The Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University

Local Testing of Multiplicity Codes

Tel Aviv University
Raymond & Beverly Sackler Faculty of Exact Sciences

This work is submitted as part
of the requirements for the degree
“Master of Science”

School of Mathematical Sciences

By
Dan Karliner

Under the supervision of
Professor Amnon Ta-Shma

Acknowledgements

I would like to thank my advisor, Professor Amnon Ta-Shma, for his support, for asking questions that challenge my understanding, and for many fruitful discussions.

Improved local testing for multiplicity codes

Dan Karliner and Amnon Ta-Shma

Contents

Abstract

Multiplicity codes are a generalization of Reed-Muller codes which include derivatives as well as the values of low degree polynomials, evaluated in every point in $\mathbb{F}_p^m$. Similarly to Reed-Muller codes, multiplicity codes have a local nature that allows for local correction and local testing. Recently, [KSTS22] showed that the *plane test*, which tests the degree of the codeword on a random plane, is a good local tester for *small enough degrees*. In this work we simplify and extend the analysis of local testing for multiplicity codes, giving a more general and tight analysis. In particular, we show that multiplicity codes $\mathrm{MRM}_p(m, d, s)$ over prime fields with *arbitrary* d are locally testable by an appropriate *k-flat test*, which tests the degree of the codeword on a random k-dimensional affine subspace. The relationship between the degree parameter d and the required dimension k is shown to be nearly optimal, and improves on [KSTS22] in the case of planes.

Our analysis relies on a generalization of the technique of *canonincal monomials* introduced in [HSS13]. Generalizing canonical monomials to the multiplicity case requires substantially different proofs which exploit the algebraic structure of multiplicity codes.

1 Introduction

The Reed-Muller code $\mathrm{RM}_p(m,d)$ is the set of evaluation tables of m-variate degree-d polynomials. That is, a function $f:\mathbb{F}_p^m \to \mathbb{F}_p$ is in $\mathrm{RM}_p(m,d)$ if there exists a polynomial P of degree at most d such that $f(a)=P(a)$ for any $a\in\mathbb{F}_p^m$. The RM code is a popular building block in CS constructions, due, to a large extent, to its strong local properties.

We say a code $C\subset\Sigma^n$ is *locally-testable* if given a word $w\in\Sigma^n$, the tester distinguishes between the case $w\in C$ and the case that w is ϵ-far from C while reading few characters of w. More precisely, for a code C and a word w, we define $\delta(w,C)$ to be the relative Hamming distance of w to the closest codeword in C, i.e., $\delta(w,C)=\min_{z\in C}(\Pr_{i\in[n]}(w_i\neq z_i))$. Then,

Definition 1.1. *A local tester $\mathcal{A}$ for $C\subset\Sigma^n$ is a distribution on subsets of $[n]$.*

- *We say $\mathcal{A}$ is q-query if any subset in its support is of size $\leq q$.*
- *We say $\mathcal{A}$ has soundness function s if for any $w\in\Sigma^n$,*

$$\mathrm{REJ}_{\mathcal{A}}(w)=\Pr_{S\sim\mathcal{A}}\left(w|_S\notin C|_S\right)\geq s(\delta(w,C)).$$

A typical soundness function s is of the form $s(\delta)=\min(\alpha\delta,c)$ for some fixed constants α and c. We say $\mathcal{A}$ is a good local test for C if it has a nonzero soundness function independent of n.

We also work with a weaker notion called *local characterization*. We say $\mathcal{A}$ is a local characterization for C if $REJ_{\mathcal{A}}(w)=0$ implies $w\in C$. In other words, C is defined by equations with support in $\mathcal{A}$.

Local testing Reed-Muller codes has been studied extensively and in several parameter regimes [RS96, FS95, AKK+05, KR06, BKS+10, HSS13, KM22]. A natural local tester for $\mathrm{RM}_p(m,d)$ is the *line test*, where we pick a random line and check if its restriction is consistent with a low-degree polynomial. More generally, the *k-flat test* is uniformly distributed over k-dimensional affine subspaces of $\mathbb{F}_p^m$. We denote the rejection probability of the k flat test by $\mathrm{REJ}_{k,d}$.

Let us first consider the line test for prime p. For simplicity, let us consider $\mathrm{RM}_p(m=2,d=p-1)$, i.e., codewords of polynomials in two variables of total degree at most $d=p-1$ over $\mathbb{F}_p$. The code $\mathrm{RM}_p(2,p-1)$ is non-trivial, e.g., the word w consistent with the polynomial $p(x,y)=x^{p-1}y^{p-1}$ is not in the code. On the one hand, w restricted to the line $\ell(t)=(a_1t+b_1,a_2t+b_2)$ evaluates the polynomial $g(t)=(a_1t+b_1)^{p-1}(a_2t+b_2)^{p-1}$, and because $t^p=t$ for every $t\in\mathbb{F}_p$, g behaves as the polynomial $g \bmod (t^p-t)$, which is a degree $p-1$ polynomial, and therefore passes the test. Thus, the line tests is not even a local characterization for $\mathrm{RM}_p(2,d=p-1)$.

The above reasoning can be generalized to an arbitrary number of variables, and to the k flat test. Any polynomial is equivalent (in the sense of having the same values) to one whose degree in every variable is at most $p-1$, and therefore any polynomial on k variables is equivalent to one of degree at most $d_k\stackrel{\text{def}}{=}k(p-1)$. Therefore, the k-flat test is not a local characterization for $\mathrm{RM}_p(m,d)$ when $d\geq d_k$.

Quite surprisingly, it was shown in [KR06] that for any $d<k(p-1)$ the k-flat test is a local characterization for $\mathrm{RM}_p(m,d)$, and that it has soundness independent of m. That is,

whenever the line test is not trivially bad, it is a good local test. More concretely, suppose a word $w : \mathbb{F}_p^m \to \mathbb{F}_p$ has distance δ from $\mathrm{RM}_p(m,d)$. The k-flat test selects p^k points in $\mathbb{F}_q^m$, and so the probability that a "bad" character is read is $\leq \delta p^k$. Therefore, the best soundness one could hope for in the k-flat test is δp^k. Remarkably, later analysis of the k-flat [HSS13, KM22] test shows it is essentially optimal given the number of queries in a wide range of parameters:

Theorem 1.2. *(Soundness of the RM k-flat test)[KM22] There exists a constant $c > 0$ (independent of p) such that the k-flat test rejects with probability at least $p^{-c}\min(p^k\delta, 1)$*

We note the above discussion can be generalized to prime power fields where the following is known: if $\mathbb{F}_q$ is of characteristic p then [KR06] show the k-flat test is a local characterization for $d < k(q - \frac{q}{p})$ and that this bound is tight. Additionally, in this case the k-flat test also gives a good local test.

1.1 The k-flat test for Multiplicity codes

Multiplicity codes were defined in [GW13, KSY14]. $\mathrm{MRM}_p(m,d,s)$ is the set of evaluation tables of m-variate, degree d polynomials, where in the evaluation table we record not only the function evaluation, but also the evaluations of all its derivatives up to order s. More precisely, we define a "multiplicity table" as a function $T : \mathbb{F}_p^m \to \Sigma_{m,s}$, where

$$\Sigma_{m,s} \cong \mathbb{F}_p^{\binom{m+s-1}{s-1}}$$

is indexed by m-tuples of weight less than s. Given a polynomial $P \in \mathbb{F}_p[x_1, x_2, \ldots, x_m]$ we define its evaluation table T^P as a multiplicity table satisfying, for any $x \in \mathbb{F}_p^m$ and any m-tuple $\mathbf{I}$ with $wt(\mathbf{I}) < s$,

$$T^P(x)_{\mathbf{I}} = P^{(\mathbf{I})}(x)$$

where $P^{(\mathbf{I})}(x)$ denotes the direction-$\mathbf{I}$ Hasse derivative of P at the point x (see Section 2). Then, the multiplicity code $\mathrm{MRM}_p(m,d,s)$ is defined as the set of evaluation tables of polynomials of total degree at most d. Notice that this definition makes sense even for $d > p$.

With some care, the k-flat test may be adapted to multiplicity codes. Consider the example of the line test for $s = 2, m = 2$. That is, we are given for each $\mathbb{F}_p^2$ the value of a function, as well as its derivatives in direction x and y. When restricting to a line $x = a_1t + b_1, y = a_2t + b_2$ we are not interested in the derivatives in direction x, y but rather in the one derivative in the direction of our new variable t. This corresponds to the chain rule

$$\frac{d}{dt}P(a_1t + b_1, a_2t + b_2) = a_1\frac{\partial}{\partial x}P(a_1t + b_1, a_2t + b_2) + a_2\frac{\partial}{\partial y}P(a_1t + b_1, a_2t + b_2)$$

More generally, when restricting $\mathrm{MRM}_p(m,d,s)$ to a k-flat we want to reduce the alphabet from $\Sigma_{m,s}$ to $\Sigma_{k,s}$. Given a k-flat Q with a chosen basis for its linear part $\mathbf{h}_1, \ldots, \mathbf{h}_k$, one

may define the chain rule map $\phi : \Sigma_{m,s} \to \Sigma_{k,s}$ given in [KSTS22](following the $k = 1$ case from [Kop13]) by:

$$(\phi(z))_{\mathbf{J}} = \sum_{\mathbf{I}\in\mathbb{N}^m} z_{\mathbf{I}} \cdot \sum_{\substack{\mathbf{I}_1+\cdots+\mathbf{I}_k=\mathbf{I} \\ w(\mathbf{I}_r)=j_r}} \binom{\mathbf{I}}{\mathbf{I}_1,\ldots,\mathbf{I}_k} \prod_{i=1}^{k} \mathbf{h}_k^{\mathbf{I}_k} \tag{1.1}$$

For a polynomial P, this is the map that calculates the derivative in direction $\mathbf{J}$ of $P|_Q$ from the directional derivatives of P. Accordingly, if $w : \mathbb{F}_p^m \to \Sigma_{m,s}$ is in $\mathrm{MRM}_p(m, d, s)$ then $\phi \circ w|_Q$ is in $\mathrm{MRM}_p(k, d, s)$.

1.2 For which degree can the k-flat test be effective?

Given a function $f : \mathbb{F}_p^m \to \mathbb{F}_p$ there is more than one polynomial equal to f everywhere: since we are only interested in the values of P, we may add, e.g., $x_0^p - x_0$ to P and get the same value set. More generally, we may add any polynomial in the ideal

$$\mathcal{I}_m = \langle x_1^p - x_1, x_2^p - x_2, \ldots, x_m^p - x_m \rangle$$

Any polynomial P has a unique representative mod $\mathcal{I}_m$ with all individual degrees smaller than p. We refer to it as its minimal representative. The minimal representative for P can only have a lower degree than P.

Given any polynomial P and another polynomial Q equal to it everywhere in $\mathbb{F}_p^m$, their difference evaluates to zero everywhere. Choosing the minimal representative for $P - Q$, we see by the Schwartz-Zippel lemma that this representative must in fact be 0. Therefore, P has the same evaluation table as Q if and only if $P \equiv Q \mod \mathcal{I}_m$. This, in particular, shows that any table on k variables has a representation as a polynomial of degree at most $k(p-1)$: we may reduce any individual degree to lower than $(p-1)$, and any monomial contains at most k variables.

