Robust Multiplication-Based Tests for Reed-Muller Codes

Prahladh Harsha[1] **and Srikanth Srinivasan**[2]

1 **TIFR, Mumbai, India**
prahladh@tifr.res.in
2 **Dept. of Mathematics, IIT Bombay, Mumbai, India**
srikanth@math.iitb.ac.in

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.

- $\mathrm{Test}_{e,k}$: 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.

1998 ACM Subject Classification F.2.1 Numerical Algorithms and Problems

Keywords and phrases Polynomials over finite fields, Schwartz-Zippel lemma, Low degree testing, Low degree long code

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2016.17

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 [1], 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 [3, 6]. 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) [4, 5]. In this work, we give a robust version of one of these latter multiplication based tests due to Dinur and Guruswami [4]. 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 polynomials of degree at most d. If n, d and q are clear from context, $r := (q-1)n - d$.

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.* [1] for the case when $q = 2$.

- 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.* [3] showed the following optimal analysis of this test.

▶ **Theorem 1.1** ([1, 3]). *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 [6] 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.* [2] which has played an important role in several improved hardness of approximation results [4, 5, 9, 10, 7].

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.* [3] that led to the optimal analysis in Theorem 1.1 is the following robust analysis of $\text{Test}_{1,1}$.

▶ **Lemma 1.2** ([3]). *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*

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

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** ([4]). *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 [4, 5, 9, 10, 7].

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.** *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 $r = q(n-1) - d$, $q^{\varepsilon r} \leq \Delta \leq q^{r/4(q-1)-2}$, 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*

$$\Pr_{P_1,\ldots,P_k}[fP_1P_2\cdots P_k \in \mathcal{P}_q(n, d+ek)] \leq \frac{1}{q^{q^{\Omega(r)}}}$$

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 [4].

▶ **Lemma 1.5.** *Let $q \in \mathbb{N}$ be a constant with q prime and $\varepsilon, \delta \in (0,1)$ be arbitrary constants. Let $n, d, r, \Delta, \Delta', e \in \mathbb{N}$ be such that $r = q(n-1) - d$, $q^{\varepsilon r} \leq \Delta \leq q^{r/4(q-1)-2}$, and $\delta r \leq e \leq r/4k$ where $k := 1 + \lceil \log_{q/(q-1)}(2\Delta') \rceil$. 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*

$$\Pr_P[\Delta(f \cdot P, \mathcal{P}_q(n, d+e)) < \Delta'] \leq \frac{2}{q^{q^{\Omega(r)}}}$$

where the $\Omega(\cdot)$ above hides a constant 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 tests 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.* [5] 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 $h \in \mathcal{P}_q(n,k)$ be a 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.** *Let $q,k \in \mathbb{N}$ be constants with q prime, $k < q$[†], and let $\varepsilon,\delta \in (0,1)$ be arbitrary constants. Let $n,d,r,\Delta,e \in \mathbb{N}$ be such that $r = q(n-1)-d$, $q^{\varepsilon r} \le \Delta \le q^{r/4(q-1)-2}$, 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*

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

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

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 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, when we multiply f with k random polynomials $P_1,\ldots,P_k \in \mathcal{P}_q(n,e)$, that the product $fP_1\cdots P_k$ is a polynomial of degree $d'+ek$ 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 d' that maximizes the probability that $fP_1\cdots P_k$ 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, viewed suitably, is a generalization of the Schwartz-Zippel lemma over $\mathbb{F}_q$ (see Section 3.1 and the full version for more details).

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

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 [4] which corresponds to Theorem 1.4 in the case that $q = 2$ and $k = 1$. The argument is essentially an induction on the parameters $e, r = n-d$, and Δ. We describe this argument in some detail so that we can highlight the variations in our work.

