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

On local characterization of multiplicity codes

A thesis
submitted for
the Degree of
Master of Science
by
Roie Salama

under the supervision of Prof. Amnon Tashma

Tel Aviv University
September 2021

Table of Contents

Acknowledgments

I would like to thank my advisor, Prof. Amnon Tashma. I was lucky to be given the opportunity to work with someone with such knowledge and expertise, together with extreme dedication and patience. Doing this work was made into a really interesting and fulfilling experience, thanks to him.

1 Introduction

1.1 Background and related work

An error correcting code, is a scheme which helps to detect and correct errors in a given data. A (k, n) - linear error correcting code $\mathcal{C} = \{C_n\}$ is a family of linear spaces, of dimension k, where each C_n contains words of length n, which we call the codewords. The two basic parameters of interest when dealing with error correcting codes are

- **The rate** : The ratio $\frac{k}{n}$, which is an indicator of how much redundant information is present in the codewords.
- **The (relative) distance** : The minimal ratio of coordinates, for which two codewords of the same length differ.

It is easy to see that given a corrupt codeword, one could deduce the original codeword from it (atleast information theoretically), as long as the corruption does not reach half of the relative distance. It is known since [Sha01] and [Ham50] that optimal error correcting codes (in terms of rate and distance) exist. I.e, codes with constant rate and constant relative distance. However, optimality in terms of rate and distance is not the end of the road, and since then there has been a lot of interest regarding the **local** properties of error correcting codes. The notion of locality in codes, says that one can look at a small fraction of symbols of a given word, and detect/correct errors in it. Few notions of locality in codes are

- Local correctability (**LCC**) : We say that a code $\mathcal{C}$ is locally correctable if there is a randomized algorithm, which given a string w which is close to a codeword c, and a coordinate i, computes c_i (with good probability) by making a small amount of queries to w.
- Local Testability (**LTC**) : We say that a code $\mathcal{C}$ is locally testable if there is a randomized algorithm, which given a string w, decides whether w is a codeword of $\mathcal{C}$, or far from any codeword of $\mathcal{C}$ (usually with probability which depends on the distance from $\mathcal{C}$), by making a a small amount of queries to w.

- Low density parity check (**LDPC**) : We say that a code $\mathcal{C}$ is an $LDPC$ code, if there is a subset of the dual code $\mathcal{B} \subset \mathcal{C}^{\perp}$, such that $sp(B) = \mathcal{C}^{\perp}$, and each $z \in B$ has small weight (where weight is the number of non-zero coordinates). We think about the set $\mathcal{B}$ as the set of constraints which define the code.

Although the definition of an $LDPC$ code does not explicitly refer to testing or locality, the concepts of $LDPC$ and LTC codes are closely related, and one can think of an $LDPC$ code as having a "local characterization". More precisely, given such a set $\mathcal{B}$ as in the definition of $LDPC$ above, one could devise a test by choosing some $z \in \mathcal{B}$ and check whether $z \cdot w = 0$ (for our input w). We see that by definition, a word w will pass the test for every choice of z if and only if it is a codeword of $\mathcal{C}$. Moreover, the fact that z has small weight, means we only have to query a small number of coordinates from w in order to compute $z \cdot w$. While $LDPC$ codes provide a low-weight characterization, the definition of $LDPC$ does not promise any robustness for the test (I.e, it might so happen that a word is very far for $\mathcal{C}$, but will pass the test with a high probability).

In [KS08], Kaufman and Sudan showed that in some algebraic contexts, when the characterization is generated as the orbit of the affine group, the existence of a local characterization is in fact a sufficient condition for obtaining the robustness needed for local testing.

In this paper, we deal with the question of existence of local characterizations for a special kind of error correcting code, called the multiplicity code, which was first defined in [KSY14]. In [KSY14], multiplicity codes were proved to be locally decodable, and in [KMRZS17], they served as a building block for the construction of the state of the art locally decodable codes. However, the question of local testability, was stated as an interesting open question in [Kop13], and for all we know, it remains open to this day. Inspired by the result in [KS08] (about deriving local testing from local characterization in some algebraic contexts), we hope that our results about the local characterization of multiplicity codes, will serve as a stepping stone towards proving their local testability, although unfortunately, the result in [KS08] cannot be used directly as it is stated, mainly because the alphabet

of the code is not the underlying field over which it is linear.

1.2 Our results and techniques

In this paper, we analyse how well two of the natural tests for multiplicity codes do, in terms of local characterization. For positive integers m, d, s, q (where q is a prime power), multiplicity codes are defined as the set of vectors of evaluations of degree $\leqslant d$ polynomials in m variables over the field $\mathbb{F}_q$, and their derivatives of order $< s$ (see Section 2.3). The standard and well known local testing algorithm for Reed-Muller codes (see [FS95] for example) tests a given function by restricting it to a random line in the m dimensional space, and check if the restriction can be realised as a $\leqslant d$ univariate polynomial. One could naturally generelize this test for multiplicity codes, by checking if the line restriction can be realised as a univariate polynomial and its s derivatives (where the univariate derivatives can be computed using the multivariate ones). We call this kind of test the "line test". In the case of Reed-Muller codes, the line test works for $q \geqslant d + 2$, which is tight for these kind of codes. We prove both an upper and a lower bound on the parameters for which the line test is a local characterisation for multiplicity codes. Our two main results regarding this test are stated formally in Theorems 5.2 and 7.1. Stated informally :

Theorem 1.1 (The line test for large q (informal))**.** *The line test is a local characterization for multiplicity codes, when $q \geqslant d + 2$.*

Theorem 1.2 (The line test for small q (Informal))**.** *The line test is* NOT *a local characterization for $q \leqslant d$.*

We also devise a similar test, in which we consider restrictions to two dimensional planes. We call this test the "plane test". In Section 8 we analyse the plane test in the case $s = 2$ and prove:

Theorem 1.3 (The plane test for $s = 2$ (Informal))**.** *The plane test is a local characterization for $s = 2$, $q > 2$, and $d < 2q - 1$.*

The characterization results in Theorems 1.1 and 1.3 can (in both cases) be separated into two parts :

- **Completeness** : Every codeword of the multiplicity code passes all the tests.

- **Soundness** : Every word which passes all the tests is a codeword of the multiplicity code.

We refer to the words given as an input to the test as tables. The completeness part of Theorems 1.1 and 1.3 are the trivial parts of the proofs, and follow directly from the construction of the tests. The soundness proof for Theorem 1.1 is pretty straightforward and is done by elementary methods. Given some "table" (allegedly the valuation vector of some function and its derivatives) which passes every line test, we use the result in [FS95] for Reed-Muller codes as a black-box, in order to obtain a low degree polynomial, P, for which its evaluations match the $0-th$ derivative part of the table. We are then left to show that the rest of the table is consistent with the derivatives of P. This is done by showing that the tests impose a sufficiently large number of linear constraints on the table, such that the only way of passing all of them is by being consistent with P. To see this, the main observation will be that these constraints are closely related to the standard Reed-Muller codes, where the number of variables is now s (the number of derivatives in our context of the multiplicity code).

