Improved Local Testing for Multiplicity Codes

Dan Karliner
Department of Computer Science, Tel Aviv University, Israel

Amnon Ta-Shma
Department of Computer Science, Tel Aviv University, Israel

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, [6] 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 [6] in the case of planes.

Our analysis relies on a generalization of the technique of *canonincal monomials* introduced in [5]. Generalizing canonical monomials to the multiplicity case requires substantially different proofs which exploit the algebraic structure of multiplicity codes.

2012 ACM Subject Classification Theory of computation → Error-correcting codes

Keywords and phrases local testing, multiplicity codes, Reed Muller codes

Digital Object Identifier 10.4230/LIPIcs.APPROX/RANDOM.2022.11

Category RANDOM

Related Version *Previous Version*: https://eccc.weizmann.ac.il/report/2022/078/

Funding *Dan Karliner*: The research leading to these results was supported by Len Blavatnik and the Blavatnik Family foundation and by the Israel Science Foundation grant number 952/18.
Amnon Ta-Shma: The research leading to these results was supported by the Israel Science Foundation grant number 952/18.

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.** *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 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 $w \in C$.

Local testing Reed-Muller codes has been studied extensively and in several parameter regimes [14, 3, 1, 8, 2, 5, 7]. 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 $\mathrm{REJ}_{k,d}$.

Any polynomial in k variables is equal everywhere to one whose degree in every variable is at most $p-1$, and therefore of total 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 [8] 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 [5, 7] test shows it is essentially optimal given the number of queries in a wide range of parameters [1]:

▶ **Theorem 2** (Soundness of the RM k-flat test, [7]). *There exists a constant $c > 0$ (independent of p) such that the k-flat test rejects with probability at least $p^{-c}\min(p^k\delta, 1)$*

1.1 The k-flat test for Multiplicity codes

Multiplicity codes were defined in [13, 12, 4, 11]. $\mathrm{MRM}_p(m,d,s)$ is the set of evaluation tables of m-variate, degree d polynomials, where we also record 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 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. 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 [6](following the $k = 1$ case from [10]) by:

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

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] 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 [8] 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.

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

Given a function $f : \mathbb{F}_p^m \to \mathbb{F}_p$, any function equivalent to it mod

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

takes the same values on all of $\mathbb{F}_p^m$, and a polynomial P has the same evaluation table as Q if and only if $P \equiv Q \mod \mathcal{I}_m$.

It is established in [6] 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. 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 $d \leq d_{k,s} \stackrel{\text{def}}{=} k(p-1) + (s-1)p$.

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

The previous discussion means that 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 [6] shows the line test fails for $s = 2$ even for $d = p + 1$.

Local testing for multiplicity codes is studied in [6], with an emphasis on the 2-flat ("plane") test. Two main results are obtained: one for characterization and one for robustness. For characterization, [6] show that the *plane* test is a local characterization in degrees nearly reaching $d_{k,s}$. Concretely,

▶ **Theorem 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 [6] 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 4** (Local testing is preserved from RM to MRM, [6]). *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*

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

Then, for every T we have

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

for

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

Combining Theorems 3 and 4 one gets that under the same conditions as in Theorem 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 [5], 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 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 [6] 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 $d \geq d_{2,s} = 2(p-1) + (s-1)p = (s+1)p - 2$, [6] 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 [6] does not give good enough soundness in the general case, so we use a different technique based on the soundness analysis in [5]

▶ **Theorem 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. In Appendix C we give an example showing tightness for the case $k = 2, s = 2$ in as well as an example that shows that the degree bound cannot be improved within our technique.
- Another intriguing question is the appearance of the condition $s < p$ in our results (and also in [6]). 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 [5, 6] 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?

We now explain the canonical monomial method of [5] and its use for multiplicity codes.

1.5 The technique

We continue the discussion in Section 1.2. Multiplicity tables of multiplicity s are equivalent to elements of

$$R_{m,s} \stackrel{\text{def}}{=} \mathbb{F}_p[x_1, x_2, \ldots, x_m] \mod \mathcal{I}_m^s \tag{2}$$

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

$$\mathcal{B}_{m,s} = \left\{ \prod_{i=1}^{m} x_i^{e_i} : \sum_{i=1}^{m} \left\lfloor \frac{e_i}{p} \right\rfloor < s \right\} \tag{3}$$

as a basis for $R_{m,s}$ (this basis is different than the one chosen in [6]). 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.