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

As long as r is a sufficiently large constant, Lemma 1.2 can be used 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 $\mathcal{P}_2(n-1,d)$.*

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 $hR_1 \in \mathcal{P}_2(n-1,d+e)$ – call this event $\mathcal{E}_1$ – and $(g+h)Q_1 + hR_1 \in \mathcal{P}_2(n-1,d+e-1)$, which we call $\mathcal{E}_2$. 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 an 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.* [5] (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. For lack of space, this part of the proof has been omitted from this extended abstract.

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 $f = Xg + h$, $P_1 = XQ_1 + R_1$, 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

* 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.

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 $Q_1Q_2(g+h) \in \mathcal{P}_2(n, d+2e-1)$ 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 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 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 [4]) and the other to proving Corollary 1.6. For lack of space, many proofs have been omitted. The reader is referred to the full version of this paper for details.

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 one of the variables – say 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 $\mathbb{F}_q$ [8]) 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 $0 \le b < q-1$.*
4. *In particular, if $f, g \in \mathcal{P}_q(n,d)$ differ from each other in at most $\Delta < q^{n-a-1}(q-b)$ places, then $f = g$.*
5. *(A probabilistic version of the Schwartz-Zippel lemma [6]) 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 $\mathbb{F}_q[X_1, \ldots, X_n]$).

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. The 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.** *For any monomials m_1, m_2, m_3, we have $m_1 \le m_2 \Rightarrow m_1 * m_3 \le m_2 * m_3$.*

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 (in the 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. For an integer $s \ge 0$, we let

$$U_s(m) := \left\{ \prod_{j \in [n]} X_j^{e_j'} \;\middle|\; \forall j \; q > e_j' \ge e_j, \sum_j e_j' = d + s \right\}$$

$$D_s(m) := \left\{ \prod_{j \in [n]} X_j^{e_j'} \;\middle|\; \forall j \; e_j' + e_j < q, \sum_j e_j' = s \right\}.$$

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 $s \ge 0$, $|U_s(m)| = |D_s(m)|$.*

For non-negative integers $s \le e$, we define $U_{s,e}(m) := \bigcup_{s \le t \le e} U_t(m)$ and $D_{s,e}(m) := \bigcup_{s \le t \le e} D_t(m)$ where $U_t(m)$ and $D_t(m)$ are as defined in Section 2. Since $|U_t(m)| = |D_t(m)|$ for each t (Fact 2.3), we have $|U_{s,e}(m)| = |D_{s,e}(m)|$.

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 (Fact 2.3) that $|D_s(m')| \leq |D_s(m)|$. To this end, we show that for any $(n-2)$-tuple $\mathbf{e}' = (e'_1, \ldots, e'_{i-1}, e'_{i+2}, \ldots, e'_n)$, that $|D_s(m', \mathbf{e}')| \leq |D_s(m, \mathbf{e}')|$ where $D_s(m, \mathbf{e}')$ denotes the set of monomials $\widetilde{m} \in D_s(m)$ such that for each $j \in [n] \setminus \{i, i+1\}$, the degree of X_j in $\widetilde{m}$ 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:

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

where $a := (q-1) - e_i$, $b := (q-1) - e_{i+1}$, and $r = s - \sum_{j\notin\{i,i+1\}} e'_j$; 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 $r < 0$ or $r > a+b$, then both S and T are empty sets and the claim is trivial. So assume that $0 \leq r \leq a+b$. In this case, we see that $|T \setminus S| \leq 1$: in fact, $T \setminus S$ can only contain the element $(r-b-1, b+1)$ and this happens only when the inequalities $0 \leq r-b-1 \leq a-1$ is satisfied. But this allows us to infer that $S \setminus T$ contains $(a, r-a)$ since $0 \leq r-b-1 \leq r-a$ and $r-a \leq b$. 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 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

