other Reed-Muller testing results (which were not necessarily local tests) [DG15, GHH+14]. In this work, we give a robust version of one of these latter multiplication based tests due to Dinur and Guruswami [DG15]. Below we describe this variation of the testing problem, its context, and our results.

1.1 Local Reed-Muller tests

Given a field $\mathbb{F}_q$ of size q, let $\mathcal{F}_q(n) := \{f \mid f : \mathbb{F}_q^n \to \mathbb{F}_q\}$. The Reed-Muller code $\mathcal{P}_q(n, d)$, parametrized by two parameters n and d, is the subset of $\mathcal{F}_q(n)$ that corresponds to those functions which are evaluations of

*A preliminary version of this paper appeared in the *Proc. 36th IARCS Conf. on Foundations of Software Technology & Theoretical Computer Science (FSTTCS)*, 2016 [HS16].

†TIFR, Mumbai, India. prahladh@tifr.res.in

‡Department of Mathematics, IIT Bombay, Mumbai, India. srikanth@math.iitb.ac.in

ISSN 1433-8092

polynomials of degree at most d. If n, d and q are clear from context, we let $r := (q-1)n - d$.

The proximity of two functions $f, g \in \mathcal{F}_q(n)$ is measured by the Hamming distance. Specifically, we let $\Delta(f,g)$ denote the absolute Hamming distance between f and g, i.e., $\Delta(f,g) := \#\{x \in \mathbb{F}_q^n \mid f(x) \neq g(x)\}$. For a family of functions $\mathcal{G} \subseteq \mathcal{F}_q(n)$, we let $\Delta(f, \mathcal{G}) := \min\{\Delta(f,g) \mid g \in \mathcal{G}\}$. We say that f is Δ-close to $\mathcal{G}$ if $\Delta(f,\mathcal{G}) \leq \Delta$ and Δ-far otherwise.

The following natural local test to check membership of a function f in $\mathcal{P}_2(n,d)$ was proposed by Alon *et al.* [AKK+05] for the case when $q = 2$ (and extended by Kaufman and Ron [KR06] to larger q).

- AKKLR Test: Input $f : \mathbb{F}_2^n \to \mathbb{F}_2$
  - Pick a random $d+1$-dimensional affine space A.
  - Accept iff $f|_A \in \mathcal{P}_2(d+1, d)$.

Here, $f|_A$ refers to the restriction of the function f to the affine space A. Bhattacharyya *et al.* [BKS+10] showed the following optimal analysis of this test.

Theorem 1.1 ([AKK+05, BKS+10]). *There exists an absolute constant $\alpha > 0$ such that the following holds. If $f \in \mathcal{F}_2(n)$ is Δ-far from $\mathcal{P}_2(n,d)$ for $\Delta \in \mathbb{N}$, then*

$$\Pr_A[f|_A \notin \mathcal{P}_2(d+1,d)] \geq \min\{\Delta/2^r, \alpha\}.$$

Subsequent to this result, Haramaty, Shpilka and Sudan [HSS13] extended this result to all constant sized fields $\mathbb{F}_q$. These optimal analyses then led to the discovery of the so-called "short code" (aka the low degree long code) due to Barak *et al.* [BGH+15] which has played an important role in several improved hardness of approximation results [DG15, GHH+14, KS14, Var15, Hua15].

1.2 Multiplication-based tests

We now consider the following type of multiplication-based tests to check membership in $\mathcal{P}_q(n,d)$, parametrized by two numbers $e, k \in \mathbb{N}$.

- $\text{Test}_{e,k}$: Input $f : \mathbb{F}_q^n \to \mathbb{F}_q$
  - Pick $P_1, \ldots, P_k \in_R \mathcal{P}_q(n,e)$.
  - Accept iff $fP_1 \cdots P_k \in \mathcal{P}_q(n, d+ek)$.

This tests computes the point-wise product of f with k random degree-e polynomials $P_1, \ldots, P_k$ respectively and checks that the resulting product function $fP_1 \cdots P_k$ is the evaluation of a degree-$(d+ek)$ polynomial. Unlike the previous test, this test is not necessarily a local test.

The key lemma due to Bhattacharyya *et al.* [BKS+10] that led to the optimal analysis in Theorem 1.1 is the following robust analysis of $\text{Test}_{1,1}$.

Lemma 1.2 ([BKS+10]). *Let $f \in \mathcal{F}_2(n)$ be Δ-far from $\mathcal{P}_2(n,d)$ for $\Delta = 2^r/100$. For randomly picked $\ell \in \mathcal{P}_2(n,1)$, we have*

$$\Pr_\ell\left[\Delta(f \cdot \ell, \mathcal{P}_2(n,d+1)) < \beta\Delta\right] = O\left(\frac{1}{2^r}\right),$$

for some absolute constant $\beta > 0$.

Observe that the AKKLR test is equivalent to $\text{Test}_{1,r-1}$ for $r = n - d$. This observation coupled with a simple inductive argument using the above lemma implies Theorem 1.1.

Motivated by questions related to hardness of coloring hypergraphs, Dinur and Guruswami studied the $\text{Test}_{e,1}$ for $e = r/4$ and proved the following result.

Lemma 1.3 ([DG15])**.** *Let $f \in \mathcal{F}_2(n)$ be Δ-far from $\mathcal{P}_2(n,d)$ for $\Delta = 2^r/100$ and let $e = (n-d)/4$. For randomly picked $P \in \mathcal{P}_2(n,e)$, we have*

$$\Pr_P [f \cdot P \in \mathcal{P}_2(n, d+e)] \leq \frac{1}{2^{2^{\Omega(e)}}}.$$

Note that the $\text{Test}_{e,1}$ is not a local test (as is the case with multiplication based tests of the form $\text{Test}_{e,k}$). Furthermore, the above lemma does not give a robust analysis unlike Lemma 1.2. More precisely, the lemma only bounds the probability that the product function $f \cdot P$ is in $\mathcal{P}_2(n, d+e)$, but does not say anything about the probability of $f \cdot P$ being close to $\mathcal{P}_2(n, d+e)$ as in Lemma 1.2. Despite this, this lemma has had several applications, especially towards proving improved inapproximability results for hypergraph colouring [DG15, GHH+14, KS14, Var15, Hua15].

1.3 Our results

Our work is motivated by the question raised at the end of the previous section: can the analysis of the Dinur-Guruswami Lemma be strengthened to yield a robust version of Lemma 1.3? Such a robust version, besides being interesting of its own right, would yield a soundness analysis of the $\text{Test}_{e,k}$ for $k > 1$ (wherein the input function f is multiplied by k degree-e polynomials). This is similar to how Lemma 1.2 was instrumental in proving Theorem 1.1.

We begin by first showing this latter result (ie., the soundness analysis of the $\text{Test}_{e,k}$).

Theorem 1.4 (Soundness of $\text{Test}_{e,k}$)**.** *Let $q, k \in \mathbb{N}$ be constants with q prime and $\varepsilon, \delta \in (0,1)$ be arbitrary constants. Let $n, d, r, \Delta, e \in \mathbb{N}$ be such that $r = (q-1)n - d$, $q^{\varepsilon r} \leq \Delta \leq q^{r/4(q-1)-2}$, and $\delta r \leq e \leq r/4k$. Then, given any $f \in \mathcal{F}_q(n)$ that is Δ-far from $\mathcal{P}_q(n,d)$ and for $P_1, \ldots, P_k$ chosen independently and uniformly at random from $\mathcal{P}_q(n,e)$, we have*

$$\Pr_{P_1,\ldots,P_k} \left[f P_1 P_2 \cdots P_k \in \mathcal{P}_q(n, d+ek) \right] \leq \frac{1}{q^{q^{\Omega(r)}}},$$

where the $\Omega(\cdot)$ above hides a constant depending on $k, q, \delta, \varepsilon$.

Surprisingly, we show that the above theorem (which we had observed is a simple consequence of a robust version of Lemma 1.3), can in fact, be used to prove the following robust version of Lemma 1.3, answering an open question of Dinur and Guruswami [DG15].

Theorem 1.5 (Robust soundness of $\text{Test}_{e,1}$)**.** *Let $q \in \mathbb{N}$ be a constant with q prime and $\varepsilon, \delta \in (0,1)$ be arbitrary constants. Let $n, d, r, \Delta, e \in \mathbb{N}$ be such that $r = (q-1)n - d$, $q^{\varepsilon r} \leq \Delta \leq q^{r/4(q-1)-2}$, and $\delta r \leq e \leq r/8$. Then, there is a $\Delta' = q^{\Omega(r)}$ such that given any $f \in \mathcal{F}_q(n)$ that is Δ-far from $\mathcal{P}_q(n,d)$ and for P chosen uniformly at random from $\mathcal{P}_q(n,e)$, we have*

$$\Pr_P \left[\Delta(f \cdot P, \mathcal{P}_q(n, d+e)) < \Delta' \right] \leq \frac{1}{q^{q^{\Omega(r)}}},$$

where the $\Omega(\cdot)$s above hide constants depending on q, δ, ε.

Equipped with such multiplication-based tests, we can ask if one can prove the soundness analysis of other related multiplication-based tests. For instance, consider the following test which checks correlation of the function f with the square of a random degree-e polynomial.

- Corr-Square$_e$: Input $f : \mathbb{F}_3^n \to \mathbb{F}_3$
  - Pick $P \in_R \mathcal{P}_3(n, e)$.
  - Accept iff $f \cdot P^2 \in \mathcal{P}_3(n, d + 2e)$.

This test was used by Guruswami *et al.* [GHH+14] to prove the hardness of approximately coloring 3-colorable 3-uniform hypergraphs. However, their analysis was restricted to the squares of random polynomials. Our next result shows that this can be extended to any low-degree polynomial of random polynomials. More precisely, let $h \in \mathcal{P}_q(1, k)$ be a *univariate* polynomial of degree exactly k for some $k < q$. Consider the following test.

- Corr-h_e: Input $f : \mathbb{F}_q^n \to \mathbb{F}_q$
  - Pick $P \in_R \mathcal{P}_q(n, e)$.
  - Accept iff $f \cdot h(P) \in \mathcal{P}_q(n, d + ek)$.

We show that an easy corollary of Theorem 1.4 proves the following soundness claim about the test Corr-h.

Corollary 1.6 (Soundness of Corr-h_e)**.** *Let $q, k \in \mathbb{N}$ be constants with q prime, $k < q$, and let $\varepsilon, \delta \in (0, 1)$ be arbitrary constants.*[1] *Let $n, d, r, \Delta, e \in \mathbb{N}$ be such that $r = (q-1)n - d$, $q^{\varepsilon r} \le \Delta \le q^{r/4(q-1)-2}$, and $\delta r \le e \le r/4k$. Let $h \in \mathcal{P}_q(1, k)$ be a univariate polynomial of degree exactly k. Then, given any $f \in \mathcal{F}_q(n)$ that is Δ-far from $\mathcal{P}_q(n, d)$ and for P chosen uniformly at random from $\mathcal{P}_q(n, e)$, we have*

$$\Pr_P \left[f \cdot h(P) \in \mathcal{P}_q(n, d + ek) \right] \le \frac{1}{q^{q^{\Omega(r)}/2^k}},$$

where the $\Omega(\cdot)$ above hides a constant depending on $k, q, \delta, \varepsilon$.

A generalization of the Schwartz-Zippel lemma over $\mathbb{F}_q$. A special case of Theorem 1.4 is already quite interesting. This case corresponds to when the function f is a polynomial of degree exactly d', for some d' slightly larger than d. (It is quite easy to see by the Schwartz-Zippel lemma over $\mathbb{F}_q$ — which guarantees that a non-zero polynomial of low degree is non-zero at many points — that this f is far from $\mathcal{P}_q(n, d)$.) In this case, we would expect that when we multiply f with k random polynomials $P_1, \ldots, P_k \in \mathcal{P}_q(n, e)$, that the product $f P_1 \cdots P_k$ is a polynomial of degree exactly $d' + ek$ and hence not in $\mathcal{P}_q(n, d + ek)$ with high probability.

We are able to prove a tight version of this statement (Lemma 3.3). For every degree d', we find a polynomial f of degree exactly d' that maximizes the probability that $f P_1$ has degree $< d' + s$ for any parameter $s \le e$. This polynomial turns out to be the same polynomial for which the Schwartz-Zippel lemma over $\mathbb{F}_q$ is tight. This is not a coincidence: it turns out that our lemma is a generalization of the Schwartz-Zippel lemma over $\mathbb{F}_q$ (see Section 3.1).

Given the utility of the Schwartz-Zippel lemma in Theoretical Computer Science, we think this statement may be of independent interest.

[1] The assumption $k < q$ is necessary here since otherwise $h(P)$ could be $P^q - P$, which is always 0.

1.4 Proof ideas

The basic outline of the proof of Theorem 1.4 is similar to the proof of Lemma 1.3 from the work of Dinur and Guruswami [DG15] which corresponds to Theorem 1.4 in the case that $q = 2$ and $k = 1$. We describe this argument in some detail so that we can highlight the variations in our work.