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 $\bar{L} : R_{m,s} \to R_{k,s}$ 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. In fact, many of the results regarding Reed-Muller codes generalize to general affine-invariant codes, see e.g. [9].

In [5], this fact is used 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 7** ([5, Definition 4.1]). *A canonical monomial of degree d in $n \le m$ 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 $1 \le i < n$ $e_i = p-1$ (3) $e_n \le p-1$*[2].

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

Further, in [5] it is shown that any polynomial can be composed with a linear map L so that $P \circ L$ contains a canonical monomial of degree $\deg P$. Given that a polynomial contains a canonical monomial, local characterization and testing proofs become much easier.
A map L for which $P \circ L$ contains a canonical monomial 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 8** ([5, Lemma 4.2]). *Let $f(x_1,x_2)$ be a degree $d \le 2(p-1)$ 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.*

The proof is given in Appendix A for completeness.

[2] 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), multiplicity codes are also affine invariant. Similarly to [5] 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 8 fail? Looking at the coefficient of x_1^{p+1} in $f(x_1, x_2 + z x_1)$, 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 8, the coefficient of x_1^d in $P(x_1, x_2 + z x_1)$ 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.

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 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 $\le d^x_{\max}$, 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 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 9

▶ **Corollary 10.** *Under the same assumptions as Theorem 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 $b \le p - 1$.*

Proof. We take the same linear map as in Theorem 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 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 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* $\mathrm{Can}(P, m, s)$*, 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 $L : \mathbb{F}^m_p \to \mathbb{F}^m_p$.*

▶ **Theorem 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 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 [6] 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 4 with probability $\geq \delta\frac{1}{p}$ the restriction $P|_H$ has degree $> d$.
- Due to Theorem 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 trying to generalize this approach to the k-dimensional test, some issues occur. As the degree bound on d is $\approx (p-1)k + (s-1)p$, the space H needs to have dimension $k+2s$. In this case the first step still works. However, the number of k-dimensional subspaces in $\mathbb{F}^{k+2s}_p$ 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 $\mathbb{F}^{k+2s}_p$, analogous to the following lemma in [5].

▶ **Lemma 13** ([5], Lemma 4.6)**.** *Let $d < k(p-1)$ and let $f : \mathbb{F}^{k+1}_p \to \mathbb{F}_p$ 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 14.** *Let $d < k(p-1)+(s-1)p-(s-1)$ and let $f : \mathbb{F}^{k+1}_p \to \Sigma_{k+1,s}$ 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 6.

2 Preliminaries

For a comprehensive survey of multiplicity codes, see [10]. 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 15** (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 16** (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 17** (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:

▶ **Corollary 18.** $\mathrm{Mult}(P \cdot Q; x) \geq \mathrm{Mult}(P; x) + \mathrm{Mult}(Q; x)$.

We also need the following:

▶ **Lemma 19** (See, e.g. [6]). *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 20.** *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 Moore determinant of order 2 is

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

$D_2 = x(y^p - y) - y(x^p - x)$ is a homogeneous polynomial with vanishing multiplicity 1. As D_2 vanishes on the whole of $\mathbb{F}_p \times \mathbb{F}_p$, by Lemma 20 we get the well known fact:

▶ **Corollary 21.**

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

We show D_2 is essentially the only example of a bivariate homogeneous polynomial vanishing over $\mathbb{F}_q \times \mathbb{F}_q$:

▶ **Lemma 22.** *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 $\text{Mult}(P;(a,b)) \geq s$, we have by Lemma 20 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 Corollary 21 we see that $D_2^t | P$ as desired. ◀

We also need:

▶ **Lemma 23.** *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 $P_c = \sum_{i \equiv c \bmod (p-1)} \alpha_i x^i y^{d-i}$ 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 $Q_c = \sum_{i \equiv c \bmod (p-1)} \beta_i x^i y^{d-i}$. 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 $\sum_{i=1}^m e_i^1 < s$.