It is established in [KSTS22] that analogously to the Reed-Muller case, two polynomials P, Q have the same multiplicity tables if and only if their difference $P - Q$ is in the ideal

$$\mathcal{I}_m^s = \left\langle \prod_{k=1}^{s} (x_{i_k}^p - x_{i_k}) \mid (i_1, \ldots, i_s) \in [m]^s \right\rangle$$

This fact establishes a degree bound on any multiplicity table given m, s. Consider, for example, the case of $s = 2$: the monomial $x^p y^p$ has degree $2p$, but by subtracting the relevant generator of $\mathcal{I}_m^2$, $(x^p - x)(y^p - y)$ we see that it is equivalent to the lower degree polynomial $x^p y + xy^p + xy$. In general, if a monomial $\prod x_i^{e_i}$ has $\sum \left\lfloor \frac{e_i}{p} \right\rfloor \geq s$ then we may subtract a multiple of one of the generators of $\mathcal{I}_m^s$ to lower its degree. It follows that any polynomial is equivalent (in the sense of having the same multiplicity table) to one with $\sum \left\lfloor \frac{e_i}{p} \right\rfloor < s$, which implies

$$d \leq d_{k,s} \stackrel{\text{def}}{=} k(p-1) + (s-1)p. \tag{1.2}$$

1.3 Previous work: The plane test is effective for degree $d < ps$.

From the previous discussion, it follows that the restriction of any multiplicity table to a k-flat can be represented by a polynomial with degree $d_{k,s}$. Therefore, the k-flat test does not characterize $\mathrm{MRM}_p(m,d,s)$ for $d \geq d_{k,s}$. As $d_{k,s}$ is larger than d_k - and significantly so for large s - one may hope that the k-flat test is a local test for larger d in the case of multiplicity codes than for Reed-Muller codes. For example, one could hope that the line test is useful even for degrees up to sp. However, a simple example in [KSTS22] shows the line test fails for $s = 2$ even for $d = p + 1$.

Local testing for multiplicity codes is studied in [KSTS22], with an emphasis on the 2-flat ("plane") test. Two main results are obtained: one for characterization and one for robustness. For characterization, [KSTS22] show that the *plane* test is a local characterization in degrees nearly reaching $d_{k,s}$. Concretely,

Theorem 1.3. *(The plane test is a local characterization) Let $\mathbb{F}_q$ be a field of size q of characteristic p and assume $s \leq \min\{d, q-1\}$. Let $d < q(s - \frac{1}{p})$. Then the plane test is a local characterization for $\mathrm{MRM}_p(m,d,s)$.*

In this paper we focus on the prime field case, in which case the condition becomes $d < ps-1$. The bound $d < ps-1$ should be compared to $d_{2,s} = 2(p-1)+(s-1)p = ps+p-2$. While not tight, this result comes close to the trivial limit $d_{2,s}$.

The second result in [KSTS22] concerns robustness. It shows that if the k-flat test is a good local test for $\mathrm{RM}_p(m,d)$ then it is also a local characterization and local test for $\mathrm{MRM}_p(m,d,s)$, albeit with worse soundness. This is intuitive because multiplicity tables contain function evaluations, and the derivatives only add more information, and what is left to be shown is that when we pass the test the derivatives are also consistent with the function evaluations.

Theorem 1.4 (Local testing is preserved from RM to MRM)**.** *[KSTS22] Let $\mathbb{F}_p$ be a field of size q of characteristic p, and assume $s \leq \min\{d, q-1\}$. Suppose for $\mathrm{RM}(q,m,d)$ there exists $\alpha > 0$ and $c_0 \leq 1$ such that for every f the rejection probability of the k-flat test satisfies*

$$\mathrm{REJ}^{\mathrm{RM}}_{k,d}(f) \geq \min\left\{\alpha \cdot \delta(f, \mathrm{RM}(q,m,d)), c_0\right\}.$$

Then, for every T we have

$$\mathrm{REJ}^{\mathrm{MRM}}_{k,d}(T) \geq \min\left\{\alpha' \cdot \delta(T, \mathrm{MRM}(q,m,d,s)), c_0\right\}$$

for

$$\alpha' = \alpha \frac{q-(s-1)}{q} \frac{1}{\alpha + q^{d/(p-1)}}$$

Combining Theorems 1.3 and 1.4 one gets that under the same conditions as in Theorem 1.3, the *plane* test is a good local test.

1.4 Our new results

The main result of this paper is a new analysis of the plane test, which is based on the canonical monomials of [HSS13], and that we explain in detail in Section 1.5.1. This new analysis is simpler, applies to general k-flat test ($k \geq 2$) rather then just the plane test, and, more importantly, is tighter. Concretely, we prove:

Theorem 1.5. *Let p be prime, $m \geq 1$, $k \geq 2$ and $s < p$. Then the k-flat test is a local characterization for $\mathrm{MRM}_p(m, d, s)$ for any $d < d_{k,s} - (s-1)$.*

Thus, the theorem generalize the plane test result of [KSTS22] to general k. Moreover, let us compare the $k = 2$ case, we see that the trivial argument shows the k-flat test must fail for $d \geq d_{2,s} = 2(p-1) + (s-1)p = (s+1)p - 2$, [KSTS22] show the test is a local characterization for $d \leq ps - 2$, and, our results show the test is a local characterization for $d \leq d_{2,s} - s = (s+1)p - s - 2$.

We remark, that as before, under the same conditions the k-flat test is also a good local test. The technique used in [KSTS22] does not give good enough soundness in the general case, so we use a different technique based on the soundness analysis in [HSS13]

Theorem 1.6. *There exist constants c_1, c_2 such that for any prime p, integers $m \geq 1$, $k \geq 2$,$s < p$ and $d < d_{k,s} - (s-1)$ the k-flat test is a local tester with soundness function $\min(\delta p^{-4s-c_1}, p^{-4s-c_2})$*

Result-wise our works raises several intriguing questions:

- The question of what is the true degree threshold is intriguing and we suspect that the true answer is indeed the bound $d_{k,s} - (s-1)$ that we obtained, i.e., that there is an example of a polynomial of degree $d_{k,s} - (s-1) + 1$ where the k-flat test fails to be a local characterization.
- Another intriguing question is the appearance of the condition $s < p$ in our results (and also in [KSTS22]). Is there an inherent obstacle that appears when we try to take the (Hasse) multiplicity above the field size?
- The state of the art RM results give nearly-optimal soundness for the k-flat test as long as it is a local characterization. Can this be done for multiplicity codes as well? For instance, is it possible to show soundness on the order of $\approx p^k \delta$ for small δ?
- This work deals with prime fields, while previous works [HSS13, KSTS22] handle general finite fields for Reed Muller codes and multiplicity codes respectively. Can the improvements in this work be applied to the general finite field case?

Next, we go on to explain the canonical monomials technique of [HSS13] and our use of it for multiplicity codes.

1.5 The technique

We continue the discussion in Section 1.2. One may think of the set of tables $\mathbb{F}_p^m \to \mathbb{F}_p$ as the same as

$$R_m \stackrel{\text{def}}{=} \mathbb{F}_p[x_1, x_2, \ldots, x_m] \mod \mathcal{I}_m.$$

This is because any two polynomials that differ by an element of $\mathcal{I}_m$ generate the same evaluation table. A convenient basis to use for R_m is

$$\mathcal{B}_m = \left\{ \prod_{i=1}^{m} x_i^{e_i} : e_i < p \right\}$$

a table is in $\mathrm{RM}_p(m, d)$ if and only if its representative, written in the basis $\mathcal{B}_m$ has only monomials of degree $\leq d$.

Similarly, multiplicity tables of multiplicity s are equivalent to elements of

$$R_{m,s} \stackrel{\text{def}}{=} \mathbb{F}_p[x_1, x_2, \ldots, x_m] \mod \mathcal{I}_m^s \tag{1.3}$$

That is, any multiplicity table has a unique representative in $R_{m,s}$, and any two polynomials have the same evaluation table if and only if their difference is in $\mathcal{I}_m^s$. We choose

$$\mathcal{B}_{m,s} = \left\{ \prod_{i=1}^{m} x_i^{e_i} : \sum_{i=1}^{m} \left\lfloor \frac{e_i}{p} \right\rfloor < s \right\} \tag{1.4}$$

as a basis for $R_{m,s}$ (this basis is different than the one chosen in [KSTS22]). Just like in the Reed-Muller case, a table is in $\mathrm{MRM}_p(m, d, s)$ if and only if its representative polynomial in $R_{m,s}$ when written in the basis $\mathcal{B}_{m,s}$ has no monomials of degree larger than d.

The k-flat test may also be conveniently phrased in the algebraic language described above. The reason this works is that if $L : \mathbb{F}_p^k \to \mathbb{F}_p^m$ is an affine map then for any P in $\mathcal{I}_m$ the composition $P \circ L$ is in $\mathcal{I}_k$. Therefore, L reduces to a map $\bar{L} : R_m \to R_k$. We can think of this as modding R_m by $m - k$ additional additional linear equations. For example, restricting to the line $\{(t, t) \mid t \in \mathbb{F}_p\} \subset \mathbb{F}_p^2$ is the same as adding the linear equation $x = y$.

Phrased this way, the k-flat test takes a polynomial $P \in R_m$, applies a random full-rank affine map $\bar{L} : R_m \to R_k$ and asks whether $\bar{L}(P)$ is of degree larger than d (when written using $\mathcal{B}_k$).

Similarly, we may view the k flat test for multiplicity codes algebraicly. Given a linear map $L : \mathbb{F}_p^k \to \mathbb{F}_p^m$, any polynomial $P \in \mathcal{I}_m^s$ has $P \circ L \in \mathcal{I}_k^s$. Therefore, L reduces to a map $\bar{L} : R_{m,s} \to R_{k,s}$. Phrased this way, the k-flat test takes a polynomial $P \in R_{m,s}$, applies a random full-rank affine map $\bar{L} : R_m \to R_k$ and asks whether $\bar{L}(P)$ is of degree larger than d (when written using $\mathcal{B}_{k,s}$). This view of the k-flat test will be crucial for the soundness analysis appearing in Section 5.

1.5.1 Canonical monomials for Reed-Muller codes

An important observation is that both the code $\mathrm{RM}_p(m, d)$ and the k-flat test are affine invariant. That is, when applying an invertible affine transformation to $\mathbb{F}_p^m$, a polynomial

remains of the same degree and a k-dimensional affine space remains one. In fact, many of the results regarding Reed-Muller codes generalize to general affine-invariant codes, see e.g. [KS08].

[HSS13] use this fact to analyze the soundness of the k-flat test. The idea is, given a polynomial P, to first find an affine transformation L that puts P into a form convenient for analyzing, and then prove the soundness for the polynomial $P \circ L$.

To this end they introduce the notion of a *canonical monomial*.

Definition 1.7. *[HSS13, Definition 4.1] A canonical monomial of degree d in $n \leq m$ variables in $\mathbb{F}_p[x_1, \ldots, x_m]$ is a monomial $\prod_{i=1}^{n} x_i^{e_i}$ such that (1) $\sum_{i=1}^{m} e_i = d$ (2) For every $1 \leq i < n$ $e_i = p - 1$ (3) $e_n \leq p - 1$*[1].

Intuitively, this is a monomial which is supported on as few variables as possible.

[HSS13] go on to show that any polynomial can be composed with a linear map L so that $P \circ L$ contains a canonical monomial of degree $\deg P$. Such a map is given by the linear transformation maximizing (in the graded lexicographic order) the maximal monomial of $P \circ L$. The proof contains two stages:

- First, the result is shown for the special case $m = 2$.
- An inductive argument generalizes this to any number of variables.

We recount the $m = 2$ case here.