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

The polynomial fP has degree $< d+s$ iff for each $\widetilde{m}$ 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 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 monomial $\widetilde{m} = m \cdot m_1 = m * m_1$ (the second equality is true since m is disjoint from m_1). Let $\widetilde{\mathcal{M}}$ denote the set of all such $\widetilde{m}$. Note that each $\widetilde{m} \in \widetilde{\mathcal{M}}$ 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 $\widetilde{m}$ must vanish. Further, since $|\widetilde{\mathcal{M}}| = |D_{s,e}(m_1)| = |U_{s,e}(m_1)|$ it suffices to show that the linear equations corresponding to the different $\widetilde{m} \in \widetilde{\mathcal{M}}$ 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* $\widetilde{m} \in \widetilde{\mathcal{M}}$ if $\alpha_{m'}$ appears with non-zero coefficient in the equation corresponding to $\widetilde{m}$. We now make the following claim.

▶ **Claim 3.4.** *Let $\widetilde{m} \in \widetilde{\mathcal{M}}$ and $m \in D_{s,e}(m_1)$ be such that $\widetilde{m} = m * m_1$. Then, m influences $\widetilde{m}$. Further, if some monomial m' influences $\widetilde{m}$, 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 $\widetilde{m} = m * m_1 \in \widetilde{\mathcal{M}}$, 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 $(\widetilde{m}, m')$th entry contains the coefficient of $\alpha_{m'}$ in the equation corresponding to the coefficient of $\widetilde{m}$.

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. ◀

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

$$\sum_{(m',j):m'\cdot m_j=\widetilde{m}} \beta_j \alpha_{m'} = 0 \tag{2}$$

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 $\widetilde{m}$, it suffices to ensure that no other summand containing the variable α_m appears. That is, that $m \cdot m_j \neq \widetilde{m}$ 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

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

where the second inequality follows from the fact that $m_1 > m_j$ and hence (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 (2) and in particular, that it must influence $\widetilde{m}$.

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

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

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 $\widetilde{m}$. In particular, this means that m' cannot influence $\widetilde{m}$.

This completes the proof of the claim. ◀

▶ **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. ◀

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. This fact is not required for the other results of this paper and thus we defer it to the full version.

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

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. For lack of space, a part of the proof has been omitted.

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 [4] coupled with a suitable choice of basis for $\mathcal{P}_q(n,d)$ (see the full version for details) yields the desired conclusion.

If not, then f is Δ-close to some polynomial of degree d' that is slightly larger than d. In this case, we can argue that f is "essentially" a polynomial of degree 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 $\mathcal{P}_q(n, d + \frac{r}{4})$. For lack of space, this section has been omitted. See the full version for details.

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 $FP_1 \cdots P_k \in \mathcal{P}_q(n, d' + r/4) \subseteq \mathcal{P}_q(n, d + r/2)$. 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 $d'_i + e$.

The above reasoning implies

$$\begin{aligned}\Pr_{P_1,\dots,P_k}[fP_1 \cdots P_k \in \mathcal{P}_q(n, d+ek)] &\le \Pr_{P_1,\dots,P_k}[\deg(FP_1 \cdots P_k) < d' + ek] \\ &\le \sum_{i=1}^{k} \Pr_{P_1 \cdots P_k}[\deg(FP_1 \cdots P_{i-1}P_i) < d'_i + e \mid \deg(FP_1 \cdots P_{i-1}) = d'_i]. \qquad (3)\end{aligned}$$

For each i, conditioning on any fixed choice of $P_1, \dots, P_{i-1}$, the right hand side of (3) can be bounded by $q^{-q^{\Omega(e/q)}} = q^{-q^{\Omega(r)}}$ using Corollary 3.5 applied with d replaced by $d'_i \le d + r/2 - e = (q-1)n - (r/2 + e)$. This implies Theorem 1.4 in this case.

5 Two applications

5.1 A question of Dinur and Guruswami

In this section, we show how Theorem 1.4 implies Lemma 1.5, thus answering a open question raised by Dinur and Guruswami [4].