The following is results on $\mathcal{B}_{m,2}$ are technical and given in Appendix B.

▷ Claim 24. 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 25. 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 $i \bmod p \in \{d_{gap}, d_{gap}+1, \ldots p-1\}$.

We now show that a homogeneous polynomial with few monomials is not divisible by a high power of D_2.

▶ **Lemma 26.** *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 27. $J \subseteq \{c-t-k, \ldots, c-t\}$.

Proof. As P is reduced modulo $\mathcal{I}^s_m$ 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 23 D_2^r divides P_c. By Corollary 21, $\prod_{a \in \mathbb{F}_p^*}(x - ay)$ divides D_2, and therefore

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

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 28.** *Let p be prime, $2 \leq s < p$, and let P be a reduced polynomial in $R_{2,s}$ of degree d. Let $d^x_{opt} = \min(d, d^x_{\max}) = \min(d, p(s-1) + (p-1))$. There exists a linear map $L : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ such that $P \circ L \bmod \mathcal{I}^s_m$ 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 29. 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 30. If $d^x_{\text{opt}} = d$, P contains a monomial $x^e y^{d-e}$ with $e \geq d^x_{\text{opt}} - (s-1)$.

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 29, 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, $\mathrm{Mult}(P,\mathbb{F}_p^2) \geq s$ 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 $d_{gap} = d - d^x_{\mathrm{opt}}$. When $d_{gap} = 0$, i.e., $d^x_{\mathrm{opt}} = d$, we proved the theorem (Claim 30). We now assume $d_{gap} > 0$. Define $r = \min\{p-1-d_{gap}, s-1\}$.

▶ **Lemma 31.** *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 25 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 25 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 26 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 32.** *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 $d-\ell \geq (d-d_{gap}) - r = d^x_{\mathrm{opt}} - r \geq d^x_{\mathrm{opt}} - (s-1)$ 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 29, 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 16 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 22) that D_2^{r+1} divides $P^{(t_1,t_2)}$. But this is a contradiction to Lemma 31. ◀

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. ◀

4 The multivariate case

In this section we prove:

▶ **Theorem 33** (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 $\mathcal{I}^s_m$ 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 $i \in \{2, \ldots, n-1\}$.*

Notice that Theorem 33 gives Definition 7 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 9)
- $s = 1$ and arbitrary m (from [5]).

Let L be the linear map maximizing the leading monomial of $P \circ L \bmod \mathcal{I}^s_m$ in the deg-lex order. Notice that $\deg(P \circ L \bmod \mathcal{I}^s_m) = \deg(P)$, because otherwise the leading monomial of P is larger than that of $P \circ L \bmod \mathcal{I}^s_m$ in the deg-lex order. We replace P by $P \circ L \bmod \mathcal{I}^s_m$. 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 34.** *Let $P \in F[X_1, \ldots, X_m]$ be reduced modulo $\mathcal{I}^s_m$. Suppose $\prod_{i=1}^m x_i^{e_i}$ is the canonical monomial of P modulo $\mathcal{I}^s_m$.*

Let $J \subset [m]$ be a set of cardinality t. For notational clarity, suppose $J = \{a_1, \ldots, a_t\}$ 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 $P \circ L'' \bmod \mathcal{I}^s_m$ 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. Therefore, the maximal degree part of $\tilde{P} \circ L'' \bmod \mathcal{I}_m^s$ equals the maximal degree part of $P \circ L'' \bmod \mathcal{I}_m^s$. Hence, if $\tilde{P} \circ L'' \bmod \mathcal{I}_m^s$ has a maximal-degree monomial larger than $\prod_i x_i^{e_i}$ in the deg-lex order, so does $P \circ L'' \bmod \mathcal{I}_m^s$. We are therefore allowed to look at $\tilde{P} \circ L'' \bmod \mathcal{I}_m^s$ instead of $P \circ L'' \bmod \mathcal{I}_m^s$. When working with $\tilde{P} \circ L'' \bmod \mathcal{I}_m^s$, it 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 35.** *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 $J = \{a_1, \ldots, a_t\}$ 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', $P_{e_{b_1}, \ldots, e_{b_t}} \circ L'$ mod $\mathcal{I}_t^{s'+1}$ has a larger monomial in the deg-lex ordering. Since $s' \leq s - s_{rest} - 1$ so does $P_{e_{b_1}, \ldots, e_{b_t}} \circ L'$ mod $\mathcal{I}_t^{s - s_{rest}}$. The claim then follows from Lemma 34. ◀

With Lemmas 34 and 35 we prove:

▷ Claim 36. $e_2 \leq p - 1$.