The argument is essentially an induction on the parameters $e, r = n - d$, and Δ. As long as r is a sufficiently large constant, Lemma 1.2 can be used [DG15, Lemma 22] to show that for any $f \in \mathcal{F}_2(n)$ that is Δ-far from $\mathcal{P}_2(n, d)$, there is a variable X such that for each $\alpha \in \{0, 1\} = \mathbb{F}_2$, the restricted function $f|_{X=\alpha}$ is $\Delta' = \Omega(\Delta)$-far from $\mathcal{P}_2(n - 1, d)$.[2]

Now, to argue by induction, we write

$$f = Xg + h \text{ and } P_1 = XQ_1 + R_1 \tag{1}$$

where g, h, Q_1, R_1 depend on $n - 1$ variables, Q_1 is a random polynomial of degree $\leq e - 1$ and R_1 is a random polynomial of degree $\leq e$. Using the fact that $X^2 = X$ over $\mathbb{F}_2$, we get $fP_1 = X((g + h)Q_1 + gR_1) + hR_1$.

Since $f|_{X=\alpha}$ is Δ'-far from $\mathcal{P}_2(n - 1, d)$, we see that both h and $g + h$ are Δ'-far from $\mathcal{P}_2(n - 1, d)$. To apply induction, we note that $fP_1 \in \mathcal{P}_2(n, d + e)$ iff $hR_1 \in \mathcal{P}_2(n - 1, d + e)$ and $(g + h)Q_1 + hR_1 \in \mathcal{P}_2(n - 1, d + e - 1)$; we call these events $\mathcal{E}_1$ and $\mathcal{E}_2$ respectively. We bound the overall probability by $\Pr[\mathcal{E}_1] \cdot \Pr[\mathcal{E}_2 \mid R_1]$ (note that $\mathcal{E}_1$ depends only on R_1).

We first observe that $\Pr[\mathcal{E}_1]$ can be immediately bounded using the induction hypothesis since h is Δ'-far from $\mathcal{P}_q(n - 1, d + e)$ and R_1 is uniform over $\mathcal{P}_q(n - 1, e)$. The second term $\Pr[\mathcal{E}_2 \mid R_1]$ can also be bounded by the induction hypothesis with the following additional argument. We argue that (for any fixed R_1) the probability that $(g + h)Q_1 + gR_1 \in \mathcal{P}_2(n - 1, d + e - 1)$ is bounded by the probability that $(g + h)Q_1 \in \mathcal{P}_2(n - 1, d + e - 1)$: this follows from the fact that the number of solutions to any system of linear equations is bounded by the number of solutions of the corresponding homogeneous system (obtained by setting the constant term in each equation to 0). Hence, it suffices to bound the probability that $(g + h)Q_1 \in \mathcal{P}_2(n - 1, d + e - 1)$, which can be bounded by the induction hypothesis since $(g + h)$ is Δ'-far from $\mathcal{P}_2(n - 1, d)$ and Q_1 is uniform over $\mathcal{P}_2(n - 1, e - 1)$ and we are done.

Though our proofs follow the above template, we need to deviate from the proof above in some important ways which we elaborate below.

The first is the decomposition of f and P_1 from (1) obtained above, which yields two events $\mathcal{E}_1$ and $\mathcal{E}_2$, the first of which depends only on R_1 and the second on both Q_1 and R_1. For $q > 2$, the standard monomial decomposition of polynomials does not yield such a nice "upper triangular" sequence of events. So we work with a different polynomial basis to achieve this. This choice of basis is closely related to the polynomials for which the Schwartz-Zippel lemma over $\mathbb{F}_q$ is tight. While such a basis was used in the special case of $q = 3$ in the work of Guruswami *et al.* [GHH+14] (co-authored by the authors of this work), it was done in a somewhat ad-hoc way. Here, we give, what is in our opinion a more transparent construction that additionally works for all q.

Further modifications to the Dinur-Guruswami argument are required to handle $k > 1$. We illustrate this with the example of $q = 2$ and $k = 2$. Decomposing as in the Dinur-Guruswami argument above, we obtain

[2] Actually, Lemma 1.2 implies the existence of a linear function with this property and not a variable. But after a linear transformation of the underlying space, we may assume that it is a variable.

$f = Xg + h$, $P_1 = XQ_1 + R_1$, and $P_2 = XQ_2 + R_2$. Multiplying out, we get

$$fP_1P_2 = X(\underbrace{Q_1Q_2(g+h) + (g+h)(Q_1R_2 + Q_2R_1) + gR_1R_2}_{:=Q}) + hR_1R_2 \ .$$

Bounding the probability that $fP_1P_2 \in \mathcal{P}_2(n, d+2e)$ thus reduces to bounding the probability of event that $hR_1R_2 \in \mathcal{P}_2(n-1, d+2e)$ — $\mathcal{E}_1$ depending only on R_1 and R_2 — and then the probability that $Q \in \mathcal{P}_2(n-1, d+2e-1)$ — denoted $\mathcal{E}_2$ — given any fixed R_1 and R_2. The former probability can be bounded using the induction hypothesis straightforwardly.

By a reasoning similar to the $k = 1$ case, we can reduce bounding $\Pr[\mathcal{E}_2 \mid R_1, R_2]$ to the probability that $Q_1Q_2(g+h) \in \mathcal{P}_2(n-1, d+2e-1)$. However, now we face a problem. Note that we have $g + h = f|_{X=1}$ is Δ'-far from $\mathcal{P}_2(n-1, d)$ and $Q_1, Q_2 \in \mathcal{P}_2(n-1, e-1)$. Thus, the induction hypothesis only allows us to upper bound the probability that $Q_1Q_2(g+h) \in \mathcal{P}_2(n-1, d+2e-2)$ which is not quite the event that we want to analyze. Indeed, if f is a polynomial of degree exactly $d+1$, then the polynomial $Q_1Q_2(g+h) \in \mathcal{P}_2(n-1, d+2e-1)$ with probability 1. A similar problem occurs even if f is a polynomial of degree d' slightly larger than d or more generally, when f is *close* to some polynomial of degree d'.

This naturally forces us to break the analysis into two cases. In the first case, we assume not just that f is far from $\mathcal{P}_2(n, d)$ but also from $\mathcal{P}_2(n, d')$ but for some d' a suitable parameter larger than d. In this case, we can modify the proof of Dinur and Guruswami to bound the probability that $fP_1P_2 \in \mathcal{P}_2(n, d+2e)$ as claimed in Theorem 1.4. In the complementary case when f is close to some polynomial $F \in \mathcal{P}_2(n, d')$, we can essentially assume that f *is* a polynomial of degree exactly d'. In this case, we can use the extension of Schwartz-Zippel lemma referred to above to show that with high probability fP_1P_2 is in fact a polynomial of degree exactly $d' + 2e$ and is hence not of degree $d + 2e < d' + 2e$.

1.5 Organization

We begin with some notation and definitions in Section 2. We prove the extension of the Schwartz-Zippel lemma (Lemma 3.3) in Section 3 and then Theorem 1.4 in Section 4. Finally, we give two applications of Theorem 1.4 in Section 5: one to proving a robust version of the above test (thus resolving a question of Dinur and Guruswami [DG15]) and the other to proving Corollary 1.6.

2 Preliminaries

For a prime power q, let $\mathbb{F}_q$ denote the finite field of size q. We use $\mathbb{F}_q[X_1, \ldots, X_n]$ to denote the standard polynomial ring over variables $X_1, \ldots, X_n$ and $\mathcal{P}_q(n)$ to denote the ring $\mathbb{F}_q[X_1, \ldots, X_n] / \langle X_1^q - X_1, \ldots, X_n^q - X_n \rangle$.

We can think of the elements of $\mathcal{P}_q(n)$ as elements of $\mathbb{F}_q[X_1, \ldots, X_n]$ of individual degree at most $q-1$ in a natural way. Given $P, Q \in \mathcal{P}_q(n)$, we use $P \cdot Q$ or PQ to denote their product in $\mathcal{P}_q(n)$. We use $P * Q$ to denote their product in $\mathbb{F}_q[X_1, \ldots, X_n]$.

Given a set $S \subseteq \mathbb{F}_q^n$ and an $f \in \mathcal{P}_q(n)$, we use $f|_S$ to denote the restricted function on the set S. Typically, S will be specified by a polynomial equation. One special case is the case when S is a hyperplane: i.e., there is a non-zero homogeneous degree-1 polynomial $\ell(X) \in \mathcal{P}_q(n)$ and an $\alpha \in \mathbb{F}_q$ such that $S = \{x \mid \ell(x) = \alpha\}$. In this case, it is natural to think of $f|_{\ell(X)=\alpha} = f|_S$ as an element of $\mathcal{P}_q(n-1)$ by applying a linear transformation that transforms $\ell(X)$ into the variable X_n and then setting $X_n = \alpha$.

For $d \geq 0$, we use $\mathcal{P}_q(n,d)$ to denote the polynomials in $\mathcal{P}_q(n)$ of degree at most d.

The following are standard facts about the ring $\mathcal{P}_q(n)$ and the space of functions mapping $\mathbb{F}_q^n$ to $\mathbb{F}_q$.

Fact 2.1.
1. *Consider the ring of functions mapping $\mathbb{F}_q^n$ to $\mathbb{F}_q$ with addition and multiplication defined pointwise. This ring is isomorphic to $\mathcal{P}_q(n)$ under the natural isomorphism that maps each polynomial $P \in \mathcal{P}_q(n)$ to the function (mapping $\mathbb{F}_q^n$ to $\mathbb{F}_q$) represented by this polynomial.*

2. *In particular, each function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ can be represented uniquely as a polynomial from $\mathcal{P}_q(n)$. As a further special case, any non-zero polynomial from $\mathcal{P}_q(n)$ represents a non-zero function $f : \mathbb{F}_q^n \to \mathbb{F}_q$.*

3. *(Schwartz-Zippel lemma over $\mathbb{F}_q$ [KLP68]) Any non-zero polynomial from $\mathcal{P}_q(n,d)$ is non-zero on at least $q^{n-a-1}(q-b)$ points from $\mathbb{F}_q^n$ where $d = a(q-1)+b$ and $0 \leq b < q-1$.*

4. *In particular, if $f, g \in \mathcal{P}_q(n,d)$ differ from each other at at most $\Delta < q^{n-a-1}(q-b)$ points, then $f = g$.*

5. *(A probabilistic version of the Schwartz-Zippel lemma (see, e.g., [HSS13])) It follows from the above that given a non-zero polynomial $g \in \mathcal{P}_q(n,d)$, then $g(x) \neq 0$ at a uniformly random point of $\mathbb{F}_q^n$ with probability at least $q^{-d/(q-1)}$. Similarly, if $f, g \in \mathcal{P}_q(n,d)$ are distinct, then for uniformly random $x \in \mathbb{F}_q^n$, the probability that $f(x) \neq g(x)$ is at least $q^{-d/(q-1)}$.*

From now on, we will use without additional comment the fact that functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ have unique representations as multivariate polynomials where the individual degrees are bounded by $q-1$.

Recall that $m_1 * m_2$ denotes the product of these monomials in the ring $\mathbb{F}_q[X_1,\ldots,X_n]$ while $m_1 \cdot m_2$ denotes their product in $\mathcal{P}_q(n) = \mathbb{F}_q[X_1,\ldots,X_n]/\langle X_1^q - X_1, \ldots, X_n^q - X_n\rangle$. We say that monomials $m_1, m_2 \in \mathcal{P}_q(n)$ are *disjoint* if $m_1 * m_2 = m_1 \cdot m_2$ (where the latter monomial is interpreted naturally as an element of $\mathbb{F}_q[X_1,\ldots,X_n]$). Equivalently, for each variable X_i ($i \in [n]$), the sum of its degrees in m_1 and m_2 is less than q.

Given distinct monomials $m_1, m_2 \in \mathbb{F}_q[X_1,\ldots,X_n]$, we say that $m_1 > m_2$ if either one of the following holds: $\deg(m_1) > \deg(m_2)$, or $\deg(m_1) = \deg(m_2)$ and we have $m_1 = \prod_i X_i^{e_i}$ and $m_2 = \prod_i X_i^{e_i'}$ where for the least j such that $e_j \neq e_j'$, we have $e_j > e_j'$.

The above is called the *graded lexicographic* order on monomials [CLO15]. This ordering obviously restricts to an ordering on the monomials in $\mathcal{P}_q(n)$, which are naturally identified as a subset of the monomials of $\mathbb{F}_q[X_1,\ldots,X_n]$. The well-known fact about this monomial ordering we will use is the following.

Fact 2.2 ([CLO15])**.** *For any monomials m_1, m_2, m_3, we have $m_1 \leq m_2 \Rightarrow m_1 * m_3 \leq m_2 * m_3$.*

Given an $f \in \mathcal{P}_q(n)$, we use $\mathrm{Supp}(f)$ to denote the set of points $x \in \mathbb{F}_q^n$ such that $f(x) \neq 0$. If $f \neq 0$, we use $\mathrm{LM}(f)$ to denote the largest monomial (w.r.t. ordering defined above) with non-zero coefficient in f.