The proof of Theorem 1.3 uses heavier machinery. In Section 3, we develop an understanding of the relation between tables of valuations and polynomials which are consistent with them. This is done by relying on the theory of Grobner bases [CLO13], and the combinatorial Nullstensatz [Alo99]. We also use a generalization of the combinatorial Nullstensatz for multiplicities higher than 1 [BS09]. In Lemma 3.13 we devise a purely algebraic criteria (i.e, in terms of polynomials and ideals) for when a table represents a codeword of the multiplicity code. In the proof of Theorem 1.3, this criteria is constantly being used, in order to translate between questions of tables and evaluations to the question of whether some specific polynomial is low degree. This translation between the algebraic objects and evaluation tables, also helps us construct a polynomial which cheats the line test in Theorem 1.2. This is essentially done by

1. Constructing a polynomial which vanishes (with multiplicity 1) on the entire cube ${\mathbb{F}_q}^m$.

2. "Homogenising" it (i.e, making the polynomial homogeneous).

3. Multiplying it by a suitable factor to make its degree equal $d+1$.

The result is a degree $> d$ polynomial, for which every restriction to a line is of degree d.

2 Preliminaries

We denote vectors (tuples) by either bold letters. We sometimes use capital letters when thinking treating the vector as a multi-index (an element of $\mathbb{N}^m$). For $\mathbf{X} = X_1, \ldots, X_m$ we denote by $\mathbb{F}[\mathbf{X}]$ the set of multivariate polynomials in the variables $X_1, \ldots X_m$. We denote by $\mathbb{F}[\mathbf{X}]^{\leqslant d}$ the set of polynomials of total degree at most d , and by $\mathbb{F}[\mathbf{X}]^{loc\leqslant d}$ the set of polynomials of local degree at most d (i.e degree in each variable). Given a vector $\mathbf{i} \in \mathbb{N}^m$, we use the notation

$$\mathbf{X}^{\mathbf{i}} \stackrel{\text{def}}{=} \prod_{j=1}^{m} X_j^{\mathbf{i}_j}.$$

For a vector $\mathbf{i} \in \mathbb{N}^m$, and a set $S \subset [m]$, we define the vector $\mathbf{i}_S$ by

$$(\mathbf{i}_S)_j = \begin{cases} \mathbf{i}_j, & j \in S \\ 0, & j \notin S \end{cases}$$

.

Recall The definition of the binomial and multinumial coefficients for natural numbers :

$$\binom{n}{k} \stackrel{\text{def}}{=} \frac{n!}{k!(n-k)!}$$
$$\binom{n}{k_1, \ldots, k_\ell} = \frac{n!}{k_1! \cdots k_m!}$$

where $\sum k_i = n$. We extend this definition to $I, J, J_1, \ldots, J_\ell \in \mathbb{N}^m$ by

$$\binom{I}{J} \stackrel{\text{def}}{=} \prod_{t=1}^{m} \binom{I_t}{J_t}$$
$$\binom{I}{I_1, \ldots, I_\ell} \stackrel{\text{def}}{=} \prod_{t=1}^{n} \binom{I_t}{(J_1)_t \cdots (J_\ell)_t}.$$

We also use the notations :

$$g(x) \stackrel{\text{def}}{=} X^q - X \in \mathbb{F}_q[X]$$
$$g^{\mathbf{b}}(\mathbf{X}) \stackrel{\text{def}}{=} \prod_{i=1}^{m} g(X_i)^{b_i} \in \mathbb{F}_q[\mathbf{X}]$$

for $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{N}^m$.

2.1 Reed-Muller code

Definition 2.1. *Let d, m be non-negative integer, and q a prime power. The (m, d, q) - Reed-Muller code, is defined as the set of evaluation vectors, of m - variate polynomials of degree $\leqslant d$, over ${\mathbb{F}_q}^m$. I.e*

$$RM(m, d, q) = \left\{ (f(\alpha))_{\alpha \in {\mathbb{F}_q}^m} \mid f \in \mathbb{F}_q[X_1, \ldots, X_m]^{\leqslant d} \right\}. \tag{2.1}$$

Lemma 2.2 (Sweartz-Zippel)**.** *Let $P \in \mathbb{F}[X_1, \ldots, X_m]$ be a non-zero polynomial of total degree $d \geqslant 0$ over a field $\mathbb{F}$. Let $S \subset \mathbb{F}$. Then*

$$Pr_{\alpha \in S^m}[P(\alpha) = 0] \leqslant \frac{d}{\mid S \mid}$$

Corollary 2.3. *$RM(m, d, q)$ has relative distance atleast $1 - \frac{d}{q}$ (when $q > d$).*

Proof. Since the code is linear, the distance is the minimal weight of a non-zero codeword. Let $f \neq 0$. By using Swearz-Zippel with $S = \mathbb{F}_q$, we conclude that f vanishes on at most $\frac{d}{q}$ fraction of ${\mathbb{F}_q}^m$. Thus, f has a relative weight of atleast $1 - \frac{d}{q}$. □

2.2 Hasse Derivatives

Definition 2.4. *(Hasse derivative) For a multivariate $P(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ where $\mathbf{X} = (X_1, \ldots X_m)$ for some $m \in \mathbb{N}$ and a non-negative vector $\mathbf{i} \in \mathbb{N}^m$, the i-th Hasse derivative of P , denoted by $P^{(\mathbf{i})}(\mathbf{X})$, is the coefficient of Z^i in the polynomial $P(\mathbf{X}, \mathbf{Z}) = P(\mathbf{X} + \mathbf{Z})$. Thus*

$$P(\mathbf{X} + \mathbf{Z}) = \sum_{\mathbf{i}} P^{(\mathbf{i})}(\mathbf{X}) \cdot \mathbf{Z}^i$$

Hasse derivatives are linear. I.e, for all $P, Q \in \mathbb{F}[\mathbf{X}]$ and $\lambda \in \mathbb{F}$,

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

.

Claim 2.5 (The product rule)**.** *For $P, Q \in \mathbb{F}[\mathbf{X}]$ we have*

$$(PQ)^{(r)}(\mathbf{X}) = \sum_{i=0}^{r} P^{(i)}(\mathbf{X}) \cdot Q^{(r-i)}(\mathbf{X}). \tag{2.2}$$

Proof. We calculate the coefficient of $\mathbf{Z}^r$ in $PQ(\mathbf{X} + \mathbf{Z})$. By definition we have

$$\begin{aligned}(PQ)(\mathbf{X} + \mathbf{Z}) &= P(\mathbf{X} + \mathbf{Z}) \cdot Q(\mathbf{X} + \mathbf{Z}) \\ &= \left(\sum P^{(i)}(\mathbf{X})\mathbf{Z}^i\right) \cdot \left(\sum Q^{(i)}(X)\mathbf{Z}^i\right) \\ &= \sum_{\ell+k=r} P^{(\ell)}(\mathbf{X})Q^{(k)}(\mathbf{X}) \cdot \mathbf{Z}^r,\end{aligned}$$

and the coefficient of $\mathbf{Z}^r$ is indeed $\sum_{i=0}^{r} P^{(i)}(\mathbf{X}) \cdot Q^{(r-i)}(\mathbf{X})$. □

Definition 2.6 (Multiplicity)**.** *For $P(\mathbf{X}) \in \mathbb{F}[\mathbf{X}]$ and $\mathbf{a} \in \mathbb{F}^m$, the multiplicity of P at $\mathbf{a}$, denoted by $mult(P, \mathbf{a})$, is the largest integer M such that for every non-negative vector $\mathbf{i}$, with $wt(\mathbf{i}) < M$, we have $P^{(\mathbf{i})}(\mathbf{a}) = 0$. If M may be taken arbitrarily large, we set $mult(P, \mathbf{a}) = \infty$.*

Note that by definition $mult(P, \mathbf{a}) \geqslant 0$ for every $\mathbf{a}$. One important property about multiplicities, is a generalization of the Schwartz-Zippel lemma for multivariate polynomials.