Proof. Let $s_{rest} = \sum_{i \geq 3} \lfloor \frac{e_i}{p} \rfloor \leq s - 1$. By Lemma 34, $x_1^{e_1} x_2^{e_2}$ is the canonical monomial of $P_{(e_3, \ldots, e_m)}(x_1, x_2)$ modulo $\mathcal{I}_2^{s - s_{rest}}$. However, Corollary 10 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 37. 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 35, $x_2^{e_2} \cdot \ldots \cdot x_n^{e_n}$ is the canonical monomial of $P_{(e_1)}(x_2, \ldots, x_m)$ modulo $\mathcal{I}_{m-1}^{s'+1}$. As $s' + 1 = 1$, Definition 7 implies that $e_2 = e_3 = \ldots = e_{n-1} = p - 1$ as desired. ◁

Finally we prove Item 3:

▷ Claim 38. $e_1 \geq \min\{(s-1)p + (p-1), d\} - (s-1)$.

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 34, $x_1^{e_1} x_2^{e_2}$ 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 28 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 12 to prove our main theorem, Theorem 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 39.** *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 [5] and show that reducing the dimension of tests from $k+1$ to k does not hurt soundness too much. This is Lemma 13 in in the RM case. It should be noted that this lemma is the central tool in the soundness analysis in [7].

We now show an analogous lemma for multiplicity codes

▶ **Lemma 40.** *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 $\frac{1}{p} \cdot \frac{1}{p} = \frac{1}{p^2}$.

Essentially, because the power of x_1 is $\geq (s-1)p$ and because we are focused on 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 39 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 13 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 $\left(x_1^{e_1} f_{e_1}|_{L=0}\right) = x_1^{e_1}\left(f_{e_1}|_{L=0}\right)$ 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 $\deg f \geq \deg\left(x_1^{e_1} f_{e_1}|_{L=0}\right) = e_1 + \deg g > d$. ◀

▶ **Corollary 41.** *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 40, 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 6.

▶ **Theorem 42.** *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 4 together with Theorem 2 we know that there exists a universal constant c such that $\mathbb{P}_{H_1}\left(\deg f|_{H_1} > d\right) \geq \min\{\alpha, p^{-c}\}$ 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 41 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

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. Dan Karliner, Roie Salama, and Amnon Ta-Shma. The plane test is a local tester for multiplicity codes. *preprint*, 2022. URL: `https://eccc.weizmann.ac.il/report/2022/028/`.
7. Tali Kaufman and Dor Minzer. Improved optimal testing results from global hypercontractivity, 2022. `arXiv:2202.08688`.
8. Tali Kaufman and Dana Ron. Testing polynomials over general fields. *SIAM Journal on Computing*, 36(3):779–802, 2006.
9. 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.
10. Swastik Kopparty. Some remarks on multiplicity codes. *Discrete Geometry and Algebraic Combinatorics*, 625:155–176, 2013.
11. Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. *Journal of the ACM (JACM)*, 61(5):1–20, 2014.
12. Rasmus Refslund Nielsen. *List decoding of linear block codes*. PhD thesis, DTU, 2001.
13. M Yu Rosenbloom and Michael Anatol'evich Tsfasman. Codes for the m-metric. *Problemy Peredachi Informatsii*, 33(1):55–63, 1997.
14. Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM Journal on Computing*, 25(2):252–271, 1996.

A Proof of bivariate Reed Muller canonincal monomials

The following proof is taken from [5].