Proof of Lemma 1.5. The proof of the lemma for robustness Δ' can be reduced to Theorem 1.4 for $k = 1 + \lceil \log_{q/(q-1)}(2\Delta') \rceil$ 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 $f \cdot P$. Define $k := 1 + \lceil \log_{q/(q-1)}(2\Delta') \rceil$. Now, choose $P_1, \ldots, P_{k-1} \in_R \mathcal{P}_q(n,e)$ and let $g = fP \cdot \prod_{i<k} P_i$. Also, let $G = F \cdot \prod_{i<k} P_i$; note that $G \in \mathcal{P}_q(n, d+ek)$.

Observe that for any x such that $F(x) \neq f(x)P(x)$, the probability that $G(x) \neq g(x)$ is at most the probability that all the $P_i(x)$ are non-zero and this is $\left(1 - \frac{1}{q}\right)^{k-1} \leq \frac{1}{2\Delta'}$. Hence, the probability that any point of difference between F and fP survives as a point of difference between G and g is at most $\frac{1}{2}$. Since no new points of difference are introduced, we see that

$$\begin{aligned}
&\Pr_{P,P_1,\ldots,P_{k-1}}[fP_1P_2\cdots P_k \in \mathcal{P}_q(n,d+ek)] \\
&\geq \Pr_P[P \text{ is lucky }] \cdot \Pr_{P,P_1,\ldots,P_{k-1}}[f \cdot P \cdot \prod_{i<k} P_i \in \mathcal{P}_q(n,d+ek) \mid P \text{ is lucky }] \\
&= \Pr_P[P \text{ is lucky }] \cdot \Pr_{P,P_1,\ldots,P_{k-1}}[g \in \mathcal{P}_q(n,d+ek) \mid P \text{ is lucky }] \\
&\geq \Pr_P[P \text{ is lucky }] \cdot \Pr_{P,P_1,\ldots,P_{k-1}}[g = G \mid P \text{ is lucky }] \geq \Pr_P[P \text{ is lucky }] \cdot \frac{1}{2}.
\end{aligned}$$

The lemma now follows since Theorem 1.4 implies that $\Pr_{P,P_1,\ldots,P_{k-1}}[fP_1P_2\cdots P_k \in \mathcal{P}_q(n,d+ek)] \leq q^{-q^{\Omega(r)}}$. ◀

▶ Remark 5.1. An anonymous reviewer for FSTTCS 2016 pointed out to us that Lemma 1.5 only works if $\log \Delta' = O(k)$, which in particular implies that Δ' must be a constant (independent of n and d). However, an easy modification of the above idea actually shows a statement of the above form for Δ' as large as $q^{\Omega(r)}$. We refer the reader to the full version for details.

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, $f, g \in \mathcal{F}_q(b)$, define $\langle f, g \rangle := \sum_{x \in \mathbb{F}_q^n} f(x) \cdot g(x)$. The set of polynomials $\mathcal{P}_q(n, r-1)$ is the dual to the set of polynomials $\mathcal{P}_q(n,d)$ in the following sense.

- For any two polynomials $P \in \mathcal{P}_q(n,d)$ and $Q \in \mathcal{P}_q(n, r-1)$, we have $\langle P, Q \rangle = 0$.
- Furthermore, for any $P \notin \mathcal{P}_q(n,d)$ and a *random* $Q \in_R \mathcal{P}_q(n, r-1)$, we have that $\langle P, Q \rangle$ is an unbiased element of $\mathbb{F}_q$.

This implies that the indicator variable for the event "$f \in \mathcal{P}_q(n,d)$" can be equivalently written as $\mathbb{1}_{f\in\mathcal{P}_q(n,d)} = \mathbf{E}_{Q\in\mathcal{P}_q(n,r-1)}\left[\omega^{\langle f,Q\rangle}\right]$, where $\omega = e^{2\pi i/q}$.