Lemma 1.8. *[HSS13, Lemma 4.2] Let $f(x_1, x_2)$ be a degree $d \leq 2(p-1)$ polynomial in $F_p[x_1, x_2]$. Then there exists $\alpha \in \mathbb{F}_p$ such that $f(x_1, x_2 + \alpha x_1)$ contains a canonical monomial of degree d.*

Proof. Write $f(x_1, x_2) = \sum_{e:0 \leq e, d-e < p} \alpha_e x_1^e x_2^{d-e}$. Monomials of degree lower than d may be ignored because they will never affect the degree-d homogeneous part of $f \circ L$. Let $e_{\max}$ be the maximal degree of x_1 in f. If $e_{\max} = p - 1$ we are done. Otherwise, consider the polynomial $f(x_1, x_2 + z x_1)$. By the binomial theorem it follows that

$$f(x_1, x_2 + z x_1) \equiv_{\mathcal{I}_2} \sum_{e \leq d} \alpha_e x_1^e \sum_{r \leq d-e} \binom{d-e}{r} (z x_1)^r x_2^{d-e-r}$$

Look at the coefficient of $x_1^{e_{\max}+1} x_2^{d-(e_{\max}+1)}$ as a polynomial in z. It is equal to

$$\sum_{r \leq e_{\max}+1} \alpha_{e_{\max}+1-r} \binom{d - (e_{\max} + 1 - r)}{r} z^r$$

This is a polynomial of degree at most $p - 1$. It is not the zero polynomial because the coefficient of z is $\alpha_{e_{\max}} \binom{d-e_{\max}}{1} \neq 0 \mod p$. Therefore, it is nonzero when $z = \alpha$ for some $\alpha \in \mathbb{F}_p$.

In this way we may increase the maximal degree of x_1 until we obtain a maximal monomial. □

[1] The definition for prime power fields is more complicated.

1.5.2 Canonical monomials for multiplicity codes

When composed with the correct chain rule map defined in Equation (1.1), multiplicity codes are also affine invariant. Similarly to [HSS13] we want to establish a canonical monomial result for multiplicity codes. This is made more complicated by the fact that individual degrees may be larger than p.

Let $s = 2$. The polynomial $D_2 = x_2^p x_1 - x_2 x_1^p$ is the minimal representative of its class in $R_{2,2}$. For a linear map $L : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ we have $D_2 \circ L = \det(L) D_2$. Therefore, despite the fact that the degree of x_1 is not at the maximum possible value, we cannot shift the monomial $x_1^p y_1$ into x_1^{p+1}.

Where does the proof of Lemma 1.8 fail? Looking at the coefficient of x_1^{p+1} in $f(x_1, x_2 + zx_1)$, we see it is equal to $g(z) \stackrel{\text{def}}{=} z - z^p$. While this polynomial is nonzero, it still evaluates to 0 everywhere on $\mathbb{F}_p$. This is possible because its degree is larger than p.

Let P be a reduced polynomial in $R_{2,2}$ of degree $d < 2p$. As in the proof of Lemma 1.8, the coefficient of x_1^d in $P(x_1, x_2 + zx_1)$ is

$$c_d(z) = \sum_{r \le d} \alpha_{d-r} z^r$$

As seen above, this polynomial may be 0 everywhere, in which case we may not be able to achieve the monomial x_1^d. This happens precisely when $g(z) = z^p - z \mid c_d$.

Compromising, we next look at the coefficient of $x_1^{d-1} x_2$.

$$c_{d-1}(z) = \sum_{r \le d-1} \alpha_{d-1-r} \binom{r+1}{1} z^r$$

It is readily observed that c_{d-1} is in fact the *Hasse derivative* of c_d. If both c_d and c_{d-1} are zero everywhere in F_p, it follows that in fact $g(z)^2 \mid c_d$. However, this implies that P has degree at least $2p$, a contradiction. Therefore, we see that when $d < 2p$ either the monomial x_1^d or $x_1^{d-1} x_2$ can be achieved. Paying some more attention to this argument, we can in fact show that the only case when x_1^d cannot be achieved is when $D_2 \mid P$.

For larger s, the polynomial D_2^{s-1} has leading monomial $x_1^{q(s-1)} x_2^{s-1}$, and due to its linear invariance we cannot get a higher degree for x_1. The argument from the preceding paragraph can be applied, and it shows that (if $d < ps$) one of the monomials $x_1^d, x_1^{d-1} x_2, \ldots, x_1^{d-(s-1)} x_2^{s-1}$ must appear in some composition $P \circ L$.

The case $d \ge ps$ is trickier but still true. In general, we prove

Theorem 1.9. *Let p be prime, $s < p$ and let P be a reduced polynomial in $R_{2,s}$ of degree d. Let $d^x_{\max} p(s-1) + (p-1)$ and let $d^x_{opt} = \min(d, d^x_{\max})$. There exists a linear map $L : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ such that $P \circ L$ contains a monomial $x_1^e x_2^{d-e}$ with $e \ge d^x_{opt} - (s-1)$.*

We clarify the different degree variables introduced so far:

- The degree $d_{m,s}$ is the highest total degree a reduced polynomial in $\mathcal{B}_{m,s}$ can have.
- The degree $d^x_{\max}$ is the highest degree in x_1 a reduced polynomial in $\mathcal{B}_{m,s}$ can have.

- The degree d^x_{opt} is the highest degree in x_1 we might hope for $P \circ L$ to have. Indeed, by definition its degree in x_1 will be $\leq d^x_{\max}$, and the total degree of $P \circ L$ is d, so its degree in x_1 cannot be larger than this.

The proof of this theorem is given in Section 3. The proof, while similar in spirit to Lemma 1.8 requires analyzing several of the polynomials c_k together as well as careful use of which monomials exist in $\mathcal{B}_{m,s}$ and which do not.

We state a simple corollary of Theorem 1.9

Corollary 1.10. *Under the same assumptions as Theorem 1.9, there exists a linear map $L : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ such that the maximal monomial of $P \circ L$, $x_1^a x_2^b$ satisfies $b \leq p-1$.*

Proof. We take the same linear map as in Theorem 1.9. Suppose $d^x_{\max} = d$. Then $a \geq d-(s-1)$ and so $b \leq (s-1) < p-1$. The other case is $d^x_{\max} = p(s-1)+(p-1)$ in which case $a \geq p(s-1)$ and so due to $x_1^a x_2^b$ being in $\mathcal{B}_{2,s}$ it must be the case that $b < p$. □

Like in the Reed-Muller case, Theorem 1.9 can be extended inductively to a canonical monomial statement about general multivariate polynomials. The reduction is slightly more complicated because the product of an $\mathcal{I}^s_{m_1}$-reduced polynomial and an $\mathcal{I}_{m_2}$-reduced polynomial is not necessarily $\mathcal{I}_{m_1+m_2}$ reduced when $s > 1$.

Taking a slightly different approach from the Reed-Muller definitions, we define canonical monomials as the highest (in graded lexicographic order) monomial achievable by composing with a linear map, and then display their properties.

Definition 1.11 (Canonical monomial - general s)**.** *Let m, s be integers, $m \geq 2$, $s \geq 1$. Let $P \in \mathbb{F}_p[X_1, \ldots, X_m]$ be reduced modulo $\mathcal{I}^s_m$. The* canonical monomial *of P modulo $\mathcal{I}^s_m$, denoted* $\text{Can}(P, m, s)$*, is the largest leading monomial of $P \circ L \bmod \mathcal{I}^s_m$ in the deg-lex ordering (where $X_1 > \ldots > X_m$), where the maximum is taken over all linear transformations $L : \mathbb{F}_p^m \to \mathbb{F}_p^m$.*

Theorem 1.12 (Canonical monomials - general s)**.** *Let p be a prime, $m \geq 2$ and $s \leq p-2$. Let $P \in \mathbb{F}_p[X_1, \ldots, X_m]$ be reduced modulo $\mathcal{I}^s_m$ and suppose $\prod_{i=1}^m x_i^{e_i} \in \mathcal{B}_{m,s}$ is the canonical monomial of P modulo $\mathcal{I}^s_m$. Then,*

1. $\sum_{i=1}^m e_i = \deg(P)$
2. $e_i \geq e_{i+1}$ *for all* $i \in [m-1]$.
3. $e_1 \geq \min\{p(s-1)+(p-1), d\} - (s-1)$.
4. *If n is the last integer such that $e_n > 0$, then $e_i = p-1$ for all $i \in \{2, \ldots, n-1\}$.*

This theorem is proved in Section 4.

1.5.3 Canonical monomials imply characterization

The canonincal monomial result Theorem 4.3 is used in the proof of our main results on the local characterization and soundness of the k-flat test, Theorem 1.5 and Theorem 1.6. As a warmup, we use it to show that the plane test is a local characterization, up to a better than the one achieved in [KSTS22].

Theorem 1.13. *Let p be a prime, let m be an integer and let $s \leq p$. Let P be a reduced polynomial in $R_{m,s}$ of degree d. Then there exists a full rank affine map $L : \mathbb{F}_p^2 \to \mathbb{F}_p^m$ such that $\deg(P \circ L) \bmod \mathcal{I}_2^s \geq \min(d, d_{2,s} - (s-1))$. In particular, for $d < d_{2,s} - (s-1)$ the plane test is a local characterization for $\mathrm{RM}_p(m,d)$.*

Proof. Replacing P by $P \circ L$ if necessary, using Theorem 1.12 we may assume that P contains a degree d canonincal monomial $\prod_{i=1}^n x_i^{e_i}$.

Essentially, we show that we may pick the plane to be parallel to the x_1, x_2 axes - the degrees of x_1, x_2 will be large enough and the other variables may be set to constants to not interfere with x_1, x_2.

We begin by noting that $e_1 + e_2 \geq \min(d, p(s-1) + 2(p-1) - (s-1))$. Indeed, if $e_3 = 0$ we have $e_1 + e_2 = d$ and we are done. Otherwise, $e_2 = p - 1$ in which case

$$\begin{aligned} e_1 + e_2 &\geq \min(d, p(s-1) + p - 1) - (s-1) + (p-1) \\ &\geq \min(d - (s-1) + (p-1), p(s-1) + 2(p-1) - (s-1)) \\ &\geq \min(d, p(s-1) + 2(p-1) - (s-1)) \end{aligned}$$

Where the last inequality uses $s \leq p$.

We build the affine map by setting all $x_i, i > 2$ to be some constants, retaining the monomial $x_1^{e_1} x_2^{e_2}$. We write out P while separating the first two variables from the others:

$$P = \sum_{d_1, d_2} x_1^{d_1} x_2^{d_2} \sum_{d_3, \ldots, d_m} \alpha_{d_1, \ldots, d_m} \prod_{i=3}^m x_i^{d_i}$$

Because P contains the canonical monomial, we know

$$\sum_{d_3, \ldots, d_m} \alpha_{e_1, e_2, d_3, \ldots, d_m} \prod_{i=3}^m x_i^{d_i} \neq 0$$

Additionally, for any $d_3, \ldots, d_m$ such that $\alpha_{e_1, e_2, d_3, \ldots, d_m} \neq 0$ we have $d_i < p$. Indeed, if $e_1 + e_2 = d$ this claim is trivial. Otherwise, $e_1 + e_2 \geq p(s-1) + 2(p-1) - (s-1)$ in which case $\lfloor \frac{e_1}{p} \rfloor + \lfloor \frac{e_2}{p} \rfloor = s - 1$, which implies $d_i < p$ for all $i \geq 3$.

It follows that the polynomial

$$\sum_{d_3, \ldots, d_m} \alpha_{e_1, e_2, d_3, \ldots, d_m} \prod_{i=3}^m x_i^{d_i}$$

Is a nonzero polynomial with all degrees smaller than p, and therefore it is nonzero for some substitution $x_3 = a_3, \ldots, x_m = a_m$. Making this substitution, we see that the monomial $x_1^{e_1} x_2^{e_2}$ has a nonzero coefficient. □

This method of proof would work to prove the general local characterization result for the k-flat test, Theorem 1.5. To prove our soundness estimate Theorem 1.6 we need another ingredient.