Let $m = \prod_{i\in[n]} X_i^{e_i}$ with $e_i < q$ for each i and let $d = \deg(m)$. For an integer $s \geq 0$, we let

$$U_s(m) := \{\prod_{j\in[n]} X_j^{e_j'} \mid \sum_j e_j' = d+s \text{ and } \forall j\; q > e_j' \geq e_j, \},$$

$$D_s(m) := \{\prod_{j\in[n]} X_j^{e_j'} \mid \sum_j e_j' = s \text{ and } \forall j\; e_j' + e_j < q\}.$$

Note that the monomials in $D_s(m)$ are precisely the monomials of degree s that are disjoint from m. Further, the map $\rho : D_s(m) \to U_s(m)$ defined by $\rho(m_1) = m_1 \cdot m$ defines a bijection between $D_s(m)$ and $U_s(m)$, and hence we have

Fact 2.3. *For any monomial m and any $s \geq 0$, $|U_s(m)| = |D_s(m)|$.*

For non-negative integers $s \leq e$, we define $U_{s,e}(m) := \bigcup_{s \leq t \leq e} U_t(m)$ and $D_{s,e}(m) := \bigcup_{s \leq t \leq e} D_t(m)$. Since $|U_t(m)| = |D_t(m)|$ for each t, we have $|U_{s,e}(m)| = |D_{s,e}(m)|$.

2.1 A different basis for $\mathcal{P}_q(n)$

Applying Fact 2.1 in the case that $n = 1$, it follows that the monomials $\{X^i \mid 0 \leq i < q\}$ form a natural basis for the space of all functions from $\mathbb{F}_q$ to $\mathbb{F}_q$. The following is another such basis which is sometimes more suitable for our purposes.

Definition 2.4 (A suitable basis for the space of functions from $\mathbb{F}_q$ to $\mathbb{F}_q$)**.** *Fix a linear ordering $\preceq$ of all the elements of $\mathbb{F}_q$. Let $\xi_0, \ldots, \xi_{q-1}$ be the elements of $\mathbb{F}_q$ according to this ordering. For any $i \in \{0, \ldots, q-1\}$, let $b_i^{\preceq}(X) = \prod_{j<i}(X - \xi_j)$. Note that for $i < q$, $b_i^{\preceq}(X)$ is a non-zero polynomial of degree i. In particular, $\{b_i^{\preceq}(X) \mid 0 \leq i < q\}$ is a basis for the space of all functions from $\mathbb{F}_q$ to $\mathbb{F}_q$. Usually, when we apply this definition, the ordering $\preceq$ will be implicitly clear and hence we will use $b_i(X)$ to refer to $b_i^{\preceq}(X)$.*

The following property of this basis will be useful.

Lemma 2.5. *Fix any ordering $\preceq$ of $\mathbb{F}_q$ and let $\{b_i(X) \mid 0 \leq i < q\}$ be the corresponding basis as in Definition 2.4. Then, for any $f : \mathbb{F}_q \to \mathbb{F}_q$ and $i \in \{0, \ldots, q-1\}$, we have $f(X) \cdot b_i(X) = f(\xi_i)b_i(X) + b_i'(X)$ where $b_i'(x) \in$* span$\{b_{i+1}(X), \ldots, b_{q-1}(X)\}$.

Proof. We know that $f(X)$ is a polynomial of degree at most $q-1$ in X. By linearity, it suffices to prove the lemma for $f(X) = X^k$ for $0 \leq k \leq q-1$. We prove this by induction on k. The base case ($k = 0$) of the induction is trivial. We also handle the case $k = 1$ by noting that

$$X \cdot b_i(X) = \xi_i b_i(X) + (X - \xi_i)b_i(X) = \xi_i b_i(X) + b_{i+1}(X)$$

which has the required form.

Now consider $k \in \{2, \ldots, q-1\}$. By the induction hypothesis, we know that $X^{k-1} \cdot b_i(X) = \xi_i^{k-1} b_i(X) + b_i'(X)$ where $b_i'(X) \in \text{span}\{b_{i+1}(X), \ldots, b_{q-1}(X)\}$. Hence, we see that $X^k \cdot b_i(X) = X \cdot \xi_i^{k-1} b_i(X) + X b_i'(X) = (X - \xi_i + \xi_i) \cdot \xi_i^{k-1} b_i(X) + X b_i'(X)$. Expanding we obtain

$$X^k \cdot b_i(X) = \xi_i^k b_i(X) + (X - \xi_i)b_i(X) + X b_i'(X) = \xi_i^k b_i(X) + b_{i+1}(X) + X b_i'(X) = \xi_i^k b_i(X) + b_i''(X)$$

where $b_i''(X) \in \text{span}\{b_{i+1}(X), \ldots, b_{q-1}(X)\}$ by using the fact that $X b_i'(X) \in \text{span}\{b_{i+1}(X), \ldots, b_{q-1}(X)\}$, which follows from the case $k = 1$. This proves the induction statement and hence also the lemma. $\square$

We now consider functions $f : \mathbb{F}_q^n \to \mathbb{F}_q$ over n variables $X_1, \ldots, X_n$. As noted above, this space of functions is ring isomorphic to $\mathcal{P}_q(n)$. We will use an alternate basis for this space also.

We fix an ordering $\preceq$ of $\mathbb{F}_q$ and let $\{b_i(X_j) \mid 0 \leq i < q\}$ be the corresponding basis in the variable X_j. We refer to functions of the form $\prod_{j \in [n]} b_{i_j}(X_j)$ as *generalized monomials* w.r.t. $\preceq$: we call this set $\mathcal{B}_q(n)$ (the orderings will be implicit). The *degree* of the monomial $\prod_{j\in[n]} b_{i_j}(X_j)$ is $\sum_{j\in[n]} i_j$. Given a degree parameter $d \in \mathbb{N}$, we let $\mathcal{B}_q(n,d)$ denote the set of all monomials in $\mathcal{B}_q(n)$ of degree at most d.

The following fact is easily proved.

Fact 2.6.

1. *For any $n,d \in \mathbb{N}$, the set $\mathcal{B}_q(n,d)$ is a basis for the space of polynomials in $\mathcal{P}_q(n,d)$.*
2. *In particular, the set $\mathcal{B}_q(n) = \mathcal{B}_q(n,(q-1)n)$ is a basis for $\mathcal{P}_q(n)$.*

What makes the above basis useful is the following lemma.

Lemma 2.7. *Fix any ordering $\xi_0,\ldots,\xi_{q-1}$ of $\mathbb{F}_q$ and let $b_i(X)$ $(0 \le i \le q-1)$ be the corresponding basis. Given any $f \in \mathcal{P}_q(n)$ and any $P \in \mathcal{P}_q(n,d)$, we may write the function $f \cdot P \in \mathcal{P}_q(n)$ as*

$$fP = \sum_{k=0}^{q-1} b_k(X_n)\left(Q_k \cdot f|_{X_n=\xi_k} + \sum_{0\le j<k} Q_j \cdot h_{j,k}\right)$$

where $P = \sum_{k=0}^{q-1} b_k(X_n)Q_k(X_1,\ldots,X_{n-1})$, and $h_{j,k}(X_1,\ldots,X_{n-1}) \in \mathcal{P}_q(n-1)$.

Remark 2.8. *The above statement encapsulates the advantage of working with the basis from Definition 2.4. Note that the coefficient of $b_k(X_n)$ only involves $Q_i(X_1,\ldots,X_{n-1})$ for $i \le k$. This gives us an "upper triangular" decomposition of the polynomial fP that we will find useful.*

Proof. By Fact 2.6 point 1, we can write $f = \sum_{i=0}^{q-1} b_i(X_n) f_i(X_1,\ldots,X_{n-1})$. Expanding fP, we get

$$\begin{aligned} fP &= \sum_{i,j\in\{0,\ldots,q-1\}} b_i(X_n)b_j(X_n)f_iQ_j \\ (\text{by Lemma 2.5}) &= \sum_{i,j} f_iQ_j \cdot \left(b_i(\xi_j)b_j(X_n) + \sum_{k>j} \alpha_{i,j,k} b_k(X_n)\right) \\ &= \sum_{k=0}^{q-1} b_k(X_n)\left(Q_k \sum_i f_i b_i(\xi_k) + \sum_{j<k,i} \alpha_{i,j,k} f_i Q_j\right) \\ &= \sum_{k=0}^{q-1} b_k(X_n)\left(Q_k f|_{X_n=\xi_k} + \sum_{j<k} Q_j \cdot h_{j,k}\right), \end{aligned}$$

where $h_{j,k} := \sum_i \alpha_{i,j,k} f_i$. □

We will also need to analyze the product of many polynomials in the above basis, for which we use the following.

Lemma 2.9. *Say $P_1,\ldots,P_k \in \mathcal{P}_q(n,d)$ with $P_i = \sum_{j=0}^{q-1} b_j(X_n)Q_{i,j}(X_1,\ldots,X_{n-1})$. Let $P = \prod_{i=1}^k P_i = \sum_{j=0}^{q-1} b_j(X_n)Q_j(X_1,\ldots,X_{n-1})$. Given $j_1,\ldots,j_k \in \{0,\ldots,q-1\}$, we say that $(j_1,\ldots,j_k) \le j$ if $j_i \le j$ for each $i \in [k]$ and $(j_1,\ldots,j_k) < j$ if $j_i \le j$ for each $i \in [k]$* and *there is some i such that $j_i < j$. Also, let $Q_{(j_1,\ldots,j_k)}$ denote $\prod_{i\in[k]} Q_{i,j_i}$.*

For each $j \in \{0, \ldots, q-1\}$, we have

$$Q_j = \sum_{(j_1,\ldots,j_k)\leq j} \beta^{(j)}_{(j_1,\ldots,j_k)} Q_{(j_1,\ldots,j_k)},$$

where $\beta^{(j)}_{(j_1,\ldots,j_k)} \in \mathbb{F}_q$ and further $\beta^{(j)}_{(j,\ldots,j)} \neq 0$.

Proof. We prove the lemma by induction on k. The base case $k = 1$ is trivial since we can take $\beta^{(j)}_{(j_1)} = 1$ if $j_1 = j$ and 0 otherwise.

Now, consider the inductive case $k > 1$. For $\tilde{P} = \prod_{i<k} P_i$, we have the above claim, which yields

$$\tilde{Q}_j = \sum_{(j_1,\ldots,j_{k-1})\leq j} \tilde{\beta}^{(j)}_{(j_1,\ldots,j_{k-1})} Q_{(j_1,\ldots,j_{k-1})},$$

where $\tilde{P} = \sum_j b_j(X_n)\tilde{Q}_j$. Also, $\tilde{\beta}^{(j)}_{(j,j,\ldots,j)} \neq 0$.

To prove the inductive claim, we expand $P = \prod_i P_i = \tilde{P}P_k$ and use Lemma 2.5. The computation is as follows.

$$\begin{aligned} P = \tilde{P}P_k &= \left(\sum_j b_j(X_n)\tilde{Q}_j\right) \cdot \left(\sum_{\ell=0}^{q-1} b_\ell(X_n)Q_\ell\right) \\ &= \sum_{j,\ell} \tilde{Q}_j Q_\ell b_j(X_n) b_\ell(X_n). \end{aligned} \tag{2}$$

By Lemma 2.5, it follows that

$$b_j(X_n)b_\ell(X_n) = \sum_{r\geq(j,\ell)} \gamma^{(r)}_{(j,\ell)} b_r(X_n),$$

where $\gamma^{(r)}_{(j,\ell)} \in \mathbb{F}_q$ for each $(j,\ell) \leq r$ and in particular $\gamma^{(r)}_{(r,r)} = b_r(\xi_r) \neq 0$. Substituting in (2) we get

$$\begin{aligned} P &= \sum_{j,\ell} \tilde{Q}_j Q_\ell \sum_{r\geq(j,\ell)} \gamma^{(r)}_{(j,\ell)} b_r(X_n) \\ &= \sum_r b_r(X_n) \sum_{(j,\ell)\leq r} \gamma^{(r)}_{(j,\ell)} \tilde{Q}_j Q_\ell \\ \text{(by Induction Hypothesis)} \quad &= \sum_r b_r(X_n) \sum_{(j,\ell)\leq r} \gamma^{(r)}_{(j,\ell)} Q_\ell \sum_{(j_1,\ldots,j_{k-1})\leq j} \tilde{\beta}^{(j)}_{(j_1,\ldots,j_{k-1})} Q_{(j_1,\ldots,j_{k-1})} \\ &= \sum_r b_r(X_n) \sum_{(j_1,\ldots,j_{k-1},\ell)\leq r} \beta^{(r)}_{(j_1,\ldots,j_{k-1},\ell)} Q_{(j_1,\ldots,j_{k-1},\ell)}, \end{aligned}$$

where

$$\beta^{(r)}_{(j_1,\ldots,j_{k-1},\ell)} = \sum_{j\geq(j_1,\ldots,j_{k-1}),j\leq r} \gamma^{(r)}_{(j,\ell)} \tilde{\beta}^{(j)}_{(j_1,\ldots,j_{k-1})}.$$

In particular, $\beta^{(r)}_{(r,\ldots,r)} = \gamma^{(r)}_{(r,r)} \tilde{\beta}^{(r)}_{(r,\ldots,r)} \neq 0$ since we showed that $\gamma^{(r)}_{(r,r)} \neq 0$ above and $\tilde{\beta}^{(r)}_{(r,\ldots,r)} \neq 0$ by the Induction Hypothesis. $\square$

2.2 Multilinear and set-multilinear systems of equations

Fix any set $\mathcal{Z}$ of variables and say we have a partition $\Pi = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_k\}$ of $\mathcal{Z}$. A polynomial $P \in \mathbb{F}_q[\mathcal{Z}]$ is Π-*set-multilinear* (or just *set-multilinear* if Π is clear from context) if every monomial appearing in P involves exactly one variable from each $\mathcal{Z}_i$ ($i \in [k]$). The polynomial P is Π-multilinear if every monomial involves *at most* one variable from each $\mathcal{Z}_i$ ($i \in [k]$). Note that a Π-set-multilinear polynomial is homogeneous of degree k and a Π-multilinear polynomial has degree at most k.