Lemma 2.7 (3.3 in [KSY14]). *Let $P \in \mathbb{F}[\mathbf{X}]$ be a nonzero polynomial of total degree at most d. Then for any finite $S \in \mathbb{F}$,*

$$\sum_{\mathbf{a} \in S^m} mult(P, \mathbf{a}) \leqslant d \cdot \mid S \mid^{m-1}$$

In particular, for any integer $s > 0$,

$$Pr_{\mathbf{a} \in S^m}[mult(P, \mathbf{a}) \geqslant s] \leqslant \frac{d}{s \mid S \mid}$$

Remark 2.8. *In the univariate case, this gives us a generalization of the "degree mantra" . A non-zero univariate polynomial $P \in \mathbb{F}[X]$ of degree $< d$ satisfies*

$$\sum_{a \in \mathbb{F}_q} mult(P, a) \leqslant d$$

2.3 Multiplicity codes

Definition 2.9 (Multiplicity code). *Let s, d, m be non-negative integers, and let q be a prime power. Let*

$$\Sigma_{m,s} = \mathbb{F}_q{}^{\{\mathbf{i}: wt(\mathbf{i}) < s\}} \simeq \mathbb{F}^{\binom{m+s-1}{m}}.$$

For $P(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots X_m]$, we define the order s evaluation of P at $\mathbf{a}$, denote by $P^{(<s)}(\mathbf{a})$ to be the vector $(P^{(\mathbf{i})}(\mathbf{a}))_{\mathbf{i}: wt(\mathbf{i}) < s} \in \Sigma_{m,s}$. The multiplicity code $Mult(m, d, s, q)$ is defined as follows. The alphabet of the code is $\Sigma_{m,s}$, and the length is q^m. Every polynomial $P(\mathbf{X}) \in \mathbb{F}_q[X_1, \ldots, X_m]$ of $deg(P) \leqslant d$ defines a codeword by $\left(P^{(<s)}(\mathbf{a})\right)_{\mathbf{a}: \mathbf{a} \in \mathbb{F}_q{}^m} \in (\Sigma_{m,s})^{q^m}$.

Definition 2.10. *We will use the notation $MRM_q(m, d, s) \coloneqq Mult(m, d, s, q)$ ("Reed-Muller multiplicity codes") and $MRS_q(d, s) \coloneqq Mult(1, d, s, q)$ ("Reed-Solomon multiplicity codes").*

The following lemma states the relationship between the derivatives of a polynomial to the derivatives of its restriction to a line. This lemma plays

an important role in the local decodability result in [KSY14], and it will also play an essential role in our results.

Lemma 2.11 ([KSY14], Sec 4)**.** *Let $P \in \mathbb{F}[\mathbf{X}]$ be a multivariate polynomial where $\mathbf{X} = (X_1, \ldots, X_m)$. Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$, and define a univariate polynomial by $Q(t) = P(\mathbf{a} + \mathbf{b}t)$. Then*

$$Q^{(j)}(t) = \sum_{\mathbf{i}: wt(\mathbf{i})=j} P^{(\mathbf{i})}(\mathbf{a} + \mathbf{b}t) \cdot \mathbf{b}^{\mathbf{i}}$$

Proof. By the definition of Hasse derivatives, we get the following two identities:

$$P(\mathbf{a} + \mathbf{b}(t+R)) = Q(t+R) = \sum_j Q^{(j)}(t) R^j$$

$$P(\mathbf{a} + \mathbf{b}(t+R)) = \sum_{\mathbf{i}} P^{(\mathbf{i})}(\mathbf{a} + \mathbf{b}t)(\mathbf{b}R)^{\mathbf{i}}$$

and by comparing coefficients of R^j we get

$$Q^{(j)}(t) = \sum_{\mathbf{i}: wt(\mathbf{i})=j} P^{(\mathbf{i})}(\mathbf{a} + \mathbf{b}t) b^{\mathbf{i}}$$

. □

We would also like to derive a formula for the derivatives of restrictions to a 2 dimensional plane.

Lemma 2.12. *Let $P \in \mathbb{F}[\mathbf{X}]$ be a multivariate polynomial where $\mathbf{X} = (X_1, \ldots, X_m)$. Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$, and define a bivariate polynomial by $Q(t, r) = P(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$. Then for $\mathbf{j} \in \mathbb{N}^2$:*

$$Q^{(\mathbf{j})}(t, r) = \sum_{\mathbf{i} \in \mathbb{N}^m} P^{(\mathbf{i})}(\mathbf{a}t + \mathbf{b}r + \mathbf{c}) \cdot \sum_{k=0}^{m} \sum_{\substack{S \subset [m] \\ |S|=k \\ wt(\mathbf{i}_S)=\mathbf{j}_1, wt(\mathbf{i}_{\bar{S}})=\mathbf{j}_2}} \mathbf{a}^{\mathbf{i}_S} \mathbf{b}^{\mathbf{i}_{\bar{S}}}.$$

where $\bar{S}$ is the complement of S (see the notation $\mathbf{i}_S$ in section 2).