1.5.4 Canonical monomials imply local testing

Suppose a reduced polynomial P in $R_{m,s}$ has degree $> d$ and distance δ from $\mathrm{MRM}_p(m,d,s)$. Informally, the approach to proving the robustness of the plane test in [KSTS22] is to select a plane by first selecting an intermediate uniform $2s$-dimensional subspace H, and within it a uniform plane Q. The reason this method has soundness on the order of $p^{-O(s)}$ is:

- Due to Theorem 1.4 with probability $\geq \delta\frac{1}{p}$ the restriction $P|_H$ has degree $> d$.
- Due to Theorem 1.3 at least one plane Q in H has $\deg P|_Q > d$.
- The number of planes in H is $O(p^{cs})$ for some constant c, so the overall soundness is $\geq \delta\Omega(p^{-cs-1})$.

When attempting to generalize this approach to the general k-dimensional test, some issues occur. The degree bound on d is $\approx (p-1)k + (s-1)p$, so the intermediate space H needs to have dimension $k+2s$. In this case the first step still works. However, the number of k-dimensional subspaces in $\mathbb{F}_p^{k+2s}$ can be on the order of $p^{O(ks+s^2)}$, and this would affect the soundness.

Instead, we replace the second stage with a stronger statement regarding the soundness of the k-dimensional test within $\mathbb{F}_p^{k+2s}$, analogous to the following lemma in [HSS13].

Lemma 1.14 ([HSS13], Lemma 4.6)**.** *Let $d < k(p-1)$ and let $f : \mathbb{F}_p^{k+1} \to \mathbb{F}_p$ have degree larger than d. Then the k-dimensional test rejects f with probability $\geq \frac{1}{p}$.*

For the case of multiplicity codes, we show

Lemma 1.15. *Let $d < k(p-1) + (s-1)p - (s-1)$ and let $f : \mathbb{F}_p^{k+1} \to \Sigma_{k+1,s}$ have degree larger than d. Then the k-dimensional test rejects f with probability $\geq \frac{1}{p^2}$.*

This lemma is then applied repeatedly $2s$ times, showing total soundness of at least p^{-4s}.

It follows that the probability that a k-dimensional subspace Q within the intermediate subspace H has $\deg P|_Q > d$ is at least $p^{-O(s)}$, giving Theorem 1.6.

2 Preliminaries

For a comprehensive survey of multiplicity codes, see [Kop13]. We present some properties that we use here for completeness. We denote the polynomial ring $\mathbb{F}_p[X_1, \ldots, X_m]$ by $F[\mathbf{X}]$. Given a non-negative tuple $\mathbf{i} = (i_1, \ldots, i_m)$, $\mathbf{X}^\mathbf{i}$ denotes the monomial $\prod_{j=1}^m X_j^{i_j}$.

Definition 2.1 (Hasse derivative)**.** *For $P(\mathbf{X}) \in \mathbb{F}_p[\mathbf{X}]$ and a non-negative tuple $\mathbf{i}$, the direction $\mathbf{i}$ Hasse derivative of P, denoted $P^{(\mathbf{i})}(\mathbf{X})$ is the coefficient of $\mathbf{Z}^\mathbf{i}$ in the polynomial $P(\mathbf{X}+\mathbf{Z})$*

Proposition 2.2 (Basic properties of Hasse derivatives)**.** *Let $P(\mathbf{X}), Q(\mathbf{X}) \in \mathbb{F}_p[\mathbf{X}]^m$ and let $\mathbf{i}$, $\mathbf{j}$ be vectors of non-negative tuples. Then:*

1. $P^{(\mathbf{i})}(\mathbf{X}) + Q^{(\mathbf{i})}(\mathbf{X}) = (P+Q)^{(\mathbf{i})}(\mathbf{X})$.

2. $(P \cdot Q)^{(\mathbf{i})}(\mathbf{X}) = \sum_{0 \leqslant \vec{e} \leqslant \mathbf{i}} P^{(\vec{e})}(\mathbf{X}) \cdot Q^{(\mathbf{i}-\vec{e})}(\mathbf{X})$.

3. $\left(P^{(\mathbf{i})}\right)^{(\mathbf{j})}(\mathbf{X}) = \binom{\mathbf{i}+\mathbf{j}}{\mathbf{i}} P^{(\mathbf{i}+\mathbf{j})}(\mathbf{X})$.

Definition 2.3 (Vanishing multiplicity)**.** *We say a polynomial P has* vanishing multiplicity *s at x, and write* $\mathrm{Mult}(P; x) \geq s$*, if for any $\mathbf{i}$ with $wt(\mathbf{i}) < s$, $P^{(\mathbf{i})}(x) = 0$. We say P vanishes with multiplicity exactly s at x, if* $\mathrm{Mult}(P; x)$ *is at least s but not $s+1$.*

A simple fact derived from Item 2 is:

Fact 2.1. $\mathrm{Mult}(P \cdot Q; x) \geq \mathrm{Mult}(P; x) + \mathrm{Mult}(Q; x)$.

Any polynomial of the form $x_i^p - x_i$ vanishes on the entire space $\mathbb{F}_p^m$. Therefore, any product of s of these will vanish with multiplicity s. In fact, any polynomial that vanishes with multiplicity s is in the ideal generated by these products.

Fact 2.2 (See, e.g. [KSTS22])**.** *A polynomial has vanishing multiplicity $\geq s$ if and only if*

$$P \in \mathcal{I}_m^s = \left\langle \prod_{k=1}^{s} (x_{i_k}^p - x_{i_k}) \mid (i_1, \ldots, i_s) \in [m]^s \right\rangle$$

Lemma 2.4. *Let P be a bivariate homogeneous polynomial, and $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p \setminus (0, 0)$. Then,* $\mathrm{Mult}(P; (a, b)) \geq t$ *iff $(bx - ay)^t | P$.*

Proof. From Item 2 it is clear that $(bx - ay)^t | P$ implies $\mathrm{Mult}(P; (a, b)) \geq t$. We prove the other direction by induction on t. Suppose $\mathrm{Mult}(P; (a, b)) \geq t$, and let $d = \deg(P)$.

For $t = 1$, suppose w.l.o.g. that $b \neq 0$ and define $p(x) = P(x, 1)$. Then

$$0 = P(a, b) = P(b \cdot (\frac{a}{b}, 1)) = b^d \cdot p(\frac{a}{b}).$$

Thus $p(\frac{a}{b}) = 0$ and $(x - \frac{a}{b}) | p$, i.e., $(bx - a) | p$. Then, the homogeneous form of $bx - a$ divides the homogeneous form of p, i.e., $(bx - ay) | P$.

Now let us assume for $t \geq 1$ and prove for $t + 1$. Suppose $\mathrm{Mult}(P; (a, b)) \geq t + 1$. Then, by induction, $P = (bx - ay)^t \cdot Q$ for some homogeneous polynomial Q. Let $\mathbf{i}$ be of weight t. Then,

$$0 = P^{(\mathbf{i})}(a, b) = Q^{(0,0)}(a, b) \cdot ((bx - ay)^t)^{\mathbf{i}}(a, b),$$

because all $(bx - ay)^t$ derivatives of weight less than t vanish. However, for some $\mathbf{i}$ of weight t we must have $((bx - ay)^t)^{\mathbf{i}}(a, b) \neq 0$ (e.g., if $a \neq 0$, take $\mathbf{i} = (t, 0)$) and therefore $Q(a, b) = 0$. Thus, by the base case, $bx - ay | Q$, and therefore $(bx - ay)^{t+1} | P$ as desired. □

2.1 The Moore matrix

We pay special attention to the case where $m = 2$ and P is homogeneous. The Moore matrix of order 2 is $\begin{pmatrix} x & x^p \\ y & y^p \end{pmatrix}$ and the Moor determinant of order 2 is

$$D_2(x, y) \stackrel{\text{def}}{=} \det \begin{pmatrix} x & x^p \\ y & y^p \end{pmatrix} = xy^p - yx^p.$$

D_2 is an example of a homogeneous polynomial with vanishing multiplicity 1 (as it can be expressed as $x(y^p - y) - y(x^p - x) \in \mathcal{I}_2$). As D_2 vanishes on the whole of $\mathbb{F}_p \times \mathbb{F}_p$, by Lemma 2.4 we get the well known fact:

Fact 2.3.

$$D_2(x, y) = (-y) \cdot \prod_{a \in \mathbb{F}_p} (x - ay).$$

This is true since D_2 must be divisible by all these factors because it vanishes on the corresponding points, these factors are co-prime, and the degree and leading coefficient of both sides match. We show D_2 is essentially the only example of a bivariate homogeneous polynomial vanishing over $\mathbb{F}_q \times \mathbb{F}_q$:

Lemma 2.5. *Let $s < p$. Suppose P is a degree-d homogeneous polynomial that vanishes over $\mathbb{F}_p \times \mathbb{F}_p$ with multiplicity s. Then P is divisible by D_2^s.*

Proof. For every point $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p \setminus (0, 0)$ such that $\mathrm{Mult}(P; (a, b)) \geq s$, we have by Lemma 2.4 that $(bx - ay)^t | P$. Taking the points $\{(a, 1)\}_{a \in \mathbb{F}_p *}$ and $(1, 0)$ we see that $(-y)^t, (x - ay)^t$ divide P, for every $a \in \mathbb{F}_p^*$. As these polynomials are co-prime we get that their product divides P. Using Fact 2.3 we see that $D_2^t | P$ as desired. □

We also need:

Lemma 2.6. *Let $P = \sum_i \alpha_i x^i y^{d-i}$ be a degree-d homogeneous bivariate polynomial. Suppose P is divisible by D_2^r. Then each polynomial*

$$P_c = \sum_{i \equiv c \mod (p-1)} \alpha_i x^i y^{d-i},$$

is individually divisible by D_2^r.

Proof. Let $P = D_2^r \cdot Q$. Write $Q = \sum_i \beta_i x^i y^{d-i}$, and define

$$Q_c = \sum_{i \equiv c \mod (p-1)} \beta_i x^i y^{d-i}.$$

Notice that all the powers of x in $D_2^r = (xy^p - x^p y)^r$ are $r \bmod (p-1)$. Therefore, $P_c = D_2^r \cdot Q_{c-r \bmod (p-1)}$. □

2.2 The basis $\mathcal{B}_{m,s}$

We recall the definition

$$\mathcal{B}_{m,s} = \left\{ \prod_{i=1}^m x_i^{e_i} : \sum_{i=1}^m \left\lfloor \frac{e_i}{p} \right\rfloor < s \right\}$$

We set up the notation $e_i = pe_i^1 + e_i^0$ where $e_i^0 < p$. That is, $e^1 e^0$ is the base p expansion of e. Due to working with $s < p$, we require only two digits for the exponents. With this notation, the restriction on the set of exponents becomes $\sum_{i=1}^m e_i^1 < s$.

We pay special attention to which monomials $\mathbf{X}^e$ appear in $\mathcal{B}_{m,s}$:

- For $d < ps$, any monomial of degree d is contained in $\mathcal{B}_{m,s}$. Indeed, if $\sum_{i=1}^{m} e_i^1 \geq s$ then $d = \sum e_i \geq ps$.
- On the other hand, the highest possible degree is

$$d_{m,s} = p(s-1) + (p-1)m.$$

  Indeed, $p\sum_{i=1}^{m} e_i^1$ is bounded by $p(s-1)$ and $\sum_{i=1}^{m} e_i^0$ is bounded by $(p-1)m$. We now check which monomials of degree $ps \leq d \leq d_{m,s}$ appear in $\mathcal{B}_{m,s}$.