Given a Π as above and a Π-multilinear polynomial P, its homogeneous degree k component is a Π-set-multilinear polynomial Q. We call Q the *set-multilinear part* of P.

Lemma 2.10. *Fix any set $\mathcal{Z} = \{Z_1, \ldots, Z_N\}$ of variables and a partition $\Pi = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_k\}$ of $\mathcal{Z}$. Let $P_1, \ldots, P_m$ be any set of Π-multilinear polynomials with set-multilinear parts $Q_1, \ldots, Q_m$ respectively. Then, we have*

$$\Pr_{z \sim \mathbb{F}_q^N}\left[P_1(z) = 0 \wedge \cdots \wedge P_m(z) = 0\right] \leq \Pr_{z \sim \mathbb{F}_q^N}\left[Q_1(z) = 0 \wedge \cdots \wedge Q_m(z) = 0\right].$$

The above lemma generalizes the well-known fact that a system of (inhomogeneous) linear equations has at most as many solutions as the corresponding *homogeneous* system of linear equations obtained by setting the constant term in each equation to 0.

Proof. The proof uses the above fact about the number of solutions for systems of linear equations. Consider the following systems of multilinear polynomial equations. For $j \in \{0, \ldots, k\}$ and $i \in [m]$, define $P_{j,i}$ as follows: $P_{0,i} = P_i$ and given $P_{j,i}$ for $j < k$, we define $P_{j+1,i}$ by dropping all monomials from $P_{j,i}$ that do *not* involve the variables from $\mathcal{Z}_{j+1}$. In particular, we see that $P_{k,i} = Q_i$ for each $i \in [m]$.

We claim that for each $j < k$ we have

$$\Pr_{z \sim \mathbb{F}_2^N}\left[\bigwedge_{i \in [m]} P_{j,i}(z) = 0\right] \leq \Pr_{z \sim \mathbb{F}_2^N}\left[\bigwedge_{i \in [m]} P_{j+1,i}(z) = 0\right]. \tag{3}$$

The above clearly implies the lemma.

To show that (3) holds, we argue as follows. Fix any assignment to all the variables in $\mathcal{Z} \setminus \mathcal{Z}_{j+1}$. For each such assignment, the event on the Left Hand Side of (3) is the event that a system of m linear equations $\mathcal{L}$ in $\mathcal{Z}_{j+1}$ is satisfied by a uniformly random assignment to $\mathcal{Z}_{j+1}$: this follows since each $P_{j,i}$ is a multilinear polynomial w.r.t. Π. On the Right Hand Side, we have the event that some other system $\mathcal{L}'$ of m linear equations is satisfied. By inspection, it can be verified that $\mathcal{L}'$ is the homogeneous version of $\mathcal{L}$: i.e., each equation in $\mathcal{L}'$ is obtained by zeroing the constant term of the corresponding equation in $\mathcal{L}$. By standard linear algebra, $\mathcal{L}'$ has at least as many solutions as $\mathcal{L}$. Hence, the probability that a random assignment to the variables in $\mathcal{Z}_{j+1}$ satisfies $\mathcal{L}'$ is at least the probability that a random assignment satisfies $\mathcal{L}$. This implies (3). □

2.3 A result of Haramaty, Shpilka, and Sudan

The following is an easy corollary of a result from the work of Haramaty, Shpilka, and Sudan [HSS13]. Analogous corollaries have been observed before by Dinur and Guruswami [DG15] (using [BKS+10]) and Guruswami *et al.* [GHH+14].

Lemma 2.11. *Let q be any constant prime. There is a constant $c_q > q$ depending only on q such that the following holds. Let n, d, Δ, r be non-negative integers with $d < (q-1)n$, $r := (q-1)n - d$, $q^5 < \Delta < q^{r/(q-1)}$, and $r \geq c_q$. Then, for any $f \in \mathcal{P}_q(n)$ that is Δ-far from $\mathcal{P}_q(n,d)$, there is a non-zero homogeneous linear function $\ell(X_1, \ldots, X_n)$ such that for each $\alpha \in \mathbb{F}_q$, the restriction $f|_{\ell(X)=\alpha}$ is at least Δ/q^3-far from $\mathcal{P}_q(n-1,d)$.*

We need the following theorem due to Haramaty, Shpilka and Sudan [HSS13].

Theorem 2.12 ([HSS13, Theorem 1.7 and 4.16] using absolute distances instead of fractional distances)**.** *For every prime q, there exists a constant λ_q such that the following holds. For $\beta : \mathbb{F}_q^n \to \mathbb{F}_q$, let $A_1, \ldots, A_K$ be hyperplanes such that $\beta|_{A_i}$ is Δ_1-close to some degree d polynomial on A_i. If $K > q^{\lceil \frac{d+1}{q-1} \rceil + \lambda_q}$ and $\Delta_1 < q^{n-d/(q-1)-2}/2$, then $\Delta(\beta, \mathcal{P}_q(n,d)) \leq 2q\Delta_1 + 4(q-1) \cdot q^n/K$.*

Proof of Lemma 2.11. Let $c_q = cq\lambda_q$ where λ_q is the constant from Theorem 2.12 and c is an absolute constant determined below.

Suppose Lemma 2.11 were false with $r \geq c_q$. Then, for every nonzero homogeneous linear function ℓ, at least one of $\{f|_{\ell=\alpha} \mid \alpha \in \mathbb{F}_q\}$ is Δ/q^3-close to a degree d polynomial. We thus, get $K = (q^n-1)/(q-1)$ hyperplanes such that the restriction of f to these hyperplanes is Δ/q^3-close to a degree d polynomial. Observe that $K \geq q^{n-1} > q^{\lceil \frac{d+1}{q-1} \rceil + \lambda_q}$ if $r \geq c_q$ and the constant c is chosen large enough. Also note that since $\Delta < q^{r/(q-1)}$, we have $\Delta/q^3 < q^{(r/(q-1))-3} \leq q^{n-d/(q-1)-2}/2$. Hence, by Theorem 2.12 we have $\Delta(f, \mathcal{P}_q(n,d)) \leq 2\Delta/q^2 + 4 \cdot (q-1)^2 \cdot q^n/(q^n-1) < 2\Delta/q^2 + 8(q-1)^2 < \Delta$ (since $\Delta \geq q^5$). This contradicts the hypothesis that f is Δ-far from $\mathcal{P}_q(n,d)$. $\square$

3 An extension of the Schwartz-Zippel Lemma over $\mathbb{F}_q$

The results of this section hold over $\mathbb{F}_q$ where q is any prime power.

Lemma 3.1. *Let $d, s \geq 0$ be arbitrary integers with $d + s \leq n(q-1)$. Assume $d = (q-1)u + v$ for $u, v \geq 0$ with $v < (q-1)$. Then the monomial $m_0 := X_1^{q-1} \cdots X_u^{q-1} X_{u+1}^v$ of degree d satisfies $|U_s(m_0)| \leq |U_s(m)|$ for all monomials m of degree exactly d.*

Proof. Fix any monomial m of degree d such that $|U_s(m)|$ is as small as possible; say $m = \prod_{j\in[n]} X_j^{e_j}$. By renaming the variables if necessary, we assume that $e_1 \geq e_2 \geq \cdots \geq e_n$.

If $m \neq m_0$, then we can find an $i < n$ such that $0 < e_{i+1} \leq e_i < q-1$. Consider the monomial $m' = X_i^{e_i+1} X_{i+1}^{e_{i+1}-1} \prod_{j \notin \{i,i+1\}} X_j^{e_j}$. We claim that $|U_s(m')| \leq |U_s(m)|$. This will complete the proof of the lemma, since it is easy to check that by repeatedly modifying the monomial in this way at most d times, we end up with the monomial m_0. By construction, we will have shown that $|U_s(m_0)| \leq |U_s(m)|$.

We are left to show that $|U_s(m')| \leq |U_s(m)|$ or equivalently (by Fact 2.3) that $|D_s(m')| \leq |D_s(m)|$. To this end, we show that for any $(n-2)$-tuple $\mathbf{e}' = (e_1', \ldots, e_{i-1}', e_{i+2}', \ldots, e_n')$, we have $|D_s(m', \mathbf{e}')| \leq |D_s(m, \mathbf{e}')|$ where $D_s(m, \mathbf{e}')$ denotes the set of monomials $\tilde{m} \in D_s(m)$ such that for each $j \in [n] \setminus \{i, i+1\}$, the degree of X_j in $\tilde{m}$ is e_j'. To see this, note that $D_s(m, \mathbf{e}')$ and $D_s(m', \mathbf{e}')$ are in bijective correspondence with the sets S and T respectively, defined as follows:

$$S = \{(d_1, d_2) \mid 0 \leq d_1 \leq a, 0 \leq d_2 \leq b, d_1 + d_2 = c\},$$
$$T = \{(d_1, d_2) \mid 0 \leq d_1 \leq a-1, 0 \leq d_2 \leq b+1, d_1 + d_2 = c\},$$

where $a := (q-1) - e_i$, $b := (q-1) - e_{i+1}$, and $c = s - \sum_{j \notin \{i,i+1\}} e'_j$; note that by assumption, $(q-1) > e_i \geq e_{i+1}$ and hence $1 \leq a \leq b$. Our claim thus reduces to showing $|T| \leq |S|$, which is done as follows.

If $c < 0$ or $c > a+b$, then both S and T are empty sets and the claim is trivial. So assume that $0 \leq c \leq a+b$. In this case, we see that $|T \setminus S| \leq 1$: in fact, $T \setminus S$ can only contain the element $(c-b-1, b+1)$ and this happens only when the inequalities $0 \leq c-b-1 \leq a-1$ are satisfied. But this allows us to infer that $S \setminus T$ contains $(a, c-a)$ since $0 \leq c-b-1 \leq c-a$ and $c-a \leq b$. Thus, $|T \setminus S| \leq |S \setminus T|$ and hence $|T| \leq |S|$. ☐

We have the following immediate corollary of Lemma 3.1.

Corollary 3.2. *Let $d, e, s \geq 0$ be arbitrary parameters with $s \leq e$ and $d \leq n(q-1)$. Assume $d = (q-1)u + v$ for $u, v \geq 0$ with $v < (q-1)$. Then the monomial $m_0 := X_1^{q-1} \cdots X_u^{q-1} X_{u+1}^v$ satisfies $|U_{s,e}(m_0)| \leq |U_{s,e}(m)|$ for all monomials m of degree exactly d.*

The main technical lemma of this section is the following.

Lemma 3.3 (Extension of the Schwartz-Zippel lemma over $\mathbb{F}_q$). *Let $e, d, s \geq 0$ be integer parameters with $s \leq e$. Let $f \in \mathcal{P}_q(n)$ be non-zero and of degree* exactly *d with* $\mathrm{LM}(f) = m_1$. *Then,*

$$\Pr_{P \in_R \mathcal{P}_q(n,e)} [\deg(fP) < d+s] \leq \frac{1}{q^{|U_{s,e}(m_1)|}}.$$

In particular, using Corollary 3.2, the probability above is upper bounded by $\frac{1}{q^{|U_{s,e}(m_0)|}}$ where the monomial m_0 is as defined in the statement of Corollary 3.2.

Proof. Let $P = \sum_{m : \deg(m) \leq e} \alpha_m m$ where m ranges over all monomials in $\mathcal{P}_q(n)$ of degree at most e and the α_m are chosen independently and uniformly at random from $\mathbb{F}_q$. Also, let $f = \sum_{i=1}^N \beta_i m_i$ where $\beta_i \neq 0$ for each i and we have $m_1 > m_2 > \cdots > m_N$ in the graded lexicographic order defined earlier.

Thus, we have

$$fP = \left(\sum_{m : \deg(m) \leq e} \alpha_m m \right) \cdot \left(\sum_{i=1}^N \beta_i m_i \right) = \sum_{\tilde{m}} \left(\sum_{(m,j) : m m_j = \tilde{m}} \alpha_m \beta_j \right) \tilde{m}.$$

The polynomial fP has degree $< d+s$ iff for each $\tilde{m}$ of degree at least $d+s$, its coefficient in the above expression is 0. Since the β_i's are fixed, we can view this event as the probability that some set of *homogeneous* linear equations in the α_m variables (one equation for each $\tilde{m}$ of degree at least $d+s$) are satisfied. By standard linear algebra, this is exactly q^{-t} where t is the rank of the linear system. So it suffices to show that there are at least $|U_{s,e}(m_1)|$ many *independent* linear equations in the system.

Recall that $|D_{s,e}(m_1)| = |U_{s,e}(m_1)|$. Now, for each $m \in D_{s,e}(m_1)$, consider the "corresponding" monomial $\tilde{m} = m \cdot m_1 = m * m_1 \in U_{s,e}(m_1)$ (the second equality is true since m is disjoint from m_1). Note that each $\tilde{m} \in U_{s,e}(m_1)$ has degree exactly $\deg(m) + \deg(m_1) \in [d+s, d+e]$. Thus, for fP to have degree $< d+s$, the coefficient of each $\tilde{m}$ must vanish. Further, since $|D_{s,e}(m_1)| = |U_{s,e}(m_1)|$ it suffices to show that the linear equations corresponding to the different $\tilde{m} \in U_{s,e}(m_1)$ are all linearly independent.