Proof. Given $R_1, R_2 \in \mathbb{F}$, we write the expression $P(\mathbf{a}(t+R_1)+\mathbf{b}(r+R_2)+\mathbf{c})$ in two different ways. Denote $\mathbf{v} = (t, r)$ and $\mathbf{R} = (R_1, R_2)$. Then on one hand

$$\begin{aligned} P(\mathbf{a}(t+R_1)+\mathbf{b}(r+R_2)+\mathbf{c}) &= Q(t+R_1, r+R_2) = Q(\mathbf{v}+\mathbf{R}) \\ &= \sum_{j\in\mathbb{N}^2} Q^{(j)}(\mathbf{v}) R_1^{\mathbf{j}_1} R_2^{\mathbf{j}_2}. \end{aligned}$$

On the other hand

$$\begin{aligned} P(\mathbf{a}(t+R_1)+\mathbf{b}(r+R_2)+\mathbf{c}) &= P(\mathbf{a}t+\mathbf{b}r+c+R_1\mathbf{a}+R_2\mathbf{b}) \\ &= \sum_{\mathbf{i}\in\mathbb{N}^m} P^{(\mathbf{i})}(\mathbf{a}t+\mathbf{b}r+c)\cdot(R_1\mathbf{a}+R_2\mathbf{b})^{\mathbf{i}} \\ &= \sum_{\mathbf{i}\in\mathbb{N}^m} P^{(\mathbf{i})}(\mathbf{a}t+\mathbf{b}r+c)\cdot\prod_{\ell=1}^{m}(a_kR_1+b_kR_2)^{\mathbf{i}_\ell} \\ &= \sum_{\mathbf{i}\in\mathbb{N}^m} P^{(\mathbf{i})}(\mathbf{a}t+\mathbf{b}r+c)\cdot\sum_{k=0}^{m}\sum_{\substack{S\subset[m]\\|S|=k}} \mathbf{a}^{\mathbf{i}_S}\mathbf{b}^{\mathbf{i}_{\bar{S}}} R_1^{wt(\mathbf{i}_S)} R_2^{wt(\mathbf{i}_{\bar{S}})}. \end{aligned}$$

By comparing coefficients of $R_1^{j_1}R_2^{j_2}$ for every $\mathbf{j} = (\mathbf{j}_1, \mathbf{j}_2) \in \mathbb{N}^2$ we get the result.

□

2.4 Grobner bases and Nullstellensatz

We now look at the ring of m variate polynomials over a field $R = \mathbb{F}[X_1, \ldots, X_m]$. The theory of Grobner bases, describes the structure of ideals in this ring. We briefly explain some of the essential concepts of this theory. We refer to [CLO13] for a thorough treatment of this theory.

Definition 2.13. *A monomial order $\succ$ on R is a relation $\succ$ on $\mathbb{Z}^n_{\geqslant 0}$, or equivalently a relation on the set of monomials x^α, $\alpha \in \mathbb{Z}^n_{\geqslant 0}$ satisfying:*

1. *$\succ$ is a total ordering.*
2. *If $\alpha \succ \beta$ and $\gamma \in \mathbb{Z}^n_{\geqslant 0}$ then $\alpha+\gamma \succ \beta+\gamma$.*

3. $\succ$ *is a well-ordering. I.e, every non-empty* $A \subset \mathbb{Z}^n_{\geqslant 0}$ *has a minimal element.*

Example 2.1 (Lexicographic order)**.** *Let* $\alpha, \beta \in \mathbb{Z}^m_{\geqslant 0}$*. We say* $\alpha \succ_{lex} \beta$ *if the minimal* i *which satisfies* $\alpha_i \neq \beta_i$*, also satisfies* $\alpha_i > \beta_i$ *.*

Example 2.2 (Total degree lexicographic order)**.** *The total degree lexicographic order is defined as follows: A monomial* m_1 *is greater than* m_2 *if it has higher total degree, where ties are broken lexicographically (i.e* $X_1 > X_2 > \cdots > X_m$ *). More formally , let* $\alpha, \beta \in \mathbb{Z}^m_{\geqslant 0}$*. Then* $\alpha \succ_{tot} \beta$ *if*

$$wt(\alpha) = \sum \alpha_i > wt(\beta) = \sum \beta_i, \text{ or } wt(\alpha) = wt(\beta) \text{ and } \alpha \succ_{lex} \beta$$

Definition 2.14. *Let* $f(\mathbf{X}) = \sum_{\mathbf{i}} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$ *and* $\succ$ *a monomial order.*

1. *The multidegree of* f *is*

$$multideg(f) = \max \{\mathbf{i} \mid a_{\mathbf{i}} \neq 0\}$$

(maximum is taken w.r.t $\succ$*)*

2. *The leading coefficient of* f *is*

$$LC(f) = a_{multideg(f)} \in \mathbb{F}$$

3. *The leading monomial of* f *is*

$$LM(f) = \mathbf{X}^{multideg(f)}$$

4. *The leading term of* f *is*

$$LT(f) = LC(f) \cdot LM(f)$$

The following are very useful properties of multidegrees:

Lemma 2.15 ([CLO13] Chapter 2, lemma 8)**.** *Let $f, g \in \mathbb{F}[X_1, \ldots, X_m]$ be nonzero polynomials. Then:*

1. $multideg(fg) = multideg(f) + multideg(g)$.
2. *If $f + g \neq 0$, then $multideg(f + g) \leqslant \max(multideg(f), multideg(g))$. If, in addition, $multideg(f) \neq multideg(g)$, then equality occurs.*

Definition 2.16 (Multivariate polynomial division)**.** *Let $\succ$ be a monomial order on $\mathbb{Z}^n_{\geqslant 0}$, and let $F = (f_1, \ldots, f_s)$ be an ordered s tuple of polynomials in $\mathbb{F}[\mathbf{X}]$. Then every $f \in \mathbb{F}[\mathbf{X}]$ can be written as*

$$f = q_1 f_1 + \cdots + q_s f_s + r,$$

where $q_i, r \in \mathbb{F}[\mathbf{X}]$, and either $r = 0$ or r is a linear combination, with coefficients in $\mathbb{F}$, of monomials, none of which is divisible by any of $LT(f_1), \ldots, LT(f_s)$. We call r a reminder of the division by F. Moreover,

$$multideg(q_i f_i) \leqslant multideg(f)$$

for every $i \in [s]$. The reminder r is not necessarily unique, and might be dependent on the order of division.

Definition 2.17. *Let $I \neq \{0\} \subseteq \mathbb{F}[\mathbf{X}]$ be an ideal. Fix a monomial ordering on $\mathbb{F}[\mathbf{X}]$. Then*

1. *We denote by $LT(I)$ the set of leading terms of non-zero elements of I.*

$$LT(I) = \left\{ c\mathbf{X}^{\mathbf{i}} \mid \exists f \in I \setminus \{0\} \, . LT(f) = c\mathbf{X}^{\mathbf{i}} \right\}$$

2. *We denote by $\langle LT(I) \rangle$ the ideal generated by elements of $LT(I)$.*

Definition 2.18. *Let $I \neq \{0\} \subseteq \mathbb{F}[\mathbf{X}]$ be an ideal. Fix a monomial ordering on $\mathbb{F}[\mathbf{X}]$. A subset $G = \{g_1, \ldots, g_t\} \subset I$ is said to be a **Grobner basis** for I, if*

$$\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle.$$

Fact 2.1. *Every ideal $I \subset \mathbb{F}[X_1, \ldots, X_m]$ is finitely generated, and moreover, has a Grobner basis.*

The importance of a Grobner basis, is that it gives us a natural way of choosing representatives for the quotient space $\mathbb{F}[X_1, \ldots, X_m] / I$.

Theorem 2.19 (Sec 2 Prop 1 in [CLO13])**.** *Let $I \subset \mathbb{F}[X_1, \ldots, X_m]$ be an ideal and $G = \{g_1, \ldots, g_t\}$ a Grobner basis. Then given $f \in \mathbb{F}[X_1, \ldots, X_m]$ there is a **unique** $r \in \mathbb{F}[X_1, \ldots, X_m]$ such that*

1. *No term of r is divisible by any of $LT(g_1), \ldots, LT(G_t)$.*
2. *There is a $g \in I$ such that $f = g + r$.*

In other words, the reminder of the polynomial division by G is unique. We call this r, the reduced form of f (relative to I).