The case $m = 2$ will be of special interest.

Fact 2.4. *The highest degree in x a monomial in $\mathcal{B}_{2,s}$ can have is*

$$d^x_{\max} = p(s-1) + (p-1) = ps - 1.$$

Claim 2.7. *Let $s < p$ and and suppose $d = d^x_{\max} + d_{gap}$ where $d_{gap} \geq 0$ (and notice that $d_{gap} \leq p-1$). The monomial $x^i y^{d-i}$ is in $\mathcal{B}_{2,s}$ if and only if $0 \leq i \leq d$ and $i \bmod p \in \{d_{gap}, d_{gap}+1, \ldots p-1\}$.*

Proof. Fix $x^i y^{d-i}$. Let us denote $j = d - i$. We have:

$$\begin{aligned} i + j &= d = d^x_{\max} + d_{gap} = ps - 1 + d_{gap}, \text{ and,} \\ i + j &= p(i^1 + j^1) + (i^0 + j^0) \end{aligned}$$

and hence

$$ps + d_{gap} - 1 = p(i^1 + j^1) + (i^0 + j^0). \tag{2.1}$$

Now, if $x^i y^{d-i}$ is in $\mathcal{B}_{2,s}$ then, by definition, $i^1 + j^1 \leq s - 1$. In fact $i^1 + j^1 = s - 1$ for otherwise $i^0 + j^0 \leq 2(p-1)$ cannot complete $p(s-2)$ to $d \geq ps - 1$. Thus,

$$i^0 + j^0 = p - 1 + d_{gap}.$$

As $j^0 \leq p - 1$ we have $i^0 \geq d_{gap}$ as desired.

For the other direction, if $x^i y^{d-i}$ is not in $\mathcal{B}_{m,s}$ then $i^1 + j^1 \geq s$. Hence,

$$ps + d_{gap} - 1 = p(i^1 + j^1) + (i^0 + j^0) \geq ps + i_0 + j_0.$$

It follows that $i_0 \leq i_0 + j_0 \leq d_{gap} - 1$ as desired. □

Our next lemma shows that a homogeneous polynomial with few monomials (like the monomials allowed in Claim 2.7) cannot have high vanishing multiplicity over $\mathbb{F}_p \times \mathbb{F}_p$. Equivalently, using Section 2.1, it cannot be divisible by a high power of D_2.

Lemma 2.8. *Let $P = \sum_i \alpha_i x^i y^{d-i}$ be a non-zero, degree-d homogeneous bivariate polynomial, reduced modulo $\mathcal{I}^s_m$ for $s < p$. Suppose further that the set*

$$\{i \bmod p \mid \alpha_i \neq 0\} \subseteq \{t, t+1, \ldots, t+k\},$$

i.e., it is contained in a consecutive sequence of at most $k+1$ integers. Then P is not divisible by D_2^{k+1}.

Proof. Let c be such that $P_c = \sum_{i \equiv c \bmod (p-1)} \alpha_i x^i y^{d-i}$ is non-zero. We can write

$$P_c = \sum_{j \in J} \alpha_{c+j(p-1)} x^{c+j(p-1)} y^{d-(c+j(p-1))},$$

for some non-empty $J \subset \mathbb{N}$, where for every $j \in J$, $\alpha_{c+j(p-1)} \neq 0$.

Claim 2.9. $J \subseteq \{c-t-k, \ldots, c-t\}$.

Proof. As P is reduced modulo $\mathcal{I}_m^s$ its degree in x is at most $ps-1$. Therefore, for $j \in J$, $c + j(p-1) < ps$. Hence, $j < p \cdot \frac{s}{p-1} \leq p$. Now notice that $c + j(p-1) = c - j \bmod p$. Thus, the assumption that $\{i \bmod p \mid \alpha_i \neq 0\}$ is contained in $\{t, \ldots, t+k\}$, implies that $J \subseteq \{c-t-k, \ldots, c-t\}$. □

Therefore, the number of nonzero monomials in P_c is at most $k+1$ (because different j lead to different $i \bmod p$, as $j < p$) and it can be written as

$$\begin{aligned} P_c &= \sum_{j=c-t-k}^{c-t} \alpha_{c+j(p-1)} x^{c+j(p-1)} y^{d-(c+j(p-1))} \\ &= x^{c+(c-t-k)(p-1)} y^{d-c-(c-t)(p-1)} \sum_{j=0}^{k} \alpha_{c+(c-t-k+j)(p-1)} x^{j(p-1)} y^{(k-j)(p-1)}. \end{aligned}$$

Suppose r is the largest integer such that D_2^r divides P. By Lemma 2.6 D_2^r divides P_c. By Fact 2.3, $\prod_{a \in \mathbb{F}_p^*} (x - ay)$ divides D_2, and therefore

$$\left(\prod_{a \in \mathbb{F}_p^*} (x - ay)\right)^r \mid \sum_{j=0}^{k} \alpha_{c+(c-t-k+j)(p-1)} x^{j(p-1)} y^{(k-j)(p-1)}.$$

Thus, a polynomial of degree $r(p-1)$ divides a polynomial of degree $k(p-1)$. It follows that $r \leq k$ as desired. □

3 The two variable case

We restate the main result proven in this section.

Theorem 3.1. *Let p be prime, $2 \leq s < p$, and let P be a reduced polynomial in $R_{2,s}$ of degree d. Let*

$$d^x_{opt} = \min\left(d, d^x_{\max}\right) = \min\left(d, p(s-1) + (p-1)\right).$$

There exists a linear map $L : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ such that $P \circ L \bmod \mathcal{I}_m^s$ contains a monomial $x^i y^{d-i}$ with $i \geq d^x_{opt} - (s-1)$.

Recall that d^x_{opt} is the highest degree we could hope for $P \circ L$ to have in x: its degree in x cannot be higher than d and cannot be higher than $d^x_{\max}$. The lemma states that while we cannot guarantee reaching d^x_{opt}, we can get close to it.

Proof. We first note that it suffices to prove the lemma in the case where P is a degree d homogeneous polynomial. Indeed, given a general polynomial P of degree d, express it as $P = P_d + P_{rest}$, where P_d is homogeneous degree d, and $\deg(P_{rest}) < d$. Thus, if we know the result for homogeneous polynomials, then $P_d \circ L$ contains a monomial as required, and $P_{rest} \circ L$ cannot cancel that monomial, because $\deg(P_{rest} \circ L) \leq \deg(P_{rest}) < d$, and therefore all monomials in $P_{rest} \circ L$ have degree smaller than d.

So assume P is homogeneous of degree d and write $P = \sum_{i=0}^{d} \alpha_i x^i y^{d-i}$. Let $MON(P)$ be the union over all linear maps $L : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ of the monomials of $\mathcal{B}_{m,s}$ that appear in $(P \circ L) \bmod \mathcal{I}_{m,s}$.

Claim 3.2. *Suppose $\ell < p$. If $x^{d-\ell}y^\ell$ appears in $\mathcal{B}_{m,s}$ but not in $MON(P)$ then for every t_1, t_2 such that $t_1 + t_2 = \ell$, $P^{(t_1,t_2)}$ vanishes over $\mathbb{F}_p \times \mathbb{F}_p$.*

Proof. Suppose for any linear map $L : x \to a_1 x + a_2 y$, $y \to b_1 x + b_2 y$ the coefficient of $x^{d-\ell}y^\ell$ in $(P \circ L) \bmod \mathcal{I}_{m,s}$ is 0. We write out the coefficient of $x^{d-\ell}y^\ell$ explicitly:

$$\begin{aligned} P \circ L(x,y) &= \sum_{i=0}^{d} \alpha_i (a_1 x + a_2 y)^i (b_1 x + b_2 y)^{d-i} \\ &= \sum_{i=0}^{d} \alpha_i \sum_{\ell=0}^{d} x^{d-\ell} y^\ell \sum_{t_1+t_2=\ell} \binom{i}{t_1} a_1^{i-t_1} a_2^{t_1} \cdot \binom{d-i}{t_2} b_1^{d-i-t_2} b_2^{t_2}. \end{aligned}$$

Therefore, the coefficient of $x^{d-\ell}y^\ell$ in $P \circ L$ is

$$c_\ell(a_1, a_2, b_1, b_2) = \sum_{i=0}^{d} \alpha_i \sum_{t_1+t_2=\ell} \binom{i}{t_1} a_1^{i-t_1} a_2^{t_1} \cdot \binom{d-i}{t_2} b_1^{d-i-t_2} b_2^{t_2}$$

We now look at $(P \circ L) \bmod \mathcal{I}_{m,s}$. Notice that each monomial $x^i y^j$ either appears in $\mathcal{B}_{m,s}$, in which case it is left untouched, or not, in which case it gets reduced and becomes a strictly lower degree polynomial. By assumption $x^{d-\ell}y^\ell$ appears in $\mathcal{B}_{m,s}$ and is reduced modulo $\mathcal{I}_{m,s}$. It also has total degree d, and therefore cannot be mixed with residues from other terms. Thus, the fact that it does not appear in $MON(P)$ implies that $c_\ell(a_1, a_2, b_1, b_2) = 0$ for all $a_1, a_2, b_1, b_2 \in \mathbb{F}_p$.

Now fix arbitrary $a_1, a_2 \in \mathbb{F}_p$ and look at $C_{\ell,a_1,a_2}(a_2, b_2) = c_\ell(a_1, a_2, b_1, b_2)$. C_{ℓ,a_1,a_2} is a homogeneous polynomial in a_2, b_2 of degree $\ell < p$. Since it is zero on all of $\mathbb{F}_p \times \mathbb{F}_p$, by Schwartz-Zippel it must be the zero polynomial. Hence, for all $(a_1, a_2) \in \mathbb{F}_p \times \mathbb{F}_p$ and all t_1, t_2 such that $t_1 + t_2 = \ell$, we have:

$$\sum_{i=0}^{d} \alpha_i \cdot \binom{i}{t_1} a_1^{i-t_1} \cdot \binom{d-i}{t_2} b_1^{d-i-t_2} = 0.$$

The value on the left is $P^{(t_1,t_2)}(a_1, a_2)$, and therefore

$$P^{(t_1,t_2)}(a_1, a_2) = 0$$

□

Claim 3.3. *If $d^x_{opt} = d$, P contains a monomial $x^e y^{d-e}$ with $e \geq d^x_{opt} - (s-1)$.*

Proof. Suppose $d^x_{\max} = d$. We want to show there exists a monomial $x^{d-\ell}y^\ell \in MON$ with $0 \leq \ell \leq s-1$, because then $d - \ell = d^x_{\max} - \ell \geq d^x_{\max} - (s-1)$ as desired.

Suppose not. Then, for every $0 \leq \ell \leq s-1$, $x^{d-\ell}y^\ell$ is not in MON. Also, notice that for every such ℓ, $x^{d-\ell}y^\ell$ is a monomial in $\mathcal{B}_{m,s}$ (because $d \leq d^x_{\max}$ and $\ell < s < q$). Thus, by Claim 3.2, and using $s - 1 < p$, $P^{(t_1,t_2)}$ vanishes over $\mathbb{F}_p \times \mathbb{F}_p$ for all (t_1, t_2) such that $t_1 + t_2 < s$. In other words, $\text{Mult}(P, \mathbb{F}_p^2) \geq s$ and $P \in I_{2,s}$. Thus, the reduced form of P in $R_{2,s}$ is zero. A contradiction to P being degree d. □

Define

$$d_{gap} = d - d^x_{\text{opt}}.$$

When $d_{gap} = 0$, i.e., $d^x_{\text{opt}} = d$, we proved the theorem (Claim 3.3). We now assume $d_{gap} > 0$. Define

$$r = \min\{p - 1 - d_{gap}, s - 1\}.$$

Lemma 3.4. *If $d_{gap} \geq 0$ then for every (t_1, t_2) with $t_1 + t_2 = d_{gap}$, $P^{(t_1,t_2)}$ is not divisible by D_2^{r+1}.*

Proof. As $r = \min\{p - 1 - d_{gap}, s - 1\}$ we have two cases:

- Case 1: $r = s - 1$.