To prove this, we argue as follows. Let m' be a monomial of degree at most e. We say that m' *influences* $\tilde{m} \in U_{s,e}(m_1)$ if $\alpha_{m'}$ appears with non-zero coefficient in the equation corresponding to $\tilde{m}$. We now make the following claim.

Claim 3.4. *Let $\tilde{m} \in U_{s,e}(m_1)$ and $m \in D_{s,e}(m_1)$ be such that $\tilde{m} = m * m_1$. Then, m influences $\tilde{m}$. Further, if some monomial m' influences $\tilde{m}$, then $m' \geq m$.*

Assuming the above claim, we complete the proof of the lemma as follows. Consider the matrix B of coefficients obtained by writing the above linear system in the following manner. For each $\tilde{m} = m * m_1 \in U_{s,e}(m_1)$, we have a row of B and let the rows be arranged from top to bottom in increasing order of m (w.r.t. the graded lexicographic order). Similarly, for each m' of degree at most e, we have a column and again the columns are arranged from left to right in increasing order of m'. The $(\tilde{m}, m')$th entry contains the coefficient of $\alpha_{m'}$ in the equation corresponding to the coefficient of $\tilde{m}$.

Restricting our attention only to columns corresponding to $m' \in D_{s,e}(m_1)$, Claim 3.4 guarantees to us that the submatrix thus obtained is a $|D_{s,e}(m_1)| \times |D_{s,e}(m_1)|$ matrix that is upper triangular with non-zero entries along the diagonal. Hence, the submatrix is full rank. In particular, the matrix B (and hence our linear system) has rank at least $|D_{s,e}(m_1)|$. This proves the lemma. $\square$

Proof of Claim 3.4. We start by showing that m does indeed influence $\tilde{m}$. The linear equation corresponding to $\tilde{m}$ is

$$\sum_{(m',j):m'\cdot m_j=\tilde{m}} \beta_j \alpha_{m'} = 0 \tag{4}$$

where m' runs over all monomials of degree at most e.

Clearly, one of the summands in the LHS above is $\beta_1\alpha_m$. Thus, to ensure that m influences $\tilde{m}$, it suffices to ensure that no other summand containing the variable α_m appears. That is, that $m \cdot m_j \neq \tilde{m}$ for any $j > 1$. (Note that in general unique factorization is *not true* in $\mathcal{P}_q(n)$, since $X^q = X$.)

To see this, note further that $m \cdot m_j$ is either equal to $m * m_j$ (if they are disjoint) or has smaller degree than $m * m_j$. In either case, we have $m \cdot m_j \leq m * m_j$. Thus, we obtain

$$m \cdot m_j \leq m * m_j < m * m_1 = \tilde{m}$$

where the second inequality follows from the fact that $m_1 > m_j$ and hence (by Fact 2.2) $m' * m_1 > m' * m_j$ for any monomial m'. This shows that α_m appears precisely once in the left hand side of (4) and in particular, that it must influence $\tilde{m}$.

Now, we show that no $m' < m$ influences $\tilde{m}$. Fix some $m' < m$. For any $j \in [N]$ we have

$$m' \cdot m_j \leq m' * m_j \leq m' * m_1 < m * m_1 = \tilde{m}$$

where the first two inequalities follow from a similar reasoning to above and the third from the fact that $m' < m$. Hence, we see that no monomial that is a product of m' with another monomial from f can equal $\tilde{m}$. In particular, this means that m' cannot influence $\tilde{m}$.

This completes the proof of the claim. $\square$

Corollary 3.5. *Let n, e, d, P, f be as in Lemma 3.3. Further, let r be such that $(q-1)n - d = r$ and assume $r \geq 2e + (q-1)$. Then, $\Pr_{P\sim\mathcal{P}_q(n,e)}[\deg(fP) < d + e] \leq q^{-q^{\Omega(e/q)}}$.*

Proof. To prove the corollary, we use Lemma 3.3 with $s = e$ and prove a lower bound on $|U_{e,e}(m_0)| = |U_e(m_0)| = |D_e(m_0)|$ where m_0 is the monomial from the statement of Lemma 3.1. Let T index the $t = \left\lfloor \frac{r}{q-1} \right\rfloor$ variables not present in the monomial m_0. We can lower bound $|D_e(m_0)|$ by the number of monomials of degree exactly e in $\mathcal{P}_q(n,e)$ supported on variables from T; let $\mathcal{M}$ denote this set of monomials.

Partition T arbitrarily into two sets T_1 and T_2 such that $|T_1| = e' = \lfloor e/(q-1) \rfloor$.

To lower bound $|\mathcal{M}|$, note that given any monomial m_1 in $\mathcal{P}_q(n,e)$ in the variables of T_1, we can find a monomial m_2 over the variables of T_2 such that their product has degree e. The reason for this is that m_1 can have degree at most $e'(q-1) \leq e$ and further, the maximum degree of any monomial in the variables in T_2 is

$$(t - e')(q-1) \geq \left(\frac{r}{q-1} - 1 - \frac{e}{q-1}\right)(q-1) = r - e - (q-1) \geq e$$

where the last inequality follows from our assumed lower bound on r. Hence, we can always find a monomial m_2 such that $\deg(m_1 m_2) = e$. Hence, we can lower bound $|\mathcal{M}|$ by the number of monomials m_1 over the variables in T_1 which is $q^{|T_1|} = q^{\Omega(e/q)}$. We have thus shown that $|U_{e,e}(m_0)| = q^{\Omega(e/q)}$. An application of Lemma 3.3 now implies the corollary. $\square$

3.1 Connection to the Schwartz-Zippel Lemma over $\mathbb{F}_q$

Consider the special case of Lemma 3.3 when $e = (q-1)n$ and $s = 0$. In this case, note that $\mathcal{P}_q(n,e)$ is just the ring $\mathcal{P}_q(n)$ and hence the above lemma implies $\Pr_{P \sim \mathcal{P}_q(n)}[\deg(fP) < d] \leq \frac{1}{q^{|U_{s,e}(m_0)|}}$ where m_0 is the monomial from the statement of Lemma 3.1. Note that as a special case, this implies that $\Pr_{P \sim \mathcal{P}_q(n)}[fP = 0] \leq \frac{1}{q^{|U_{s,e}(m_0)|}}$.

Observe that by Fact 2.1, $fP = 0$ if and only if the polynomial fP vanishes at each point of $\mathbb{F}_q^n$. However, since P evaluates to an independent random value in $\mathbb{F}_q$ at each input $x \in \mathbb{F}_q^n$, we see that the probability that fP evaluates to 0 at each point is exactly the probability that $P(x) = 0$ at each point where $f(x) \neq 0$. This happens with probability exactly $\frac{1}{q^{|\mathrm{Supp}(f)|}}$.

Putting it all together, we see that $\frac{1}{q^{|\mathrm{Supp}(f)|}} \leq \frac{1}{q^{|U_{s,e}(m_0)|}}$ and hence, $|\mathrm{Supp}(f)| \geq |U_{s,e}(m_0)| = |D_{s,e}(m_0)|$.

For the chosen values of e and s, the latter quantity is exactly the total number of monomials — of *any* degree — that are disjoint from m_0, which is exactly $(q-v)q^{n-u-1}$, matching the Schwartz-Zippel lemma over $\mathbb{F}_q$ (Fact 2.1).

It is also known that the Schwartz-Zippel lemma over $\mathbb{F}_q$ is tight for a suitably chosen degree d polynomial f. Lemma 3.3 is also tight for the same polynomial f, as we show below.

The Schwartz-Zippel lemma is tight for any $d \leq n(q-1)$ for the polynomial $f(X_1, \ldots, X_n)$ defined as follows. Write $d = u(q-1) + v$ so that $0 \leq v < q-1$. Fix any ordering $\xi_0, \ldots, \xi_{q-1}$ of $\mathbb{F}_q$. Recall (see Section 2.1) that $\mathcal{B}_q(n,d)$ is the space of *generalized monomials* w.r.t. this ordering of degree at most d. Let $f = b_v(X_{u+1}) \cdot \prod_{i=1}^{u} b_{q-1}(X_i)$. Note that $f \in \mathcal{B}_q(n,d)$.

We show that this same f also witnesses the tightness of Lemma 3.3.

Claim 3.6. *Let $f \in \mathcal{P}_q(n)$ be as defined above. Then, for any $e, s \geq 0$ we have*

$$\Pr_{P \sim \mathcal{P}_q(n,e)}[\deg(fP) < d + s] = \frac{1}{q^{|U_{s,e}(m_0)|}}$$

where m_0 is as defined in the statement of Corollary 3.2.

Proof. By Lemma 3.3, we already know that

$$\Pr_{P\sim\mathcal{P}_q(n,e)}[\deg(fP) < d+s] \leq \frac{1}{q^{|U_{s,e}(m_0)|}}.$$

So it suffices to prove the opposite inequality. Namely that

$$\Pr_{P\sim\mathcal{P}_q(n,e)}[\deg(fP) < d+s] \geq \frac{1}{q^{|U_{s,e}(m_0)|}}. \tag{5}$$

For this proof, it is convenient to work with generalized monomials w.r.t. two different orderings. Consider the reverse ordering to the one defined above: i.e., $\xi_{q-1},\ldots,\xi_0$. Let $b'_i(X)$ denote the basis from Section 2.1 w.r.t. this ordering. We define $\mathcal{B}'_q(n,e)$ to be the generalized monomials (see Section 2.1) w.r.t. this ordering of degree at most e.

We make a simple observation. Since each b_i vanishes *exactly* at $\xi_0,\ldots,\xi_{i-1}$ and each b'_j vanishes exactly at $\xi_{q-1},\ldots,\xi_{q-j}$, we obtain

$$b_i(X)\cdot b'_j(X) = 0 \text{ iff } i+j \geq q. \tag{6}$$

We say that b_i and b'_j are disjoint if $i+j<q$. Similarly, two generalized monomials $\prod_{i\in[n]} b_{j_i}(X_i)$ and $\prod_{j\in[n]} b'_{j'_i}(X_i)$ are disjoint if for each i, the basis elements b_{j_i} and $b'_{j'_i}$ are disjoint. From (6) above, the product of any pair of non-disjoint generalized monomials with one from each of $\mathcal{B}_q(n,d)$ and $\mathcal{B}'_q(n,e)$ is 0.

Since $\mathcal{B}'_q(n,e)$ forms a basis for $\mathcal{P}_q(n,e)$ (Fact 2.6), we can view the process of sampling P uniformly from $\mathcal{P}_q(n,e)$ as picking $\alpha_{i_1,\ldots,i_n}\in\mathbb{F}_q$ independently and uniformly at random for each $(i_1,\ldots,i_n)$ such that $\sum_{j\in[n]} i_j \leq e$ and setting

$$P = \sum_{(i_1,\ldots,i_n):\sum_j i_j\leq e} \alpha_{i_1,\ldots,i_n}\prod_{j\in[n]} b'_{i_j}(X_j).$$

We now consider the product fP, which is expanded as

$$fP = \sum_{(i_1,\ldots,i_n):\sum_j i_j\leq e} \alpha_{i_1,\ldots,i_n} f\cdot\prod_{j\in[n]} b'_{i_j}(X_j). \tag{7}$$

From the definition of f and using (6), we see that the product of f with each generalized monomial from $\mathcal{B}'_q(n,e)$ is non-zero if and only if $i_j=0$ for all $j\in[u]$ and $i_{u+1}+v<q$. In particular, the number of generalized monomials in $\mathcal{B}'_q(n,e)$ of degree exactly $t\leq e$ that are disjoint from f is equal to the cardinality of the set

$$D'_t(f) = \{(i_1,\ldots,i_n) \mid \sum_j i_j = t, i_j = 0\ \forall j\in[u], i_{u+1}+v<q\}$$

By inspection, it is easily verified that the above set has the same cardinality as $D_t(m_0)$. In particular the size of the set $\bigcup_{s\leq t\leq e} D'_t(f)$ is $\sum_{s\leq t\leq e}|D'_t(f)| = |D_{s,e}(m_0)| = |U_{s,e}(m_0)|$.

Note that when $\alpha_{i_1,\ldots,i_n}=0$ for all $(i_1,\ldots,i_n)\in\bigcup_{s\leq t\leq e} D'_t(f)$, then we have $\deg(fP)<d+s$. Since the coefficients $\alpha_{i_1,\ldots,i_n}$ are chosen independently and uniformly at random from $\mathbb{F}_q$, this happens with probability $q^{-|U_{s,e}(m_0)|}$. This implies (5) and completes the proof of the claim. $\square$

4 Analyzing $\text{Test}_{e,k}$

We prove the main theorem of the paper, namely Theorem 1.4, in this section. The results of this section only hold for *prime* fields.

We argue that the theorem holds by considering two cases. We argue that when f is Δ-far from polynomials of degree $d + r/4$ — a much stronger assumption than the hypothesis of the theorem — then a modification of the proof of Dinur and Guruswami [DG15] coupled with a suitable choice of basis for $\mathcal{P}_q(n, d)$ yields the desired conclusion.