Note that the reduced form of any polynomial is equivalent to this polynomial modulo I. Thus, as said above, this theorem gives us a natural way of choosing representatives modulo I.

Theorem 2.20. *Let $R = \mathbb{F}[\mathbf{X}]$ be the ring of polynomials, and $I \subset R$ an ideal. Let G be a Grobner basis for I. Then the set*

$$\mathcal{B} = \{M(\mathbf{X}) \mid M \text{ is a monomial which is not divisible by any of } LT(g) \text{ for } g \in G\},$$

is a basis for R / I .

Proof. To see that this set is a spanning set, just note that by 2.19, any f can be reduced to some $r \in R / I$ such that every monomial of r is in $\mathcal{B}$. To see that it is independent, note that a linear combination $\sum \alpha_i M_i$ of elements in $\mathcal{B}$ is already a polynomial in its reduced form, and thus, it is zero in R / I if and only if it is zero as a polynomial. In other words, $\alpha_i = 0$ for every i. □

The following criterion determines whether G is a Grobner basis.

Definition 2.21 (LCM and S polynomials)**.** *Let $f, g \in \mathbb{F}[X] = \mathbb{F}[X_1, \ldots, X_m]$ be nonzero polynomials. Let $\alpha = multideg(f)$ and $\beta = multideg(g)$.*

1. *The least common multiple of* $LM(f)$ *and* $LM(g)$*, denoted* $LCM(f,g)$*, is* $\mathbf{X}^{\boldsymbol{\gamma}}$*, where* $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_m)$ *and* $\gamma_i = \max\{\alpha_i, \beta_i\}$ *for each* i*.*

2. *The* $S-$ *polynomial of* f *and* g *is*

$$S(f,g) = \frac{LCM(f,g)}{LT(f)} \cdot f - \frac{LCM(f,g)}{LT(g)} \cdot g$$

Theorem 2.22 (Buchberger's Criterion (Sec 6 in [CLO13]))**.** *Let* $I \subset \mathbb{F}[\mathbf{X}]$ *be an ideal. Then a basis of* $G = \{g_1, \ldots, g_t\}$ *of* I *is a Grobner basis of* I *if and only if for all pairs* $i \neq j$*, the reminder on division of* $S(g_i, g_j)$ *by* G *(listed in any order) is zero .*

Note that we always have $S = S(g_i, g_j) \in I$ by the definition of S. When saying the reminder of the division by G is zero, we mean that there are $\{f_i\}$, such that

$$S = \sum f_i g_i,$$

and $multideg(f_i g_i) \leqslant multideg(S)$ for every i (as in definition 2.16).

Theorem 2.23 (Combinatorical Nullstellensatz [Alo99])**.** *Let* $\mathbb{F}$ *be a field, and* $A_1, \ldots, A_m \subseteq \mathbb{F}$ *. Let* $g_i(X) = \prod_{\alpha \in A_i}(X - \alpha)$ *for* $i = 1, \ldots, m$*. Assume a polynomial* $f \in \mathbb{F}[\mathbf{X}]$ *satisfies* $f(\alpha) = 0$ *for all* $\alpha \in A_1 \times \cdots \times A_m$*. Then there are* $h_1, \ldots, h_t$ *such that*

$$f = \sum h_i g_i,$$

and $deg(h_i) + deg(g_i) \leqslant deg(f)$ *for all* i*.*

When $A_i = \mathbb{F}_q$ denote

$$g(X) \quad = \quad \prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X^q - X.$$

Also, let I_m denote the ideal

$$I_m = \{f \in R \mid \forall \alpha \in {\mathbb{F}_q}^m \quad f(\alpha) = 0\}.$$

Corollary 2.24. $I_m = \langle (g(X_1), \ldots, g(X_m)) \rangle$.

Proof. Let $f \in I_m$. By Theorem 2.23, taking $S_i = \mathbb{F}_q$ for every i, we get that $f = \sum h_i g_i$ for some $\{h_i\}$ and so $f \in \langle (g_i)_{i=1}^m \rangle$. The other inclusion is trivial, since $g(X_i) = X_i^q - X_i$ vanishes on ${\mathbb{F}_q}^m$ for every i. □

Lemma 2.25. *$G = \{g(X_i)\}$ is a Grobner basis for I_m (relative to the total degree lexicographic order).*

Proof. We use Theorem 2.22. We start by computing the S- polynomial for g_i, g_j. For convenience we denote $X = X_i$, $Y = X_j$. We have

$$lcm(X^q, Y^q) = X^q Y^q$$

Now,

$$\begin{aligned} S(X^q - X, Y^q - Y) &= \frac{X^q Y^q}{X^q} \cdot (X^q - X) - \frac{X^q Y^q}{Y^q} \cdot (Y^q - Y) \\ &= Y^q X^q - XY^q - XY^q - YX^q = -(X^q Y + XY^q) \\ &= -Y(X^q - X) - X(Y^q - Y) = 0 \bmod I_m. \end{aligned}$$

Thus, the reminder is indeed zero, and the criteria in Theorem 2.22 is satisfied. □

Let $s \in \mathbb{N}$ and let $I_{m,s}$ denote the ideal

$$I_{m,s} = \{f \in R \mid \forall \alpha \in {\mathbb{F}_q}^m \ \ Mult(f; \alpha) \geq s\}.$$

In this notation, $I_{m,1} = I_m$ defined before.

For every $\mathbf{b} \in \mathbb{N}^m$, such that $wt(b) = s$, define

$$g^{\mathbf{b}} = \prod_{i=1}^{m} g(X_i)^{b_i}.$$

Theorem 2.26 (Combinatorical Nullstellensatz with multiplicity, [BS09] Sec 3)**.** *$I_{m,s} = \langle g^{\mathbf{b}} \rangle_{wt(\mathbf{b})=s}$. Furthermore, the set $\mathcal{G}_{m,s} = \left\{g^{\mathbf{b}}\right\}_{wt(\mathbf{b})=s}$ is a Grobner basis for $I_{m,s}$.*

Proof. To see that $I_{m,s}$ is indeed an ideal, fix $f \in I_{m,s}$ and $g \in \mathbb{F}[\mathbf{X}]$. Then for $r < s$: $(gf)^{(r)} = \sum_{i=0}^{r} f^{(i)} \cdot g^{(r-i)} = 0$ and so $gf \in I_{m,s}$. Also, clearly, $g^{\mathbf{b}} \in I_{m,s}$

for every $\mathbf{b}$ with $wt(\mathbf{b}) = s$. [BS09] Sec 3 shows that every $f \in I_{m,s}$ can be expressed as a combination of the $g^{\mathbf{b}}$ and, furthermore, $f = \sum_{\mathbf{b}:wt(\mathbf{b})=s} g^{\mathbf{b}} h_{\mathbf{b}}$ for some $h_{\mathbf{b}}$ with $deg(h_{\mathbf{b}}) \leqslant deg(f) - s\deg(g)$.