Proof. Write $f(x_1,x_2)=\sum_{e:0\le e,d-e<p}\alpha_e x_1^e x_2^{d-e}$. 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 $f(x_1,x_2+zx_1)$. By the binomial theorem it follows that

$$f(x_1,x_2+zx_1)\equiv_{\mathcal{I}_2}\sum_{e\le d}\alpha_e x_1^e\sum_{r\le d-e}\binom{d-e}{r}(zx_1)^r x_2^{d-e-r}$$

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

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

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. ◀

B Monomials in $\mathcal{B}_{m,2}$

In this appendix, we establish bounds on the degrees of monomials in $\mathcal{B}_{m,2}$.

- For $d<ps$, any monomial of degree d is contained in $\mathcal{B}_{m,s}$. Indeed, if $\sum_{i=1}^m e_i^1\ge s$ then $d=\sum e_i\ge ps$.
- 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 $ps\le d\le d_{m,s}$ appear in $\mathcal{B}_{m,s}$.

  In the case $m=2$ this gives

▷ Claim 43. The highest degree in x a monomial in $\mathcal{B}_{2,s}$ can have is

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

In general,

▷ Claim 44. Let $s<p$ and and suppose $d=d^x_{\max}+d_{gap}$ where $d_{gap}\ge 0$ (and notice that $d_{gap}\le p-1$). The monomial x^iy^{d-i} is in $\mathcal{B}_{2,s}$ if and only if $0\le i\le d$ and $i \mod p\in\{d_{gap},d_{gap}+1,\dots p-1\}$.

Proof. Fix x^iy^{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

$$ps + d_{gap} - 1 = p(i^1 + j^1) + (i^0 + j^0). \tag{4}$$

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. ◁

C Tightness of results

In this subsection, we demonstrate that some of the degree bounds in the results described above are tight. The first example is derived from the Moore determinant, $D_2 = x_1^p x_2 - x_2^p x_1$. More properties of the Moore determinant are given in Section 2.1.

▶ **Lemma 45.** *The loss of $(s-1)$ in Theorem 9 cannot be improved. That is, there exists a polynomial P in $R_{2,s}$ for which, for any linear map L, the degree of x_1 is at most $d^x_{opt} - (s-1)$*

Proof. The polynomial $P = D_2^{s-1}$ is of degree $(p+1)(s-1)$, so for it $d^x_{\text{opt}} = \deg(P)$. This polynomial has leading monomial $x_1^{p(s-1)} x_2^{s-1}$. As is shown in Section 2.1, $D_2 \circ L = \det(L) D_2$. Therefore, the degree $p(s-1)$ is the highest achievable for x_1. ◀

We now give an example of the tightness of Theorem 5 for a special case. This example was found using linear algebra.

▶ **Lemma 46.** *The degree bound in is tight for $k = 2, s = 2$.*

To demonstrate this, we need to show a polynomial of degree $d_{2,2} = 2(p-1) + p(2-1) = 3p - 2$ that drops a degree when restricted to any plane. Define

$$P = x_1 x_2^{p-1} x_3^{p-1} (-x_1^{p-1} + x_2^{p-1} + x_3^{p-1})$$

This polynomial is of degree $3p - 2$. We claim that it drops a degree when restricted to any plane.

Proof. When restricting to a plane with variables y_1, y_2, there are only two relevant monomials of degree $3p-2$ in $\mathcal{B}_{2,2}$: $y_1^{2p-1} y_2^{p-1}$ and $y_1^{p-1} y_2^{2p-1}$. Given a generic linear substitution $(x_1, x_2, x_3) = (a_1, a_2, a_3) y_1 + (b_1, b_2, b_3) y_2$, the coefficient of $y_1^{2p-1} y_2^{p-1}$ may be expressed as a polynomial $C(a_i, b_i)$ in $a_1, a_2, a_3, b_1, b_2, b_3$. The polynomial C may be confirmed to be divisible by $-a_2^7 a_3 b_1 + a_2 a_3^7 b_1 + a_1^7 a_3 b_2 - a_1 a_3^7 b_2 - a_1^7 a_2 b_3 + a_1 a_2^7 b_3$, which is 0 for all values of a_i, b_i. By symmetry, the coefficient of $y_1^{p-1} y_2^{2p-1}$ will also always be 0. ◀