If not, then f is Δ-close to some polynomial of degree exactly d' that is slightly larger than d. In this case, we can argue that f is "essentially" a polynomial of degree exactly d' and for any such polynomial, the product $fP_1 \dots P_k$ is, w.h.p., a polynomial of degree exactly $d' + ek$ and hence $f \notin \mathcal{P}_q(n, d + ek)$. This requires the results of Section 3.

We will assume throughout that r is greater than or equal to some fixed constant (possibly depending on q, k) since otherwise the statement of the theorem is trivial.

Case 1: f is Δ-far from $\mathcal{P}_q(n, d + \frac{r}{4})$. See Section 4.1 below.

Case 2: f is Δ-close to $\mathcal{P}_q(n, d + \frac{r}{4})$. Let $F \in \mathcal{P}_q(n, d + \frac{r}{4})$ be such that f is Δ-close to F. Let $d' = \deg(F)$. Note that $d' > d$ since f is Δ-far from $\mathcal{P}_q(n, d)$ by assumption. Hence, we must have $d < d' \le d + \frac{r}{4}$.

Note that for any $P_1, \dots, P_k \in \mathcal{P}_q(n, e)$, we have $fP_1 \cdots P_k$ is Δ-close to $FP_1 \cdots P_k$ (since $f(x) = F(x)$ implies that $f(x) \cdot \prod_i P_i(x) = F(x) \cdot \prod_i P_i(x)$). We have $FP_1 \cdots P_k \in \mathcal{P}_q(n, d' + ek) \subseteq \mathcal{P}_q(n, d' + r/4) \subseteq \mathcal{P}_q(n, d + r/2)$. Now if $fP_1 \cdots P_k \in \mathcal{P}_q(n, d + ek) \subseteq \mathcal{P}_q(n, d + r/2)$, then by the Schwartz Zippel lemma over $\mathbb{F}_q$ (Fact 2.1) applied to polynomials of degree at most $d + r/2$, we see that $fP_1 \cdots P_k = FP_1 \cdots P_k$. Hence, we have $FP_1 \cdots P_k \in \mathcal{P}_q(n, d + ek)$ which in particular implies that $FP_1 \cdots P_k$ must have degree strictly less than $d' + ek$.

For this event to occur there must be some $i < k$ such that $FP_1 \cdots P_i$ has degree exactly $d'_i := d' + ei$ but $FP_1 \cdots P_{i+1}$ has degree strictly less than $d'_i + e$.

We have shown that

$$\begin{aligned} \Pr_{P_1, \dots, P_k}\left[fP_1 \cdots P_k \in \mathcal{P}_q(n, d + ek)\right] &\le \Pr_{P_1, \dots, P_k}\left[\deg(FP_1 \cdots P_k) < d' + ek\right] \\ &\le \sum_{i=0}^{k-1} \Pr_{P_1 \cdots P_k}\left[\deg(FP_1 \cdots P_i P_{i+1}) < d'_i + e \mid \deg(FP_1 \cdots P_i) = d'_i\right]. \end{aligned} \tag{8}$$

For each i, conditioning on any fixed choice of $P_1, \dots, P_{i-1}$, the right hand side of (8) can be bounded by $q^{-q^{\Omega(e/q)}} = q^{-q^{\Omega(r)}}$ using Corollary 3.5 applied with d replaced by $d'_i \le d + r/2 - e = (q-1)n - (r/2 + e)$ (the parameter r satisfies the hypothesis of Corollary 3.5 as long as r is a large enough parameter depending on q). This implies Theorem 1.4 in this case.

4.1 Case 1 of Theorem 1.4: f is Δ-far from $\mathcal{P}_q(n, d + \frac{r}{4})$

In this case, we adopt the method of Dinur and Guruswami [DG15] along with a suitable choice of basis (Section 2.1) and Lemma 2.10 to bound the required probability. The proof is an induction, the key technical component of which is Lemma 2.11, which follows from the work of Haramaty et al. [HSS13].

Let $d' = d + r/4$. Since we know that f is not of degree d' (indeed it is Δ-far from $\mathcal{P}_q(n, d')$), we intuitively believe that $fP_1 \cdots P_k$ should not even belong to $\mathcal{P}_q(n, d' + ek) \supsetneq \mathcal{P}_q(n, d + ek)$. Hence, we associate with the event that $fP_1 \cdots P_k \in \mathcal{P}_q(n, d + ek)$ the "surprise" parameter $s := d' - d$. This will be one of the parameters we will track in the induction. Recall that for our setting of parameters $s = r/4 \geq ek$.

For any positive integers n_1, e_1, r_1, Δ_1 and $s_1 \geq e_1 k$, we define the quantity $\rho(n_1, e_1, r_1, \Delta_1, s_1)$ to be the largest $\rho \in \mathbb{R}$ such that for any $d_1 \geq 0$ such that $d_1 \leq (q-1)n_1 - s_1 - r_1$ and for any f that is Δ_1-far from $\mathcal{P}_q(n_1, d_1 + s_1)$, we have

$$\Pr_{P_1, \ldots, P_k \sim \mathcal{P}_q(n_1, e_1)} \left[fP_1 \cdots P_k \in \mathcal{P}_q(n_1, d_1 + e_1 k) \right] \leq q^{-\rho}.$$

We prove by induction on e_1, r_1, and Δ_1 that for any $n_1, e_1, r_1, \Delta_1, s_1$ as above,

$$\rho(n_1, e_1, r_1, \Delta_1, s_1) \geq q^{\Omega(\min\{e_1/q, \log_q \Delta_1, r_1/q\})}. \tag{9}$$

Note that (9) immediately implies the result of this section (i.e., Case 1 of Theorem 1.4) since in that setting we have $e_1 = e = \Omega(r), r_1 = 3r/4, \Delta_1 = \Delta \geq q^{\Omega(r)}$ and $s_1 = r/4$.

The base case of the induction — which we apply when either $e_1 < q$, $r_1 \leq c_q$, where c_q is as defined in Lemma 2.11, or $\Delta_1 \leq q^5$ — is the following simple lemma. (It is stated in greater generality than needed in the rest of the proof.)

Lemma 4.1. *For any positive n_1, e_1, r_1, Δ_1 and $s_1 \geq e_1 k$, we have $\rho(n_1, e_1, r_1, \Delta_1, s_1) = \Omega(1)$.*

The inductive case is captured in the following lemma.

Lemma 4.2. *For any positive n_1, e_1, r_1, Δ_1 and $s_1 \geq e_1 k$ with $e_1 \geq q$, $r_1 \geq c_q$ and $q^5 < \Delta_1 < q^{r_1/(q-1)}$, we have*

$$\rho(n_1, e_1, r_1, \Delta_1, s_1) \geq \sum_{i=0}^{q-1} \rho(n_1 - 1, e_1 - i, r_1 - (q-1), \Delta_1/q^3, s_1 - ki).$$

Assuming both these lemmas, by applying the induction lemma (Lemma 4.2) repeatedly $t = \min\left\{\frac{e_1 - q}{q}, \frac{\log_q \Delta_1 - 5}{3}, \frac{r_1 - c_q}{q}\right\}$ times and then the base case (Lemma 4.1), we get

$$\rho(n_1, e_1, r_1, \Delta_1, s_1) \geq q^t \cdot \Omega(1) = q^{\Omega(t)}$$

which implies (9).

Proof of Lemma 4.1. Fix any $d_1 \leq (q-1)n_1 - s_1 - r_1$ and any $f \in \mathcal{P}_q(n_1)$ that is Δ_1-far from $\mathcal{P}_q(n_1, d_1 + s_1)$. In particular, $f \notin \mathcal{P}_q(n_1, d_1)$. Say f is of degree d' for some $d' > d_1$. As we have $d_1 + e_1 k \leq d_1 + s_1 < (q-1)n_1$, we can fix some d'' such that $d_1 + e_1 k < d'' \leq \min\{(q-1)n_1, d' + e_1 k\}$.

We first show that there exists a monomial m of degree d'' and a choice for $P_1, \ldots, P_k$ such that the monomial m has non-zero coefficient in $fP_1 \cdots P_k$. If $d'' = d'$, then we can take m to be any monomial of degree d' with non-zero coefficient in f and $P_1, \ldots, P_k$ to each be the constant polynomial 1. Otherwise, let $d'' = d' + \delta$; note that $\delta \leq e_1 k$. Let $\tilde{m} = \mathrm{LM}(f)$ (of degree d'). We choose any $m' \in D_\delta(\tilde{m})$. Since $\deg(m') = \delta \leq e_1 k$, we can find $m'_1, \ldots, m'_k$ of degrees at most e_1 each such that $m' = m'_1 \cdots m'_k$.

We set $m = \tilde{m}m'$. It can be checked that if $P_1 = m'_1, \ldots, P_k = m'_k$, then the monomial m appears with non-zero coefficient in $fP_1 \cdots P_k = fm'$.

We now consider the probability that m has a non-zero coefficient in the random polynomial $g = fP_1 \cdots P_k$ obtained when each P_i is chosen uniformly from $\mathcal{P}_q(n_1, e_1)$. The coefficient of m in g can be seen to be a polynomial R of degree at most k in the coefficients of $P_1, \ldots, P_k$. Since we have seen above that there is a choice of $P_1, \ldots, P_k$ such that this coefficient is non-zero, we know that R is a non-zero polynomial. By the Schwartz-Zippel lemma (Fact 2.1), we see that the probability that R is non-zero is at least $q^{-k/(q-1)}$. Thus, with probability at least $q^{-k/(q-1)}$, the monomial m has non-zero coefficient in g and hence $\deg(g) \geq d'' > d_1 + e_1 k$.

Hence, the probability that $\deg(g) \leq d_1 + e_1 k$ is upper bounded by $(1 - q^{-k/(q-1)}) \leq q^{-a}$ for some constant a depending on q and k. This proves the lemma. □

Proof of Lemma 4.2. Fix any $d_1 \leq (q-1)n_1 - s_1 - r_1$ and any $f \in \mathcal{P}_q(n_1)$ that is Δ_1-far from $\mathcal{P}_q(n_1, d_1 + s_1)$. Since $r_1 \geq c_q$, Lemma 2.11 is applicable to f. Hence, there is a linear function $\ell(X)$ such that for each $\alpha \in \mathbb{F}_q$, the restricted function $f|_{\ell(X)=\alpha}$ is Δ_1/q^3-far from $\mathcal{P}_q(n_1 - 1, d_1 + s_1)$. By applying a linear transformation to the set of variables, we may assume that $\ell(X) = X_{n_1}$.

Fix any ordering $\{\xi_0, \ldots, \xi_{q-1}\}$ of the field $\mathbb{F}_q$ and consider the univariate basis polynomials $b_i(X)$ $(0 \leq j < q)$ w.r.t. this ordering as defined in Section 2.1. We can view the process of sampling each $P_i(X_1, \ldots, X_{n_1}) \in \mathcal{P}_q(n_1, e_1)$ as independently sampling $Q_{i,j}(X_1, \ldots, X_{n_1-1}) \in \mathcal{P}_q(n_1 - 1, e_1 - j)$ $(0 \leq j < q)$ and setting $P_i = \sum_{0 \leq j < q} b_j(X_{n_1}) Q_{i,j}(X_1, \ldots, X_{n_1-1})$. Let P denote $P_1 \cdots P_k$. We can also decompose $P = \sum_{0 \leq j < q} b_j(X_{n_1}) Q_j(X_1, \ldots, X_{n_1-1})$.

We now use Lemma 2.7, by which can decompose the product fP as follows

$$fP = \sum_{\ell=0}^{q-1} b_\ell(X_{n_1}) \left(Q_\ell \cdot f|_{X_{n_1}=\xi_\ell} + \sum_{0 \leq j < \ell} Q_j \cdot h_{j,\ell} \right) \tag{10}$$

where each $h_{j,\ell}(X_1, \ldots, X_{n_1-1})$ is some element of $\mathcal{P}_q(n_1 - 1)$.

By Lemma 2.9, it follows that for each $\ell < q$

$$Q_\ell = \sum_{(\ell_1,\ldots,\ell_k) \leq \ell} \beta^{(\ell)}_{(\ell_1,\ldots,\ell_k)} Q_{(\ell_1,\ldots,\ell_k)} \tag{11}$$

where $\beta^{(\ell)}_{(\ell,\ldots,\ell)} \neq 0$ and $Q_{(\ell_1,\ldots,\ell_k)} = \prod_{i \in [k]} Q_{i,\ell_i}$. Plugging (11) into (10) we obtain

$$\begin{aligned} fP &= \sum_{\ell=0}^{q-1} b_\ell(X_{n_1}) \left(f|_{X_{n_1}=\xi_\ell} \sum_{(\ell_1,\ldots,\ell_k) \leq \ell} \beta^{(\ell)}_{(\ell_1,\ldots,\ell_k)} Q_{(\ell_1,\ldots,\ell_k)} + \sum_{0 \leq j < \ell} h_{j,\ell} \sum_{(\ell_1,\ldots,\ell_k) \leq j} \beta^{(j)}_{(\ell_1,\ldots,\ell_k)} Q_{(\ell_1,\ldots,\ell_k)} \right) \\ &= \sum_{\ell=0}^{q-1} b_\ell(X_{n_1}) \underbrace{\left(\beta^{(\ell)}_{(\ell,\ldots,\ell)} Q_{(\ell,\ldots,\ell)} f|_{X_{n_1}=\xi_\ell} + \sum_{(\ell_1,\ldots,\ell_k) < \ell} Q_{(\ell_1,\ldots,\ell_k)} h^{(\ell)}_{(\ell_1,\ldots,\ell_k)} \right)}_{:= R_\ell(X_1,\ldots,X_{n_1-1})} \end{aligned} \tag{12}$$

where each $h^{(\ell)}_{(\ell_1,\ldots,\ell_k)} = h^{(\ell)}_{(\ell_1,\ldots,\ell_k)}(X_1, \ldots, X_{n_1-1}) \in \mathcal{P}_q(n_1 - 1)$. We also use $h^{(\ell)}_{(\ell,\ldots,\ell)}$ to denote $\beta^{(\ell)}_{(\ell,\ldots,\ell)} f|_{X_{n_1}=\xi_\ell}$.