In particular, this is true for the S polynomials in Theorem 2.22. I.e, every such S polynomial can be expressed as $S = \sum g^{\mathbf{b}} h_{\mathbf{b}}$ where $deg(g^{\mathbf{b}} h_{\mathbf{b}}) \leqslant deg(S)$. Thus, Buchberger's criterion holds, and $\left\{g^{\mathbf{b}}\right\}$ is a Grobner basis. □

3 Polynomials and tables

In the context of codes and local testing, it is important to distinguish between a (possibly multivariate) polynomial, which is an algebraic object, determined only by its coefficients, and the function it represents by evaluating it on tuples from the relevant field. For example, the univariate polynomials $P_1 = 0$ and $P_2 = x^q - x$ are identical as a functions on $\mathbb{F}_q$, but different as polynomials. In this section we would like to discuss polynomials and their evaluations more formally.

Given parameters s, d, m ,recall from 2.3 the definition of $\Sigma_{m,s}$:

$$\Sigma_{m,s} = \mathbb{F}_q^{\{\mathbf{i}:wt(\mathbf{i})<s\}} \simeq \mathbb{F}^{\binom{m+s-1}{m}}.$$

Definition 3.1. *A table T is an element of $(\Sigma_{m,s})^{q^m}$. The multiplicity s, evaluation function for $m-$ variate polynomials, $EVAL_{m,s} : \mathbb{F}_q[X_1, \ldots, X_m] \to (\Sigma_{m,s})^{q^m}$ is defined by*

$$EVAL_{m,s} = \left(P^{(\mathbf{i})}(a)\right)_{wt(\mathbf{i})<s, a\in\mathbb{F}_q{}^m}$$

. We say that $T \in (\Sigma_{m,s})^{q^m}$ is a table for $P \in \mathbb{F}_q[X_1, \ldots, X_m]$ if $EVAL(P) = T$.

Definition 3.2. *(Table resrictions) Given a table $T \in (\Sigma_{m,s})^{q^m}$, we denote its restriction to $\Sigma_{m,s'}$ by $T_{s'}$, for $s' < s$ (note that $\Sigma_{m,s'}$ is naturally embedded in $\Sigma_{m,s}$).*

Remark 3.3. *Note that every polynomial determines its table $EVAL(P)$. However, one table T might satisfy $T = EVAL(P_1)$ and $T = EVAL(P_2)$ for $P_1 \neq P_2$.*

Definition 3.4. *The multiplicity s evaluation function for $m-$ variate polynomials of (total) degree $\leqslant d$, $EVAL_{d,m,s} : \mathbb{F}_q^{\leqslant d}[X_1, \ldots, X_m] \to (\Sigma_{m,s})^{q^m}$ is defined by*

$$EVAL_{d,m,s} = EVAL_{m,s}|_{\mathbb{F}_q^{\leqslant d}[X_1,\ldots,X_m]}$$

Definition 3.5. *The multiplicity s evaluation function for $m-$ variate polynomials of **local** degree $\leqslant d$, $EVAL^{loc}_{d,m,s} : \mathbb{F}_q^{loc\leqslant d}[X_1, \ldots, X_m] \to (\Sigma_{m,s})^{q^m}$ is defined by*

$$EVAL^{loc}_{d,m,s} = EVAL_{m,s}|_{\mathbb{F}_q^{loc\leqslant d}[X_1,\ldots,X_m]}$$

Lemma 3.6.

$$Ker(EVAL_{m,s}) = \langle \prod_{i=1}^{m} (X_i^q - X_i)^{b_i} \rangle_{wt(b)=s}.$$

Proof. By definition, the kernel of $EVAL_{m,s}$ is

$$I_{m,s} = \{ f \in \mathbb{F}[X_1, \ldots, X_m] \mid mult(f, \alpha) = s \forall \alpha \in \mathbb{F}_q \},$$

and by 2.26,

$$I_{m,s} = \langle \prod_{i=1}^{m} (X_i^q - X_i)^{b_i} \rangle_{wt(b)=s}.$$

□

Since $I_{m,s}$ clearly does not contain any non-zero polynomial of either local or total degree less than sq, we conclude the following :

Corollary 3.7. *For $d < sq$, both $EVAL_{d,m,s}$ and $EVAL^{loc}_{d,m,s}$ are injective.*

By the first isomorphism theorem, $EVAL$ naturally induces a mapping $\overline{EVAL_{m,s}} : \mathbb{F}_q[X_1, \ldots, X_m] \Big/ I_{m,s} \to (\Sigma_{m,s})^{q^m}$.

Claim 3.8. *$\overline{EVAL_{m,s}}$ is an isomorphism when $q > s$.*

Proof. We already know that $\overline{EVAL_{m,s}}$ is injective. Thus, it is sufficient to show that

$$dim \left(\mathbb{F}_q[X_1, \ldots, X_m] \Big/ I_{m,s} \right) \geqslant dim \left((\Sigma_{m,s})^{q^m} \right).$$

Denote for $b \in \mathbb{N}^m$, the polynomial

$$g_b = \prod_{i=1}^{m} (X_i^q - X_i)^{b_i}.$$

Then $I_{m,s} = \langle g_b \rangle_{wt(b)=s}$.

Consider the set

$$\mathcal{A} = \left\{ \left(\prod_{i=1}^{m} X_i^{j_i} \right) \mathbf{X}^{bq} \mid wt(b) < s, 0 \leqslant j_i < q \right\}$$

.

We first claim, that the elements, as represented in the set, appear without repetitions. More formally,

Claim 3.9. *For $b^1, b^2, j^1, j^2 \in \mathbb{N}^m$ with $wt(b^1), wt(b^2) < s$, $0 \leqslant j_i^1, j_i^2 < q$:*

$$\left(\prod_{i=1}^{m} X_i^{j_i^1} \right) \mathbf{X}^{b^1 q} = \left(\prod_{i=1}^{m} X_i^{j_i^2} \right) \mathbf{X}^{b^2 q} \Rightarrow b^1 = b^2, j^1 = j^2$$

.

And indeed, let b^1, b^2, j^1, j^2 as above. By looking at the power of X_i for some i in the monomials above, we have

$$j_i^1 + b_i^1 q = j_i^2 + b_i^2 q$$

. Since $q > s > b_i^1, b_i^2$, both sides of the equation are representations of the same natural number as a quotient and a reminder by q. Since such a representation is unique, $b_i^1 = b_i^2, j_i^1 = j_i^2$. Since this is true for every i, we have $b^1 = b^2, j^1 = j^2$.