  Let $\alpha x^i y^j$ be a monomial in P with a nonzero coefficient ($i + j = d$). Let (t_1, t_2) be such that $t_1 + t_2 = d_{gap}$. The derivative $P^{(t_1,t_2)}$ contains the term $\alpha\binom{i}{t_1}\binom{j}{t_2}x^{i-t_1}y^{j-t_2}$. However, by Claim 2.7 we know $i \bmod p \geq d_{gap}$, and by definition $d_{gap} = t_1 + t_2 \geq t_1$, so $i \bmod p \geq t_1$. Hence, by Lucas' theorem, the binomial coefficient $\binom{i}{t_1}$ is nonzero. Similarly, $\binom{i}{t_2}$ is nonzero. Thus, since P is nonzero so is $P^{(t_1,t_2)}$. $P^{(t_1,t_2)}$ is still reduced mod $\mathcal{I}^s_m$ and, homogeneous and nonzero, and so, $P^{(t_1,t_2)}$ is not divisible by D_2^s.

- Case 2: $r = p - 1 - d_{gap}$.

  Let (t_1, t_2) be such that $t_1 + t_2 = d_{gap}$. Write

  $$P^{(t_1,t_2)} = \sum \beta_i x^i y^{d-d_{gap}-i},$$

  and note that

  $$\beta_i = \alpha_{i+t_1} \cdot \binom{i + t_1}{t_1} \cdot \binom{d - (i + t_1)}{t_2}.$$

  Applying Claim 2.7 to P we see any i with $\alpha_i \neq 0$ has

  $$i \bmod p \in \{d_{gap}, d_{gap} + 1, \ldots, p - 1\}$$

  . Therefore, any i with $\beta_i \neq 0$ has

  $$i \bmod p \in \{d_{gap} - t_1, d_{gap} - t_1 + 1, \ldots, p - 1 - t_1\}.$$

  By Lemma 2.8 the largest power of D_2 dividing $P^{(t_1,t_2)}$ is at most $(p-1) - d_{gap} = r$. I.e., $P^{(t_1,t_2)}$ is not divisible by D_2^{r+1}.

□

We are now ready to prove:

Lemma 3.5. *If $d_{gap} > 0$ then, P contains a monomial $x^i y^{d-i}$ with $i \geq d^x_{opt} - (s-1)$.*

Proof. We want to show there exists a monomial $x^{d-\ell}y^\ell \in MON$ with $d_{gap} \leq \ell \leq d_{gap} + r$, because then $d - \ell \geq (d - d_{gap}) - r = d^x_{\text{opt}} - r \geq d^x_{\text{opt}} - (s-1)$ as desired.

Suppose not. Then, for every $d_{dap} \leq \ell \leq d_{gap} + r$, $x^{d-\ell}y^\ell$ is not in MON. Also, notice that for every such ℓ, $x^{d-\ell}y^\ell$ is a monomial in $\mathcal{B}_{m,s}$ (because $d - \ell \leq d - d_{gap} = d^x_{\max}$ and $\ell \leq d_{gap} + r < p$). Thus, by Claim 3.2, and using $d_{gap} + r < p$, $P^{(t_1,t_2)}$ vanishes over $\mathbb{F}_p \times \mathbb{F}_p$ for all (t_1, t_2) such $d_{gap} \leq t_1 + t_2 \leq d_{gap} + r$.

Let t_1, t_2 be some non-negative integers with $t_1 + t_2 = d_{gap}$. Using property 3 in Proposition 2.2 we conclude that for any non-negative s_1, s_2 with $s_1 + s_2 \leq r$,

$$(P^{(t_1,t_2)})^{(s_1,s_2)} = \binom{t_1 + s_1}{s_1}\binom{t_2 + s_2}{s_2} P^{(t_1+s_1,t_2+s_2)},$$

vanishes over $\mathbb{F}_p \times \mathbb{F}_p$. Therefore it follows that $P^{(t_1,t_2)} \in \mathcal{I}_2^{r+1}$, or, equivalently (using Lemma 2.5) that D_2^{r+1} divides $P^{(t_1,t_2)}$. But this is a contradiction to Lemma 3.4. □

Thus, no matter if $d_{gap} = 0$ or $d_{gap} > 0$, in either case P contains a monomial $x^i y^{d-i}$ with $i \geq d^x_{\text{opt}} - (s-1)$, and the proof is complete. □

Corollary 3.6. *Let p be prime, $2 \leq s < p$, and let P be a reduced polynomial in $R_{2,s}$ of degree d. If $x^i y^j$ is the canonical monomial of P then $j < p$.*

Proof. Suppose $x^i y^j$ is the canonical monomial of P and $j \geq p$. Since $x^i y^j$ is a monomial in $\mathcal{B}_{m,s}$ we have $i^1 + j^1 \leq s - 1$. Since $j \geq p$ we have $j^1 \geq 1$. But then it follows that $x^{i+p}y^{j-p}$ is also a monomial in $\mathcal{B}_{m,s}$. It therefore follows that $d^x_{\text{opt}} - i \geq p$ or equivalently, $i \leq d^x_{\text{opt}} - p$. But this is in contradiction to Theorem 3.1 that guarantees that in a canonical monomial $i \geq d^x_{\text{opt}} - (s-1)$. □

4 The multivariate case

Definition 4.1. *(Canonical monomial) Lem m, s be integers, $m \geq 2$, $s \geq 1$. Let $P \in \mathbb{F}_p[X_1, \ldots, X_m]$ be reduced modulo $\mathcal{I}^s_m$. The* canonical monomial *of P modulo $\mathcal{I}^s_m$, denoted $Can(P, m, s)$, is the largest leading monomial of $P \circ L \bmod \mathcal{I}^s_m$ in the deg-lex ordering (where $X_1 > \ldots > X_m$), where the maximum is taken over all linear transformations $L : \mathbb{F}^m_p \to \mathbb{F}^m_p$.*

[HSS13] proved that there is a *unique* form for canonical monomials of polynomials in m variables modulo $\mathcal{I}_m$ (i.e., when the multiplicity s is 1). More precisely,

Theorem 4.2. *(Canonical monomials - $s = 1$) [HSS13] Let p be a prime, $m \geq 2$ and $s = 1$. Let $P \in \mathbb{F}_p[X_1, \ldots, X_m]$ be reduced modulo $\mathcal{I}_m$. Suppose $\prod_{i=1}^m x_i^{e_i} \in \mathcal{B}_{m,s}$ is the canonical monomial of P modulo $\mathcal{I}^s_m$. Then,*

1. $\sum_{i=1}^m e_i = \deg(P)$

2. *If n is the last integer such that $e_n > 0$, then $e_i = q-1$ for all $i \in \{1,\ldots,n-1\}$, and $e_n \leq p-1$.*

In this section we prove:

Theorem 4.3. *(Canonical monomials - general s) Let p be a prime, $m \geq 2$ and $s < p$. Let $P \in \mathbb{F}_p[X_1,\ldots,X_m]$ be reduced modulo $\mathcal{I}_m^s$ and suppose $\prod_{i=1}^m x_i^{e_i} \in \mathcal{B}_{m,s}$ is the canonical monomial of P modulo $\mathcal{I}_m^s$. Then,*

1. $\sum_{i=1}^m e_i = \deg(P)$
2. $e_i \geq e_{i+1}$ *for all* $i \in [m-1]$.
3. $e_1 \geq \min\{p(s-1)+(p-1), d\} - (s-1)$.
4. *If n is the last integer such that $e_n > 0$, then $e_i = p-1$ for all $i \in \{2,\ldots,n-1\}$.*

Notice that Theorem 4.3 gives Theorem 4.2 when $s = 1$.

Proof. The proof is by reduction to one of the following base cases:

- $m = 1$ and arbitrary s (vacuous),
- $m = 2$ and arbitrary s (as follows from Theorem 1.9)
- $s = 1$ and arbitrary m (which is Theorem 4.2 taken from [HSS13]).

Let L be the linear map maximizing the leading monomial of $P \circ L \bmod \mathcal{I}_m^s$ in the deg-lex order. Notice that $\deg(P \circ L \bmod \mathcal{I}_m^s) = \deg(P)$, because otherwise the leading monomial of P is larger than that of $P \circ L \bmod \mathcal{I}_m^s$ in the deg-lex order. We replace P by $P \circ L \bmod \mathcal{I}_m^s$. Let $\prod_{i=1}^m x_i^{e_i}$ be the leading monomial of P. It is immediate that $e_1 \geq e_2 \ldots \geq e_m$, for otherwise changing variables gives a larger leading monomial in the deg-lex order. Thus, we immediately have properties Items 1 and 2.

Before we start proving properties Items 3 and 4 we prove a general principle:

Lemma 4.4. *Let $P \in F[X_1,\ldots,X_m]$ be reduced modulo $\mathcal{I}_m^s$. Suppose $\prod_{i=1}^m x_i^{e_i}$ is the canonical monomial of P modulo $\mathcal{I}_m^s$.*

Let $J \subset [m]$ be a set of cardinality t. For notational clarity, suppose

$$J = \{a_1,\ldots,a_t\}, \text{ and,}$$
$$[m] \setminus J = \{b_1,\ldots,b_{m-t}\}.$$

Express P as

$$P(x_1,\ldots,x_m) = \sum_{i_1,\ldots,i_{m-t}} P_{(i_1,\ldots,i_{m-t})}(x_{a_1},\ldots,x_{a_t}) \cdot x_{b_1}^{i_1} \cdot \ldots \cdot x_{b_{m-t}}^{i_{m-t}},$$

and denote $s_{rest} = \sum_{i \notin J} \lfloor \frac{e_i}{p} \rfloor$. Then

$$\prod_{j \in J} x_j^{e_j} = x_{a_1}^{e_{a_1}} \cdot \ldots \cdot x_{a_t}^{e_{a_t}}$$

is the canonical monomial of $P_{(e_{b_1},\ldots,e_{b_{m-t}})}$ modulo $\mathcal{I}_t^{s-s_{rest}}$.

Proof. Suppose not. Then there exists a linear transformation $L' : \mathbb{F}_p^t \to \mathbb{F}_p^t$ such that

$$P_{(e_{b_1},\ldots,e_{b_{m-t}})} \circ L' \bmod \mathcal{I}_t^{s-s_{rest}}$$

gives a larger monomial in the deg-lex ordering. Define a linear transformation on $L'' : \mathbb{F}_p^m \to \mathbb{F}_p^m$ that applies L' on the variables in location $a_1, \ldots, a_t$ and is identity otherwise. Then we claim that

$$P \circ L'' \bmod \mathcal{I}_m^s$$

gives a larger monomial than $\prod_{i=1}^m x_i^{e_i}$.