Now, we analyze the probability that $fP \in \mathcal{P}_q(n_1, d_1 + e_1 k)$. We have

$$\begin{aligned}
\Pr_{Q_{i,j}}\left[fP \in \mathcal{P}_q(n_1, d_1 + e_1 k)\right] &\leq \Pr_{Q_{i,j}}\left[\bigwedge_{0\leq \ell<q} R_\ell \in \mathcal{P}_q(n_1, d_1 + e_1 k - \ell)\right] \\
&\leq \prod_{0\leq \ell<q} \Pr_{Q_{i,j}}\left[R_\ell \in \mathcal{P}_q(n_1, d_1 + e_1 k - \ell) \mid \{R_0, \ldots, R_{\ell-1}\}\right] \\
&\leq \prod_{0\leq \ell<q} \Pr_{Q_{i,j}}\left[R_\ell \in \mathcal{P}_q(n_1, d_1 + e_1 k - \ell) \mid \{Q_{i,j} \mid i \in [k], j < \ell\}\right] \qquad (13)
\end{aligned}$$

where the last inequality follows from the fact that each R_j only depends on $Q_{i,j'}$ where $i \in [k]$ and $j' \leq j$.

Let $\exp_q(\theta)$ denote q^θ. We claim that the ℓth term in the RHS of (13) can be bounded as follows.

$$\Pr_{Q_{i,j}}\left[R_\ell \in \mathcal{P}_q(n_1, d_1 + e_1 k - \ell) \mid \{Q_{i,j} \mid i \in [k], j < \ell\}\right] \leq \exp_q(-\rho(n_1 - 1, e_1 - \ell, r_1 - (q-1), \Delta_1/q^3, s_1 - k\ell)) \qquad (14)$$

Substituting into (13), this will show that

$$\rho(n_1, e_1, r_1, \Delta_1, s_1) \geq \sum_{\ell=0}^{q-1} \rho(n_1 - 1, e_1 - \ell, r_1 - (q-1), \Delta_1/q^3, s_1 - k\ell)$$

which proves the lemma.

It remains only to prove (14) for which we use Lemma 2.10. We first condition on any choice of $Q_{i,j}$ for $i \in [k]$ and $j < \ell$. The event $R_\ell \in \mathcal{P}_q(n_1 - 1, d_1 + e_1 k - \ell)$ now depends only on the random polynomials $\mathcal{Q} = \{Q_{i,\ell} \mid i \in [k]\}$. We view the process of sampling these polynomials as sampling the coefficients of the standard monomials $m \in \mathcal{P}_q(n_1 - 1, e - \ell)$[3] independently and uniformly at random from $\mathbb{F}_q$. Let $\zeta_{i,m}$ denote the (random) coefficient of the monomial m in the polynomial $Q_{i,\ell}$.

Scanning the definition of R_ℓ in (12) above, we see that R_ℓ is the sum of polynomials $Q_{(\ell_1,\ldots,\ell_k)} h^{(\ell)}_{(\ell_1,\ldots,\ell_k)}$, where $(\ell_1, \ldots, \ell_k) \leq \ell$. For each $(\ell_1, \ldots, \ell_k) < \ell$, the polynomial $Q_{(\ell_1,\ldots,\ell_k)}$ is a product of at most $k - 1$ polynomials from the set $\mathcal{Q}$.

The event that $R_\ell \in \mathcal{P}_q(n_1 - 1, d_1 + e_1 k - \ell)$ is equal to the probability that each monomial $\tilde{m}$ of degree larger than $d_1 + e_1 k - \ell$ has zero coefficient in R_ℓ. Consider the coefficient of $\tilde{m}$ in each term

$$h^{(\ell)}_{(\ell_1,\ldots,\ell_k))} Q_{(\ell_1,\ldots,\ell_k)} = Q'_{(\ell_1,\ldots,\ell_k)} \prod_{i:\ell_i=\ell} Q_{i,\ell_i} \qquad (15)$$

where $Q'_{(\ell_1,\ldots,\ell_k)}$ is the *fixed* polynomial $\prod_{i:\ell_i<\ell} Q_{i,\ell_i} \cdot h^{(\ell)}_{(\ell_1,\ldots,\ell_k)}$.

Let $\mathcal{Z} = \{\zeta_{i,m} \mid i \in [k], m \in \mathcal{P}_q(n_1 - 1, e_1 - \ell)\}$ and $\mathcal{Z}_i = \{\zeta_{i,m} \mid m \in \mathcal{P}_q(n_1 - 1, e_1 - \ell)\}$ for each $i \in [k]$. Clearly, $\Pi = \{\mathcal{Z}_1, \ldots, \mathcal{Z}_k\}$ is a partition of $\mathcal{Z}$. It can be verified from (15) that the coefficient of each monomial $\tilde{m}$ in $h^{(\ell)}_{(\ell_1,\ldots,\ell_k))} Q_{(\ell_1,\ldots,\ell_k)}$ is a Π-multilinear polynomial (see Section 2.2) $C^{(\tilde{m})}_{(\ell_1,\ldots,\ell_k)}$ applied to the random variables in $\mathcal{Z}$. In fact, it only depends on the random variables in $\bigcup_{i:\ell_i=\ell} \mathcal{Z}_i$. Hence, this polynomial is Π-set-multilinear if and only if $\ell_1 = \cdots = \ell_k = \ell$.

[3]Any reasonable basis for the space $\mathcal{P}_q(n_1 - 1, e - \ell)$ will do here. In particular, we do not need the special basis from Section 2.1.

Hence, from the definition of R_ℓ (12) we see that the coefficient of $\tilde{m}$ in R_ℓ is

$$C^{(\tilde{m})} := \sum_{(\ell_1,\ldots,\ell_k)\le \ell} C^{(\tilde{m})}_{(\ell_1,\ldots,\ell_k)} \tag{16}$$

which is a Π-multilinear polynomial in $\mathcal{Z}$ with set-multilinear part $C^{(\tilde{m})}_{(\ell,\ldots,\ell)}$. We will use Lemma 2.10 to bound the probability that $C^{(\tilde{m})}(\zeta_{i,m} : i, m) = 0$.

Now we can analyze the probability that $R_\ell \in \mathcal{P}_q(n_1 - 1, d_1 + e_1 k - \ell)$. We omit the conditioning on $Q_{i,j}$ ($j < \ell$) since they are fixed. Below, $\tilde{m}$ varies over all monomials in $\mathcal{P}_q(n_1 - 1)$ of degree $> d_1 + e_1 k - \ell$.

$$\begin{aligned}
\Pr_{Q_{i,\ell}}\left[R_\ell \in \mathcal{P}_q(n_1 - 1, d_1 + e_1 k - \ell)\right] &= \Pr_{\zeta_{i,m}}\left[\bigwedge_{\tilde{m}} C^{(\tilde{m})}(\zeta_{i,m}) = 0\right] \\
&\le \Pr_{\zeta_{i,m}}\left[\bigwedge_{\tilde{m}} C^{(\tilde{m})}_{(\ell,\ldots,\ell)}(\zeta_{i,m}) = 0\right] \\
&= \Pr_{\zeta_{i,m}}\left[Q_{(\ell,\ldots,\ell)} h^{(\ell)}_{(\ell,\ldots,\ell)} \in \mathcal{P}_q(n_1 - 1, d_1 + e_1 k - \ell)\right] \\
&= \Pr_{\zeta_{i,m}}\left[Q_{(\ell,\ldots,\ell)} f|_{X_{n_1}=\xi_\ell} \in \mathcal{P}_q(n_1 - 1, d_1 + e_1 k - \ell)\right] \qquad (17)
\end{aligned}$$

where the inequality follows from Lemma 2.10; the second equality follows from the fact that $C^{(\tilde{m})}_{(\ell,\ldots,\ell)}(\zeta_{i,m}) = 0$ for all $\tilde{m}$ if and only if each monomial of degree more than $d_1 + e_1 k - \ell$ has zero coefficient in $Q_{(\ell,\ldots,\ell)} h^{(\ell)}_{(\ell,\ldots,\ell)}$; and the last equality follows from the fact that $h^{(\ell)}_{(\ell,\ldots,\ell)} = \beta^{(\ell)}_{(\ell,\ldots,\ell)} f|_{X_{n_1}=\xi_\ell}$ and $\beta^{(\ell)}_{(\ell,\ldots,\ell)} \ne 0$.

The final expression in (17) can be bounded by the induction hypothesis applied with $n_2 = n_1 - 1$, $e_2 = e_1 - \ell$, $r_2 = r_1 - (q-1)$, $\Delta_2 = \Delta_1/q^3$ and $s_2 = s_1 - k\ell$. We show below that the parameters satisfy all the required hypotheses.

- $Q_{(\ell,\ldots,\ell)} = \prod_i Q_{i,\ell}$ is a product of ℓ independent polynomials each uniformly sampled from $\mathcal{P}_q(n_1 - 1, e_1 - \ell) = \mathcal{P}_q(n_2, e_2)$. Recall that $e_1 \ge q$ and hence $e_2 = e_1 - \ell > 0$.
- By assumption, $g := f|_{X_n=\xi_\ell}$ is $\Delta_1/q^3 = \Delta_2$-far from $\mathcal{P}_q(n_1 - 1, d_1 + s_1) = \mathcal{P}_q(n_2, d_2 + s_2)$ where $d_2 = d_1 + k\ell$ and s_2 is as defined above. Note that $s_2 = s_1 - k\ell \ge e_1 k - k\ell = e_2 k$. Also note that

  $$(q-1)n_2 - d_2 = (q-1)n_1 - (q-1) - d_1 - k\ell \ge r_1 + s_1 - (q-1) - k\ell = r_2 + s_2,$$

  where the inequality uses $d_1 \le (q-1)n_1 - r_1 - s_1$. Hence, we have $d_2 \le (q-1)n_2 - r_2 - s_2$.
- We also have $\Delta_2 = \Delta_1/q^3 < q^{r_1/(q-1)-3} < q^{r_2/(q-1)}$.
- Finally, we consider the event that $g\prod_i Q_{i,\ell} \in \mathcal{P}_q(n_1 - 1, d_1 + e_1 k - \ell) = \mathcal{P}_q(n_2, d_2 + e_2 k - \ell) \subseteq \mathcal{P}_q(n_2, d_2 + e_2 k)$.

Thus, we can upper bound the probability in (17) by $\exp_q(-\rho(n_2, e_2, r_2, \Delta_2, s_2))$, which yields (14) and proves the lemma. $\square$

5 Two applications

5.1 A question of Dinur and Guruswami

In this section, we show how Theorem 1.4 implies Theorem 1.5, thus answering a open question raised by Dinur and Guruswami [DG15].

Proof of Theorem 1.5. The proof of the lemma for robustness Δ' can be reduced to Theorem 1.4 for $k = 2$ as follows.

Let f be Δ-far from $\mathcal{P}_q(n,d)$ as stated in the lemma. Call P "lucky" if $\Delta(f \cdot P, \mathcal{P}_q(m, d+e)) \leq \Delta'$. We need to bound the probability $\Pr_{P \in \mathcal{P}_q(n,e)}[P \text{ is lucky }]$. For a lucky P, let F be a degree-$(d+e)$ polynomial that is Δ'-close to $f \cdot P$. Now, choose $P' \in_R \mathcal{P}_q(n,e)$ and let $g = fP \cdot P'$. Also, let $G = F \cdot P'$; note that $G \in \mathcal{P}_q(n, d+2e)$.

Let $D = \{x \in \mathbb{F}_q^n \mid F(x) \neq f(x)P(x)\}$. We have $|D| \leq \Delta'$. Further, if $P'(x) = 0$ for each $x \in D$, then we have $g = G$ and hence $g \in \mathcal{P}_q(n, d+2e)$.

Observe that the event that $P'(x) = 0$ for each $x \in D$ is a set of $|D| \leq \Delta'$ homogeneous linear equations in the (randomly chosen) coefficients of P. These equations are simultaneously vanish with probability at least $q^{-\Delta'}$. Hence, for a lucky P, we see that $\Pr_{P'}\left[g \in \mathcal{P}_q(n, d+2e)\right] \geq q^{-\Delta'}$.