We conclude that the size of $\mathcal{A}$ is exactly

$$\mid A \mid = \mid \{(b, j) \in \mathbb{N}^m \times \mathbb{N}^m \mid 0 \leqslant j_i < q, wt(b) < s\} \mid = q^m \cdot \binom{m+s-1}{m}.$$

We claim this set $\mathcal{A}$, is independent in the quotient space $\mathbb{F}_q[X_1, \ldots, X_m] \Big/ I_{m,s}$. Indeed, note that every element of $\mathcal{A}$ is not divisible by any of the $LT(g_b) = \mathbf{X}^{bq}$ for $wt(b) = s$. Thus $\mathcal{A}$ is a subset of the basis from 2.20. In particular,

it is an independent set. Thus

$$dim\left(\mathbb{F}_q[X_1,\ldots,X_m]\Big/I_{m,s}\right)\geqslant|\ \mathcal{A}\ |=dim\left((\Sigma_{m,s})^{q^m}\right),$$

as desired.

□

Note that from the proof of 3.8, we get the following

Corollary 3.10. *The set*

$$\mathcal{A}=\left\{\left(\prod_{i=1}^{m}X_i^{j_i}\right)\mathbf{X}^{bq}\mid wt(b)<s,0\leqslant j_i<q\right\}$$

is a basis for $\mathbb{F}[\mathbf{X}]\Big/I_{m,s}$ *for* $\mathbf{X}=(X_1,\ldots,X_m)$.
This is since it is an independent set of size $dim\left(\mathbb{F}[\mathbf{X}]\Big/I_{m,s}\right)$.

We would also like to introduce another basis for the same quotient space.

Lemma 3.11. *For* $\mathbf{b}\in\mathbb{N}^m$, *define*

$$g^{\mathbf{b}}=\prod_{i=1}^{m}(X_i^q-X_i)^{b_i}.$$

Then

$$\mathcal{B}_{m,s}=\left\{g^{\mathbf{b}}X^I\mid wt(b)<s,\forall i.0\leqslant I_i<q\right\}$$

is a basis for the quotient space $\mathbb{F}[\mathbf{X}]\Big/I_{m,s}$.

Proof. First note that $|\ \mathcal{B}_{m,s}\ |=q^m\cdot\binom{m+s-1}{m}=dim\left(\mathbb{F}[\mathbf{X}]\Big/I_{m,s}\right)$. Thus, it is sufficient to show that $\mathcal{B}$ is an independent set, in the quotient space.By a similar argument as in 3.9, we see that different elements in B have different local degree at X_i for some i. Thus, as polynomials, they are independent. Note also that each element in B is already in its reduced form, since any element of B is not divisible by any of the leading terms $LT(g^{\mathbf{b}})$, in the Grobner basis for $I_{m,s}$. Thus, they are also independent in the quotient space (since any vanishing linear combination in the quotient space $\sum\alpha_i f_i=0\text{mod }I_{m,s}$ is already in its reduced form, and thus $\sum\alpha_i f_i=0$ as polynomials, but f_i are independent as polynomials, and so $\alpha_i=0$ for every i). □

Next, we would like to give a purely algebraic criteria, which states when exactly a table belongs to the code $MRM_q(m,d,s)$.

Definition 3.12. *Let $T \in \Sigma_{m,s}^{q^m}$ be a table. By 3.8, if $q > s$, there is a unique element $P_T \in \mathbb{F}[\mathbf{X}] \Big/ I_{m,s}$, such that $EVAL_{m,s}(P) = T$. We think of P_T as a polynomial in its unique reduced form, obtained by division with the Grobner basis of $I_{m,s}$, and we call it the representing polynomial of T.*

Lemma 3.13. *Assume $d < sq$ and $q > s$. Let $T \in \Sigma_{m,s}^{q^m}$ be a table, and P_T its representing polynomial. Then*

$$T \in MRM_q(m,d,s) \iff deg(P_T) \leqslant d.$$

Proof. First, assume $deg(P_T) \leqslant d$. Then, by definition, since $EVAL_{m,s}(P) = T$, we have $T \in MRM_q(m,d,s)$. For the other direction, assume $T \in MRM_q(m,d,s)$. Then there is some $Q \in \mathbb{F}[\mathbf{X}]$ of total degree $\leqslant d$ such that $EVAL_{m,s}(Q) = T$. In particular, the local degree of Q is less than $d < sq$. Note that P_T also has local degree $< sq$ (since by definition no monomial in it is divisible by any term of the form X_i^{qs}) . By 3.7, we have $Q = P$, and thus $deg(P) = deg(Q) \leqslant d$. □

Lemma 3.14. *Let $T \in \Sigma_{m,s}^{q^m}$ be a table, and let $s' \leqslant s$. Assume the representing polynomial of T is :*

$$P = \sum_{\substack{I,J \\ wt(\mathbf{b})<s \\ I_i<q}} \alpha_{\mathbf{b},I} g^{\mathbf{b}} X^I$$

Then the representing polynomial of $T|_{s'}$ is

$$P_{<s'} = \sum_{\substack{I,J \\ wt(\mathbf{b})<s' \\ I_i<q}} \alpha_{\mathbf{b},I} g^{\mathbf{b}} X^I.$$

Proof. Note that $P_{<s'} = P \bmod I_{m,s'}$.Thus $EVAL_{m,s'}(P_{<s'}) = EVAL_{m,s'}(P) = T|_{s'}$. We get that $P_{<s'}$ satisfies both

1. $EVAL_{m,s'}(P) = T|_{s'}$.

2. $P \in Sp(\mathcal{B}_{m,s'})$.

We know from 3.8, that there is a unique polynomial which satisfies both conditions, and it is the representing polynomial of $T|_{s'}$. □

4 Bases and reductions

Consider the basis $\mathcal{B}_{m,s}$ of $\mathbb{F}[\mathbf{X}]\text{mod } I_{m,s}$ from 3.11. We denote by $\overline{f}$ the reduction of $f \in \mathbb{F}[\mathbf{X}]$ mod $I_{m,s}$. We will now be interested in the case of $m = 2$ (this will serve us in section 8). We would first like to introduce a basis for the space of polynomials in two variables $\mathbb{F}[t, r]$, which interacts "nicely" with the basis $\mathcal{B}_{m,s}$.

Claim 4.1. *Every polynomial $A(t, r) \in \mathbb{F}[t, r]$ can be expressed uniquely in the form*

$$A(t,r) = \sum_{i\in\mathbb{N},j\in\mathbb{N},k<q} A_{i,j,k}(\mathbf{a},\mathbf{b},\mathbf{c})g(t)^i r^j t^k. \tag{4.1}$$

In other words, $\mathcal{D} = \left\{g(t)^i r^j t^k \mid k < q\right\}$ is a basis for $\mathbb{F}[t, r]$. Moreover, this representation satisfies $multideg(g(t)^i r^j t^k) \leqslant multideg(A(t, r))$ both with respect to the total degree lexicographic order where $t > r$, and the total degree lexicographic order where $r > t$.