Intuitively, since by our assumption, $P_{(e_{b_1},\ldots,e_{b_{m-t}})} \circ L' \bmod \mathcal{I}_t^{s-s_{rest}}$ has a monomial $\prod_{j\in J} x_j^{f_j}$ that is larger than $\prod_{j\in J} x_j^{e_j}$ in the deg-lex ordering, then also

$$\left((P_{(e_{b_1},\ldots,e_{b_{m-t}})} \circ L')(\bmod \mathcal{I}_t^{s-s_{rest}})(x_{a_1},\ldots,x_{a_t}) \cdot \prod_{i\notin J} x_i^{e_i} \right) \bmod \mathcal{I}_m^s$$

has the monomial $\prod_{j\in J} x_j^{f_j} \cdot \prod_{i\notin J} x_i^{e_i}$ that is larger than $\prod_i x_i^{e_i}$ in the deg-lex ordering. What remains to be shown is that this is true even without the $(\bmod \mathcal{I}_t^{s-s_{rest}})$ term in the middle, i.e., that

$$\left((P_{(e_{b_1},\ldots,e_{b_{m-t}})} \circ L')(x_{a_1},\ldots,x_{a_t}) \cdot \prod_{i\notin J} x_i^{e_i} \right) \bmod \mathcal{I}_m^s$$

has the same monomial $\prod_{j\in J} x_j^{f_j} \cdot \prod_{i\notin J} x_i^{e_i}$ as a coefficient, which is a contradiction to the maximality of $\prod_i x_u^{e_i}$.

To prove this we define the polynomial

$$\tilde{P}(x_1,\ldots,x_m) = \sum_{i_1,\ldots,i_{m-t}} P_{(i_1,\ldots,i_{m-t})}(x_{a_1},\ldots,x_{a_t}) \cdot \phi(x_{b_1},i_1) \cdot \ldots \cdot \phi(x_{b_{m-t}},i_{m-t}),$$

where $\phi(x,j) = (x^p - x)^{j^1} x^{j-j^1}$ and $j^1 = \lfloor \frac{j}{p} \rfloor$. Notice that $\tilde{P}$ is not homogeneous, and that the maximal degree homogeneous part of $\tilde{P}$ is exactly P. It therefore follows that the maximal degree part of $\tilde{P} \circ L''$ mod $\mathcal{I}_m^s$ equals the maximal degree part of $P \circ L''$ mod $\mathcal{I}_m^s$. Hence, if $\tilde{P} \circ L''$ mod $\mathcal{I}_m^s$ has a maximal-degree monomial larger than $\prod_i x_i^{e_i}$ in the deg-lex ordering, so does $P \circ L''$ mod $\mathcal{I}_m^s$. We are therefore allowed to look at $\tilde{P} \circ L''$ mod $\mathcal{I}_m^s$ instead of $P \circ L''$ mod $\mathcal{I}_m^s$. The advantage of working with $\tilde{P} \circ L''$ mod $\mathcal{I}_m^s$, is that there it is easy to see the inner modulo is correct. Indeed:

- We first look at the part contributed by $i_1 = e_{b_1}, \ldots, i_{m-t} = e_{b_{m-t}}$. We see that:

$$\begin{aligned} &(P_{e_{b_1},\ldots,e_{b_t}} \circ L')(x_{a_1},\ldots,x_{a_t}) \cdot \prod_{i\notin J} \phi(x_i,e_i)) \bmod I_m^s \\ =&(P_{e_{b_1},\ldots,e_{b_t}} \circ L') \bmod \mathcal{I}_m^{s-s_{rest}}(x_{a_1},\ldots,x_{a_t}) \cdot \prod_{i\notin J} \phi(x_i,e_i) \bmod \mathcal{I}_m^s, \end{aligned}$$

  because $\prod_{i\notin J} \phi(x_i,e_i) \in \mathcal{I}_m^{s_{rest}}$.

- Thus, $\prod_{j\in J} x_j^{f_j} \cdot \prod_{i\notin J} \phi(x_i, e_i)$ appears as a monomial of the above term, because it is reduced modulo $\mathcal{I}_m^s$ (because $\sum_{j\in J}\lfloor \frac{f_j}{p} \rfloor + \sum_{j\notin J}\lfloor \frac{e_j}{p} \rfloor \leq (s - s_{rest} - 1) + s_{rest} = s - 1$).
- Furthermore, this term is not cancelled by terms contributed by other $(i_1, \ldots, i_{m-t})$, because the monomials $\phi(x_{b_1}, e_{b_1}) \cdot \ldots \phi(x_{b_{m-t}}, i_{m-t})$ are independent. Therefore, we conclude that $\prod_{j\in J} x_j^{f_j} \cdot \prod_{i\notin J} \phi(x_i, e_i)$ appears as a monomial of $(\tilde{P} \circ L'') \bmod \mathcal{I}_m^s$.

By the above discussion, the maximal-degree homogeneous part of $\prod_{j\in J} x_j^{f_j} \cdot \prod_{i\notin J} \phi(x_i, e_i)$ appears as a monomial of $(P \circ L'') \bmod \mathcal{I}_m^s$. Thus, $\prod_{j\in J} x_j^{f_j} \cdot \prod_{i\notin J} x_i^{e_i}$ appears as a monomial of $(P \circ L'') \bmod \mathcal{I}_m^s$. This is a contradiction to the maximality of $\prod_i x_i^{e_i}$, and the proof is complete. □

Similarly, we can prove:

Lemma 4.5. *Let $P \in F[X_1, \ldots, X_m]$ be reduced modulo $\mathcal{I}_m^s$. Suppose $\prod_{i=1}^m x_i^{e_i}$ is the canonical monomial of P modulo $\mathcal{I}_m^s$.*

Let $J \subset [m]$ be a set of cardinality t. For notational clarity, suppose

$$J = \{a_1, \ldots, a_t\}, \text{ and,}$$
$$[m] \setminus J = \{b_1, \ldots, b_{m-t}\}.$$

Express P as

$$P(x_1, \ldots, x_m) = \sum_{i_1,\ldots,i_{m-t}} P_{(i_1,\ldots,i_{m-t})}(x_{a_1}, \ldots, x_{a_t}) \cdot x_{b_1}^{i_1} \cdot \ldots \cdot x_{b_{m-t}}^{i_{m-t}},$$

and denote $s' = \sum_{i\in J}\lfloor \frac{e_i}{p} \rfloor$. Then

$$\prod_{j\in J} x_j^{e_j} = x_{a_1}^{e_{a_1}} \cdot \ldots \cdot x_{a_t}^{e_{a_t}}$$

is the canonical monomial of $P_{(e_{b_1},\ldots,e_{b_{m-t}})}$ modulo $\mathcal{I}_t^{s'+1}$.

Proof. Suppose for some L', $P_{e_{b_1},\ldots,e_{b_t}} \circ L' \bmod \mathcal{I}_t^{s'+1}$ has a larger monomial in the deg-lex ordering. Since $s' \leq s - s_{rest} - 1$ so does $P_{e_{b_1},\ldots,e_{b_t}} \circ L' \bmod \mathcal{I}_t^{s-s_{rest}}$. The claim then follows from Lemma 4.4. □

With Lemmas 4.4 and 4.5 we prove:

Claim 4.6. $e_2 \leq p - 1$.

Proof. Let $s_{rest} = \sum_{i\geq 3}\lfloor \frac{e_i}{p} \rfloor \leq s - 1$. By Lemma 4.4, $x_1^{e_1} x_2^{e_2}$ is the canonical monomial of $P_{(e_3,\ldots,e_m)}(x_1, x_2)$ modulo $\mathcal{I}_2^{s-s_{rest}}$. However, Corollary 3.6 shows that for $m = 2$ (and any $s' \geq 1$) the canonical monomial $x_1^{i_2} x_2^{i_2}$ has $i_2 < p$. Thus $e_2 < p$. □

Thus, for all $i \geq 2$ we have $e_i \leq p - 1$. Next we prove Item 4:

Claim 4.7. *Let n be the largest integer such that $e_n > 0$. Then $e_2 = e_3 = \ldots = e_{n-1} = p-1$.*

Proof. Let $s' = \sum_{i=2}^{m} \lfloor \frac{e_i}{p} \rfloor$. As $e_i \leq p-1$ for all $i \geq 2$, we have $s' = 0$. By Lemma 4.5, $x_2^{e_2} \cdot \ldots \cdot x_n^{e_n}$ is the canonical monomial of $P_{(e_1)}(x_2, \ldots, x_m)$ modulo $\mathcal{I}_{m-1}^{s'+1}$. As $s'+1 = 1$, Theorem 4.2 implies that $e_2 = e_3 = \ldots = e_{n-1} = p-1$ as desired. □

Finally we prove Item 3:

Claim 4.8. $e_1 \geq \min\{(s-1)p + (p-1), d\} - (s-1)$.

Proof. Let $s_{rest} = \sum_{i \geq 3} \lfloor \frac{e_i}{p} \rfloor$. As $e_i \leq p-1$ for all $i \geq 2$, we have $s_{rest} = 0$. By Lemma 4.4, $x_1^{e_1} x_2^{e_2}$ is the canonical monomial of $P_{(e_3,\ldots,e_m)}(x_1, x_2)$ modulo $\mathcal{I}_2^{s-s_{rest}}$, i.e., modulo $\mathcal{I}_2^s$. By Theorem 3.1 we see that

$$e_1 \geq \min\{p(s-1) + p - 1, e_1 + e_2\} - (s-1).$$

- If $e_3 = 0$ we have $e_1 + e_2 = d$. Thus, $e_1 \geq \min\{p(s-1) + p - 1, d\} - (s-1)$ as desired.
- If $e_3 > 0$, then $e_2 = p-1$. If $e_1 + e_2 \leq p(s-1) + p - 1$, then $e_1 \geq e_1 + e_2 - (s-1)$. Thus, $e_2 \leq s - 1 < p - 1$. A contradiction. Thus $p(s-1) + (p-1) \leq e_1 + e_2$. But then $e_1 \geq p(s-1) + (p-1) - (s-1)$ as desired.

□

□

5 Proof of the main theorem

In this section, we use Theorem 1.12 to prove our main theorem, Theorem 1.6.

We start with simple consequence of the definition of canonical monomials for multiplicity codes. The lemma shows that if the canonincal monomial has more than two variables, the variable x already has the largest multiple of p possible in $\mathcal{B}_{m,s}$ in its exponent.

Lemma 5.1. *Suppose $\prod_{i=1}^{m} x_i^{e_i}$ is a canonical monomial for P of degree d. Then either $e_1 \geq p(s-1) + (p-1) - (s-1)$ or $m \leq 2$.*

Proof. By the definition of canonical monomials, we know $e_1 \geq \min\{p(s-1) + (p-1), d\} - (s-1)$. If $m > 2$, we know $e_2 = p-1$ and $e_3 \geq 1$. Therefore, $e_1 < d - p < d - (s-1)$, so it must the case that $\min\{p(s-1) + (p-1), d\} = p(s-1) + (p-1)$. Therefore, $e_1 \geq p(s-1) + (p-1) - (s-1)$. □

We proceed similarly to [HSS13] and show that reducing the dimension of tests from $k+1$ to k does not hurt soundness too much, as long as k is not too small. The result [HSS13] show for Reed-Muller codes, which is the case $s = 1$ in the terminology of this paper, is:

Lemma 5.2. *[HSS13, Lemma 4.6] Let $d < k(p-1)$ and let $f : \mathbb{F}_p^{k+1} \to \mathbb{F}_p$ have degree larger than d. Then the k-dimensional test rejects f with probability at least $\frac{1}{p}$.*

It should be noted that this lemma is the central tool in the soundness analysis in [KM22].