Thus, we see that for independent and randomly chosen $P, P' \in \mathcal{P}_q(n,e)$,

$$\begin{aligned}
&\Pr_{P,P'}\left[fPP' \in \mathcal{P}_q(n, d+2e)\right] \\
&\geq \Pr_{P}[P \text{ is lucky }] \cdot \Pr_{P,P'}[g \in \mathcal{P}_q(n, d+2e) \mid P \text{ is lucky }] \\
&\geq \Pr_{P}[P \text{ is lucky }] \cdot \Pr_{P,P'}[g = G \mid P \text{ is lucky }] \geq \Pr_{P}[P \text{ is lucky }] \cdot \frac{1}{q^{\Delta'}}.
\end{aligned}$$

Thus, by Theorem 1.4 we get

$$\Pr_{P}[P \text{ is lucky }] \leq \frac{q^{\Delta'}}{q^{q^{\Omega(r)}}}.$$

The lemma now follows for some $\Delta' = q^{\Omega(r)}$. $\square$

5.2 Analysis of Corr-h

Recall the test Corr-h defined in the introduction where $h \in \mathcal{P}_q(n,k)$ is a polynomial of exact degree k. In this section, we analyze this test Corr-h, thus proving Corollary 1.6.

For this we need the following properties of polynomials.

Dual of $\mathcal{P}_q(n,d)$: For any two functions, $f, g \in \mathcal{F}_q(n)$, define $\langle f, g\rangle := \sum_{x \in \mathbb{F}_q^n} f(x) \cdot g(x)$. Given any $\mathbb{F}_q$-space $\mathcal{C} \subseteq \mathcal{F}_q(n)$, the dual of $\mathcal{C}$ is defined as $\mathcal{C}^{\perp} := \{f \in \mathcal{F}_q(n) \mid \forall g \in \mathcal{C}, \langle f, g\rangle = 0\}$. Recall that $r = (q-1)n - d$. It is well-know that the sets of polynomials $\mathcal{P}_q(n,d)$ and $\mathcal{P}_q(n, r-1)$ are duals of each other [Lin99]. We use these dual spaces to write the indicator variable for the event "$f \in \mathcal{P}_q(n,d)$" equivalently as $\mathbb{1}_{f\in\mathcal{P}_q(n,d)} = \mathbb{E}_{Q\in\mathcal{P}_q(n,r-1)}\left[\omega^{\langle f,Q\rangle}\right]$, where $\omega = e^{2\pi i/q}$. This follows from the following observations.

- For any polynomial $P \in \mathcal{P}_q(n,d)$, we have that for all $Q \in \mathcal{P}_q(n,r-1)$, $\langle P,Q\rangle = 0$. Thus, in this case we have $\mathbb{E}_{Q\in\mathcal{P}_q(n,r-1)}\left[\omega^{\langle P,Q\rangle}\right] = 1$.
- Let $f \notin \mathcal{P}_q(n,d)$. For each $\alpha \in \mathbb{F}_q$, let $\mathcal{C}_\alpha := \{Q \in \mathcal{P}_q(n,r-1) \mid \langle f,Q\rangle = \alpha\}$. Since $f \notin \mathcal{P}_q(n,d)$, there exists a $Q \in \mathcal{P}_q(n,r-1)$ such that $\langle f,Q\rangle \neq 0$ and hence $\mathcal{C}_0$ is a proper subspace of $\mathcal{P}_q(n,r-1)$. This implies that $\{\mathcal{C}_\alpha\}_{\alpha\in\mathbb{F}_q}$ form an equipartition of $\mathcal{P}_q(n,r-1)$. Hence, $\mathbb{E}_{Q\in\mathcal{P}_q(n,r-1)}\left[\omega^{\langle f,Q\rangle}\right] = \mathbb{E}_{\alpha\in\mathbb{F}_q}\left[\mathbb{E}_{Q\in\mathcal{C}_\alpha}\left[\omega^{\langle f,Q\rangle}\right]\right] = \mathbb{E}_{\alpha\in\mathbb{F}_q}\left[\omega^\alpha\right] = 0$.

Squaring trick: We use a standard squaring trick to bound the absolute value of the quantity $\mathbb{E}_P\left[\omega^{\langle h(P),f\rangle}\right]$. Let g be a univariate polynomial of degree exactly k with leading coefficient g_k. We will show (using induction on k) that for all $k \geq 1$, we have

$$\left|\mathop{\mathbb{E}}_{P}\left[\omega^{\langle g(P),f\rangle}\right]\right|^{2^k} \leq \mathop{\mathbb{E}}_{P_1,\ldots,P_k}\left[\omega^{\langle k!g_kP_1\cdots P_k,f\rangle}\right].$$

The base case of the induction ($k=1$) can be easily checked to be true. Let $g(P) = aP+b$ where $a \neq 0$.

$$\left|\mathop{\mathbb{E}}_{P}\left[\omega^{\langle aP+b,f\rangle}\right]\right|^{2} = \mathop{\mathbb{E}}_{P,P_1}\left[\omega^{\langle (a(P+P_1)+b),f\rangle}\cdot\omega^{\langle -(aP+b),f\rangle}\right] = \mathop{\mathbb{E}}_{P,P_1}\left[\omega^{\langle aP_1,f\rangle}\right] = \mathop{\mathbb{E}}_{P_1}\left[\omega^{\langle aP_1,f\rangle}\right].$$

We now induct from $k-1$ to k. Let g be a polynomial of degree exactly k with leading coefficient g_k. To this end, we first observe that $g(P+P_1)-g(P)$ is a polynomial of degree exactly $k-1$ in P with leading coefficient kP_1g_k.

$$\begin{aligned}\left|\mathop{\mathbb{E}}_{P}\left[\omega^{\langle g(P),f\rangle}\right]\right|^{2^k} &= \left(\left|\mathop{\mathbb{E}}_{P}\left[\omega^{\langle g(P),f\rangle}\right]\right|^{2}\right)^{2^{k-1}} = \left(\mathop{\mathbb{E}}_{P,P_1}\left[\omega^{\langle g(P+P_1)-g(P),f\rangle}\right]\right)^{2^{k-1}}\\ \text{(by convexity)} &\leq \mathop{\mathbb{E}}_{P_1}\left[\left|\mathop{\mathbb{E}}_{P}\left[\omega^{\langle g(P+P_1)-g(P),f\rangle}\right]\right|^{2^{k-1}}\right]\\ \text{(by induction)} &\leq \mathop{\mathbb{E}}_{P_1}\left[\mathop{\mathbb{E}}_{P_2,\ldots,P_k}\left[\omega^{\langle (k-1)!\cdot(kP_1g_k)\cdot P_2P_3\cdots P_k,f\rangle}\right]\right] = \mathop{\mathbb{E}}_{P_1,\ldots,P_k}\left[\omega^{\langle k!g_kP_1\cdots P_k,f\rangle}\right].\end{aligned}$$

We are now ready to prove Corollary 1.6.

Proof of Corollary 1.6. Since the class of polynomials $\mathcal{P}_q(n,d+ek)$ is closed under scalar multiplication, we can assume (by multiplying by a non-zero scalar if necessary) that h is monic.

$$\Pr_{P \in \mathcal{P}_q(n,e)}\left[f \cdot h(P) \in \mathcal{P}_q(n, d+ek)\right] = \left| \mathop{\mathbb{E}}_{P\in\mathcal{P}_q(n,e), Q\in\mathcal{P}_q(n,s-1)} \left[\omega^{\langle f\cdot h(P), Q\rangle}\right]\right| = \left| \mathop{\mathbb{E}}_{Q}\left[\mathop{\mathbb{E}}_{P}\left[\omega^{\langle h(P), fQ\rangle}\right]\right]\right|^{2^k/2^k}$$

$$\text{(by convexity)} \leq \left(\mathop{\mathbb{E}}_{Q}\left[\left|\mathop{\mathbb{E}}_{P}\left[\omega^{\langle h(P), fQ\rangle}\right]\right|^{2^k}\right]\right)^{1/2^k}$$

$$\text{(by the squaring trick)} \leq \left(\mathop{\mathbb{E}}_{Q}\left[\mathop{\mathbb{E}}_{P_1,\ldots,P_k}\left[\omega^{\langle k! P_1\cdots P_k, fQ\rangle}\right]\right]\right)^{1/2^k} = \left(\mathop{\mathbb{E}}_{P_1,\ldots,P_k}\left[\mathop{\mathbb{E}}_{Q}\left[\omega^{\langle P_1\cdots P_k f, Q\rangle}\right]\right]\right)^{1/2^k}$$

$$= \left(\Pr_{P_1,\ldots,P_k}\left[f \cdot \prod_i P_i \in \mathcal{P}_q(n, d+ek)\right]\right)^{1/2^k}$$

where the first inequality follows from Jensen's inequality and the second from the Squaring trick. For the third equality, we have used the fact that since $k < q$, the polynomials $k!P_1 \cdots P_k$ and $P_1 \cdots P_k$ are distributed identically.

The corollary now follows from Theorem 1.4. $\square$

Acknowledgements.

We thank Madhu Sudan for many encouraging discussions and feedback. We also thank the anonymous reviewers of FSTTCS 2016 for many corrections and pointing out a weakness in a previous version of Theorem 1.5.

References

[AKK+05] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. *Testing Reed-Muller codes*. IEEE Trans. Inform. Theory, 51(11):4032–4039, 2005. (Preliminary version in *7th RANDOM*, 2003). doi:10.1109/TIT.2005.856958. 1, 2

[BGH+15] Boaz Barak, Parikshit Gopalan, Johan Håstad, Raghu Meka, Prasad Raghavendra, and David Steurer. *Making the long code shorter*. SIAM J. Comput., 44(5):1287–1324, 2015. (Preliminary version in *53rd FOCS*, 2012). arXiv:1111.0405, eccc:TR11-142, doi:10.1137/130929394. 2

[BKS+10] Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. *Optimal testing of Reed-Muller codes*. In *Proc. 51st IEEE Symp. on Foundations of Comp. Science (FOCS)*, pages 488–497. 2010. arXiv:0910.0641, doi:10.1109/FOCS.2010.54. 1, 2, 11

[CLO15] David A Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer, 3rd edition, 2015. doi:10.1007/978-3-319-16721-3. 7

[DG15] Irit Dinur and Venkatesan Guruswami. *PCPs via the low-degree long code and hardness for constrained hypergraph coloring*. Israel Journal of Mathematics, 209:611–649, 2015. (Preliminary version in *54th FOCS*, 2013). eccc:TR13-122, doi:10.1007/s11856-015-1231-3. 1, 2, 3, 5, 6, 11, 17, 22

[GHH+14] Venkat Guruswami, Prahladh Harsha, Johan Håstad, Srikanth Srinivasan, and Girish Varma. *Super-polylogarithmic hypergraph coloring hardness via low-degree long codes*. In *Proc. 46th ACM Symp. on Theory of Computing (STOC)*, pages 614–623. 2014. arXiv:1311.7407, doi:10.1145/2591796.2591882. 1, 2, 3, 4, 5, 11

[HS16] Prahladh Harsha and Srikanth Srinivasan. *Robust multiplication-based tests for Reed-Muller codes*. In Akash Lal, S. Akshay, Saket Saurabh, and Sandeep Sen, eds., *Proc. 36th IARCS Annual Conf. on Foundations of Software Tech. and Theoretical Comp. Science (FSTTCS)*, volume 65 of *LIPIcs*, pages 17:1–17:14. Schloss Dagstuhl, 2016. arXiv:1612.03086, doi:10.4230/LIPIcs.FSTTCS.2016.17. 1

[HSS13] Elad Haramaty, Amir Shpilka, and Madhu Sudan. *Optimal testing of multivariate polynomials over small prime fields*. SIAM J. Comput., 42(2):536–562, 2013. (Preliminary version in *52nd FOCS*, 2011). eccc:TR11-059, doi:10.1137/120879257. 1, 2, 7, 11, 12, 17

[Hua15] Sangxia Huang. $2^{(\log N)^{1/10-o(1)}}$ *hardness for hypergraph coloring*, 2015. (manuscript). arXiv:1504.03923. 2, 3

[KLP68] Tadao Kasami, Shu Lin, and W. Wesley Peterson. *Polynomial codes*. IEEE Trans. Inform. Theory, 14(6):807–814, 1968. doi:10.1109/TIT.1968.1054226. 7

[KR06] Tali Kaufman and Dana Ron. *Testing polynomials over general fields*. SIAM J. Comput., 36(3):779–802, 2006. (Preliminary version in *45th FOCS*, 2004). doi:10.1137/S0097539704445615. 1, 2

[KS14] Subhash Khot and Rishi Saket. *Hardness of coloring 2-colorable 12-uniform hypergraphs with* $2^{(\log n)^{\Omega(1)}}$ *colors*. In *Proc. 55th IEEE Symp. on Foundations of Comp. Science (FOCS)*, pages 206–215. 2014. eccc:TR14-051, doi:10.1109/FOCS.2014.30. 2, 3

[Lin99] Jacobus Hendricus van Lint. *Introduction to Coding Theory*. Springer, 3rd edition, 1999. doi:10.1007/978-3-642-58575-3. 23

[Var15] Girish Varma. *Reducing uniformity in Khot-Saket hypergraph coloring hardness reductions*. Chicago J. Theor. Comput. Sci., 2015(3):1–8, 2015. arXiv:1408.0262, doi:10.4086/cjtcs.2015.003. 2, 3

ECCC ISSN 1433-8092

http://eccc.hpi-web.de