Squaring trick: We use a standard squaring trick to bound the absolute value of the quantity $\mathbf{E}_P\left[\omega^{\langle h(P),f\rangle}\right]$. Let us consider the case when $h(P) = P^2$. In this case we have

$$\begin{aligned}
\left|\mathop{\mathbf{E}}_{P}\left[\omega^{\langle P^2,f\rangle}\right]\right|^4 &= \left|\mathop{\mathbf{E}}_{P,P_1}\left[\omega^{\langle (P+P_1)^2,f\rangle}\cdot\omega^{\langle -P^2,f\rangle}\right]\right|^2 = \left|\mathop{\mathbf{E}}_{P,P_1}\left[\omega^{\langle 2PP_1+P_1^2,f\rangle}\right]\right|^2 \\
&\le \mathop{\mathbf{E}}_{P_1}\left[\left|\mathop{\mathbf{E}}_{P}\left[\omega^{\langle 2PP_1+P_1^2,f\rangle}\right]\right|^2\right] \\
&= \mathop{\mathbf{E}}_{P_1}\left[\mathop{\mathbf{E}}_{P,P_2}\left[\omega^{\langle 2(P+P_2)P_1+P_1^2,f\rangle}\cdot\omega^{\langle -(2PP_1+P_1^2),f\rangle}\right]\right] \\
&= \mathop{\mathbf{E}}_{P_1}\left[\mathop{\mathbf{E}}_{P,P_2}\left[\omega^{\langle 2P_1P_2,f\rangle}\right]\right] = \mathop{\mathbf{E}}_{P_1,P_2}\left[\omega^{\langle 2P_1P_2,f\rangle}\right]
\end{aligned}$$

A similar argument shows that when $h(P)$ is a polynomial of degree exactly k, we have

$$\left|\mathop{\mathbf{E}}_{P}\left[\omega^{\langle h(P),f\rangle}\right]\right|^{2^k} \le \mathop{\mathbf{E}}_{P_1,\ldots,P_k}\left[\omega^{\langle k!P_1\cdots P_k,f\rangle}\right]$$

We are now ready to prove Corollary 1.6.

Proof of Corollary 1.6.

$$\begin{aligned}
\Pr_{P\in\mathcal{P}_q(n,e)}\left[f\cdot h(P)\in\mathcal{P}_q(n,d+ek)\right] &= \left|\mathop{\mathbf{E}}_{P\in\mathcal{P}_q(n,e),Q\in\mathcal{P}_q(n,s-1)}\left[\omega^{\langle f\cdot h(P),Q\rangle}\right]\right| \\
&= \left|\mathop{\mathbf{E}}_{Q}\left[\mathop{\mathbf{E}}_{P}\left[\omega^{\langle h(P),fQ\rangle}\right]\right]\right|^{2^k/2^k} \\
&\le \left(\mathop{\mathbf{E}}_{Q}\left[\left|\mathop{\mathbf{E}}_{P}\left[\omega^{\langle h(P),fQ\rangle}\right]\right|^{2^k}\right]\right)^{1/2^k} \\
&\le \left(\mathop{\mathbf{E}}_{Q}\left[\mathop{\mathbf{E}}_{P_1,\ldots,P_k}\left[\omega^{\langle k!P_1\cdots P_k,fQ\rangle}\right]\right]\right)^{1/2^k} \\
&= \left(\mathop{\mathbf{E}}_{P_1,\ldots,P_k}\left[\mathop{\mathbf{E}}_{Q}\left[\omega^{\langle P_1\cdots P_kf,Q\rangle}\right]\right]\right)^{1/2^k} \\
&= \left(\Pr_{P_1,\ldots,P_k}\left[f\cdot\prod_i P_i\in\mathcal{P}_q(n,d+ek)\right]\right)^{1/2^k}
\end{aligned}$$

The corollary now follows from Theorem 1.4. ◀

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 of Lemma 1.5 (see Remark 5.1).

References

1 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.

2 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, doi:10.1137/130929394.

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

4 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). doi:10.1007/s11856-015-1231-3.

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

6 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). doi:10.1137/120879257.

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

8 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.

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

10 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.