The proof of Lemma 5.2 uses the algebraic language described in Section 1.5, as well as canonincal monomials. Basically, we may assume WLOG that f contains a canonical monomial. The restriction to a k-dimensional subspace within $\mathbb{F}_p^{k+1}$ may be viewed as modding out by a single linear equation. It is then showed, under the assumptions of the lemma, that the probability that the resulting polynomial has degree larger than d is at least $\frac{1}{p}$.

In the case of Lemma 5.2, the polynomials are always considered mod $\mathcal{I}_k$. Let us illustrate an example: suppose the polynomial is $x_1^{p-1}x_2^{p-1}$, and the linear equation is $x_1 - x_2 = 0$. Modding out by the equation turns the polynomial into x_1^{2p-2}, which is equivalent mod $\mathcal{I}_k$ to x_1^{p-1}, because $x_1^{2p-2} - x_1^{p-1} = x_1^{p-2}(x_1^p - x_1) \in \mathcal{I}_k$. Therefore, in this case the polynomial retains the highest possible degree for a univariate polynomial, $p-1$.

We now show an analogous lemma for multiplicity codes

Lemma 5.3. *Let $d < k(p-1) + (s-1)p - (s-1)$ and let $f : \mathbb{F}_p^{k+1} \to \Sigma_{k+1,s}$ have degree larger than d. Then the k-dimensional test rejects f with probability at least $\frac{1}{p^2}$.*

Again, we assume WLOG that f contains a canonical monomial $\prod_{i=1}^m x_i^{e_i}, m \leq k+1$ and we consider the restriction to a dimension k space as modding out by a single linear equation L. The general strategy of the proof is to show that if the x_1 coefficient of the linear equation L is zero, everything behaves like the Reed-Muller case. As the x_1 coefficient is zero with probability $\frac{1}{p}$, the overall rejection probability will be at least $\frac{1}{p} \cdot \frac{1}{p} = \frac{1}{p^2}$.

As an example, suppose $f = x_1^{(s-1)p}x_2^{p-1}x_3^{p-1}$, and that $L = x_2 - x_3$. Modding out by L we get the polynomial $f = x_1^{(s-1)p}x_2^{2p-2}$. The polynomial $(x_1^p - x_1)^s x_2^{p-2}(x_2^p - x_2)$ is in $\mathcal{I}_k^s$, and therefore this polynomial is equivalent to $x_1^{(s-1)p}x_2^{p-1}$ plus terms with lower powers of x_1.

Essentially, because the power of x_1 is above $(s-1)p$ and because we are only interested in monomials with the highest x_1-degree, we can do the same calculation as in the Reed-Muller case.

Proof. Write

$$L = L_1x_1 + L_2x_2 + \cdots + L_{k+1}x_{k+1} + c$$

We first handle the case $m = 2$. In this case, any L with $L_1 = 0, L_2 = 0$ will retain the monomial $x_1^{e_1}x_2^{e_2}$, which has degree $\deg f$. Therefore, the probability that $\deg(f|_{L=0}) \geq \deg f > d$ is at least $\frac{1}{p^2}$.

Otherwise, write

$$f = \sum_{i=0}^{e_1} x_1^i f_i(x_2, \ldots, x_{k+1})$$

by Lemma 5.1 we may assume $e_1 \geq (s-1)p + (p-1) - (s-1)$. Due to $e_1 \geq (s-1)p$, all degrees in f_{e_1} are $< p$, because otherwise $e_1 f_{e_1}$ would be $\mathcal{I}_{k+1}$-reducible. Additionally, $\deg(f_{e_1}) = deg f - e_1 > d - e_1$, and $d - e_1 < (k-1)(p-1)$. Hence f_{e_1} satisfies the conditions of Lemma 5.2 for with $d = d - e_1$ and $k = k - 1$. Therefore, conditioned on $L_1 = 0$, we

know that with probability at least $\frac{1}{p}$ there exists a polynomial g with $\deg(g) > d - e_1$ and $h \stackrel{\text{def}}{=} (g - f_{e_1}|_{L=0}) \in \mathcal{I}_k$.

In this case, $h(x_1^p - x_1)^{s-1} \in \mathcal{I}_{k+1}^s$, therefore so is $hx_1^{e-s(p-1)}(x_1^p - x_1)^{s-1}$. Subtracting this from $(x_1^{e_1} f_{e_1}|_{L=0}) = x_1^{e_1}(f_{e_1}|_{L=0})$ we see that $x_1^{e_1} f_{e_1}|_{L=0}$ is $\mathcal{I}_{k+1}^s$-equivalent to $x_1^{e_1} g$ plus terms with a lower power of x_1. This means $\deg f \geq \deg(x_1^{e_1} f_{e_1}|_{L=0}) = e_1 + \deg g > d$. □

Corollary 5.4. *Let $d < k(p-1) + (s-1)p - (s-1)$ and let $f : \mathbb{F}_p^{k+t} \to \Sigma_{k+t,s}$ have degree larger than d. Then the k-dimensional test rejects f with probability at least $\frac{1}{p^{2t}}$.*

Proof. This corollary is simply t repeated applications of Lemma 5.3, when noting that the distribution on k-dimensional affine subspaces in $\mathbb{F}_p^{k+t}$ given by selecting a $k+t-1$ dimensional subspace uniformly, and within it a $k+t-2$ dimensional subspace is uniform over all $k+t-2$ dimension subspaces. □

We now prove Theorem 1.6.

Theorem. *There exist constants c_1, c_2 such that for any prime p, integers $m \geq 1$, $k \geq 2$, $s < p$ and $d < d_{k,s} - (s-1)$ the k-flat test is a local tester with soundness function $\min(\delta p^{-4s-c_1}, p^{-4s-c_2})$*

Proof. Let $f : \mathbb{F}_p^m \to \Sigma_{m,s}$, and let $\delta = \delta(f, \mathrm{MRM}_p(m,d,s))$.

We will choose our k-dimensional subspace by choosing a $k+2s$-dimensional subspace H_1 and within it a k-dimensional subspace H_2. H_2 is uniformly distributed.

By Theorem 1.4 together with Theorem 1.2 we know that there exists a universal constant c such that

$$\mathbb{P}_{H_1}\left(\deg f|_{H_1} > d\right) \geq \min\left\{\alpha, p^{-c}\right\}$$

with

$$\alpha = p^{k+2s-c}\frac{p-(s-1)}{p}\frac{1}{p^{k+2s-c}+p^{d/(p-1)}} = \frac{1}{p^{O(1)}}$$

By Corollary 5.4 we know

$$\mathbb{P}_{H_2}\left(\deg f|_{H_2} > d\right) \geq p^{-4s}\mathbb{P}_{H_1}\left(\deg f|_{H_1} > d\right) \geq p^{-4s}\min\left\{\delta p^{-c_1}, p^{-c_2}\right\},$$

and the proof is complete. □

References

[AKK+05] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing reed-muller codes. *IEEE Transactions on Information Theory*, 51(11):4032–4039, 2005. 1

[BKS+10] Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. Optimal testing of reed-muller codes. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 488–497. IEEE, 2010. 1

[FS95] Katalin Friedl and Madhu Sudan. Some improvements to total degree tests. In *Proceedings Third Israel Symposium on the Theory of Computing and Systems*, pages 190–198. IEEE, 1995. 1

[GW13] Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of reed–solomon codes. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013. 1.1

[HSS13] Elad Haramaty, Amir Shpilka, and Madhu Sudan. Optimal testing of multivariate polynomials over small prime fields. *SIAM Journal on Computing*, 42(2):536–562, 2013. (document), 1, 1.4, 1.4, 1.4, 1.5.1, 1.7, 1.5.1, 1.8, 1.5.2, 1.5.4, 1.14, 4, 4.2, 4, 5, 5.2

[KM22] Tali Kaufman and Dor Minzer. Improved optimal testing results from global hypercontractivity, 2022. 1, 1.2, 5

[Kop13] Swastik Kopparty. Some remarks on multiplicity codes. *Discrete Geometry and Algebraic Combinatorics*, 625:155–176, 2013. 1.1, 2

[KR06] Tali Kaufman and Dana Ron. Testing polynomials over general fields. *SIAM Journal on Computing*, 36(3):779–802, 2006. 1, 1

[KS08] Tali Kaufman and Madhu Sudan. Algebraic property testing: the role of invariance. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 403–412, 2008. 1.5.1

[KSTS22] Dan Karliner, Roie Salama, and Amnon Ta-Shma. The plane test is a local tester for multiplicity codes. *preprint*, 2022. (document), 1.1, 1.2, 1.3, 1.3, 1.4, 1.4, 1.4, 1.5, 1.5.3, 1.5.4, 2.2

[KSY14] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. *Journal of the ACM (JACM)*, 61(5):1–20, 2014. 1.1

[RS96] Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM Journal on Computing*, 25(2):252–271, 1996. 1

אוניברסיטת תל-אביב
הפקולטה למדעים מדויקים
ע"ש ריימונד ובברלי סאקלר

בדיקה מקומית של קודי ריבוי

חיבור זה הוגש כחלק מהדרישות לקבלת התואר
"מוסמך אוניברסיטה" - M.Sc. באוניברסיטת תל-אביב

בית הספר למדעי המתמטיקה

על ידי
דן קרלינר

העבודה הוכנה בהדרכתו של
פרופסור אמנון תא שמע

תקציר העבודה

קודי הריבוי $\mathrm{MRM}_p(m, d, s)$ הם קודים לתיקון שגיאות המכללים את קודי Reed-Muller. מילת קוד מוגדרת עבור כל פולינום בm משתנים ממעלה לכל היותר d מעל השדה $\mathbb{F}_p$. בהינתן פולינום כזה P, מילת קוד כוללת, עבור כל נקודה במרחב $\mathbb{F}_p^m$, את הערך של הפולינום ואת הערך של הנגזרות החלקיות שלו ממעלה כוללת פחות מs. נסמן את האלף-בית מעליו מוגדר הקוד בΣ.
לקודי הריבוי יש אפליקציות רבות בתיאוריה של מדעי המחשב, והם מהווים רכיב בחלק מהבניות הטובות ביותר לקודים בעלי תכונות מקומיות.

עבודה זו עוסקת בבעיה של הפרדה יעילה, עבור מילה Σ^n, בין המקרה שבו המילה נמצאת בקוד לבין המקרה בו המילה רחוקה מהקוד, בעזרת קריאת כמות קטנה של תוים אקראיים מתוך המילה. בעיה זו נקראת local testing, "בדיקה מקומית", מכיוון שהיא כוללת התבוננת רק בחלק קטן מהמילה.

בגלל המבנה הגיאומטרי של קודי הריבוי, מועמד טבעי לאלגוריתם בדיקה מקומית הוא "הבדיקה הk-מימדית", המורכבת מצמצום מילת הקוד לתת-מרחב אפיני ממימד k של $\mathbb{F}_p^m$.
בעבודה זו אנחנו מנתחים את הבדיקה הk-מימדית ומראים שהיא מהווה אלגוריתם בדיקה מקומית אפקטיבי עבור k גדול מספיק. בנוסף, אנחנו מראים שהתלות בין פרמטרי הקוד לבין המימד k שנחוץ היא כמעט אופטימלית, ומשערים שהיא לא ניתנת לשיפור.

טכניקת ההוכחה מכלילה את הכלי בשם "מונומים קנוניים" שהוצג בעבודה של Haramaty, Shpilka, Sudan ב2013 עבור ניתוח של הבדיקה הk-מימדית עבור קודי Reed-Muller.
ההכללה של מונומים קנוניים למקרה של קודי ריבוי דורשת מציאת ההגדרה הנכונה למקרה הזה, והוכחה מהותית שונה המנצלת את המבנה האלגברי של קודי ריבוי.