Proof. We start by showing that $\mathcal{D}$ is a spanning set, i.e, we show that an arbitrary $A(t, r)$ can be expressed as a linear combination of this set. We prove the claim by induction on the local degree at t of A, $deg_t(A(t, r))$. Of course, if $deg_t(A(t, r)) < q$, then A is simply of the form

$$A(t,r) = \sum_{\substack{j \\ k<q}} A_j r^j t^k. \tag{4.2}$$

For $deg_t(A(t, r)) \geqslant q$, we use multivariate polynomial division, to write

$$A(t,r) = \tilde{A}(t,r)g(t) + R \tag{4.3}$$

where $deg_t(\tilde{A}) \leqslant deg_t(A) - q$, and $deg_t(R) < q$. By the induction hypothesis, both R and $\tilde{A}$ have a representation as above, which gives a representation

for A. To see that the set $\mathcal{D}$ is also independent, note that each element $D(t,r) = g(t)^i r^j t^k \in \mathcal{D}$ is uniquely determined by its local degree at t and at r.Indeed, any such element satisfies:

$$deg_t(D) = qi + k$$

which uniquely determines i, k, by uniqueness of division and reminder by q. Also, $deg_r(D) = j$. In other words, every two distinct elements in $\mathcal{D}$ have a different local degree (either at r or at t).This property ensures both that the set $\mathcal{D}$ is independent in $\mathbb{F}[t,r]$, and that the elements in $\mathcal{D}$ have distinct multidegrees, both w.r.t the total degree lexicographic order where $t > r$ and where $r > t$. It follows that any linear combination $\sum \alpha_i f_i$ of such elements $\{f_i\} \subset \mathcal{D}$, has a multidegree of $\max\{\alpha_i f_i\}$ by 2.15. □

We can also define a similar basis for $\mathbb{F}[\mathbf{X}]$ mod $I_{2,s}$ which is slightly different than $\mathcal{B}_{2,s}$. We define

$$\mathcal{B}^*_{2,s} = \left\{ g(t)^b r^i t^j \mid b \in \{0,1\}, i + bq < sq, j < q \right\}. \tag{4.4}$$

It is easy to see that its a basis, since every element in $\mathcal{B}_{2,s}$ can be written as a linear combination of elements in $\mathcal{B}^*_{2,s}$, and no monomial which appears in an element in $\mathcal{B}^*_{2,s}$ is divisible by $LT(g(t)^i g(r)^j)$ for $i + j = s$, and thus they are all reduced and independent mod $I_{2,s}$.

we use the notation $j \overline{\text{ mod }} N$ to denote

$$j \overline{\text{ mod }} N = \begin{cases} j & 0 \le j \le N \\ j \text{ mod } N, & j > N, N \nmid j \\ N, & j > N, N \mid j \end{cases}$$

Note that mod and $\overline{\text{mod}}$ are different only multiples of N.

Claim 4.2. *For $f \in \mathbb{F}[t,r]$, denote by $\overline{f}$ the unique representation of f mod $I_{2,s}$, obtained by division by the Grobner basis $\mathcal{G}_{m,2}$. Denote $f_{i,j,k} = g(t)^i r^j t^k$, for $i, j \in \mathbb{N}, k < q$. Then:*

1. $\overline{f_{i,j,k}} = 0$ *for* $i \geqslant s, k < q$.

2. $\overline{f_{s-1,j,k}} = f_{s-1,j\,\overline{mod}\,(q-1),k\,\overline{mod}\,(q-1)}$.

3. $deg_t(\overline{f_{i,j,k}}) \leqslant deg_t(f_{i,j,k})$, *for* $k < q$.

Proof. By 2.26, we have that

$$\mathcal{G}_{m,2} = \left\{ g(t)^{\alpha} g(r)^{\beta} \mid \alpha + \beta = s \right\} \tag{4.5}$$

is a Grobner basis for $I_{m,s}$. In particular, we see that for $i \geqslant s$, $f_{i,j,k}$ is divisible by the basis element $g(t)^s$, and thus item 1 holds. For 2, assume $j \geqslant q$. Then:

$$\begin{aligned} f_{s-1,j,k} &= g(t)^{s-1} r^j t^k = g(t)^{s-1} r^{j-q} r^q t^k \\ &= g(t)^{s-1} r^{j-q} (g(r) + r) t^k \\ &= g(t)^{s-1} r^{j-(q-1)} t^k \bmod I_{2,s} \end{aligned}$$

A similar calculation is true for t. To prove the 3rd property, note that in general, by 4.1, we can write $f_{i,j,k} = g^i r^j t^k$, in the form

$$f_{i,j,k} = \left(\sum_{\substack{i_1,i_2 \\ i_2<q}} \alpha_{i_1,i_2} g(t)^{i_1} t^{i_2} \right) \left(\sum_{\substack{j_1,j_2 \\ j_2<q}} \beta_{j_1,j_2} g(r)^{j_1} r^{j_2} \right)$$

where

$$\begin{aligned} g^i t^k &= \sum_{\substack{i_1,i_2 \\ i_2<q}} \alpha_{i_1,i_2} g(t)^{i_1} t^{i_2} \\ r^j &= \sum_{\substack{j_1,j_2 \\ j_2<q}} \beta_{j_1,j_2} g(r)^{j_1} r^{j_2}. \end{aligned}$$

The reduced representation $\overline{f_{i,j,k}}$ can now be computed by truncating the products where $i_1 + j_2 \geqslant s$, $i_2 \geqslant q$, $j_2 \geqslant q$. From this, we see that the reduction can only reduce the local degree at t (since the part which is dependent of t in the reduced form, comes only from the part which is dependent of t in the original form). Thus, 3 holds.

□

5 *Restriction to lines is a local characterisation when* deg $< q-2$

In the proof, we will make use of the following theorem, about the characterization of the Reed-Muller code :

Theorem 5.1 ([FS95])**.** *Suppose $q \geq d+2$. $f \in RM_q(m,d)$ iff for every $a, b \in \mathbb{F}^m$ $f \circ \ell_{a,b} \in RS(1,d)$.*

For $a, b \in \mathbb{F}_q^m$ define $\phi_{(a,b)} : \Sigma_{m,s} \to \Sigma_{1,s}$ by:

$$\left(\phi_{(a,b)}(z)\right)_j = \sum_{\mathbf{i}, wt(\mathbf{i})=j} z_{\mathbf{i}} \cdot b^{\mathbf{i}}. \tag{5.1}$$

for $0 \leqslant j < s$.

Theorem 5.2. *Let $\mathbb{F}$ be a field of size q, and let m, d, s be positive integers such that $q \geqslant s$, $q^m \geqslant \binom{m+s-1}{s-1}$ and $q \geqslant d+2$. Then*

$$P \in MRM_q(m,d,s) \iff \forall a, b \in \mathbb{F}^m \quad P_{(a,b)} \in MRS(d,s).$$

where

$$P_{a,b}(t) = \phi_{a,b}(EVAL_{m,s}(P; \ell_{a,b}(t)))$$

Proof. We start with the easy direction. Assume $P \in MRM_q(m,d,s)$. Fix $a, b \in {\mathbb{F}_q}^m$ and define a univariate polynomial $Q_{a,b} \in \mathbb{F}[t]$ by $Q_{a,b}(t) = P(a+bt)$. $Q \in \mathbb{F}_q^{\leq d}[X]$. Then,

$$\begin{aligned} P_{a,b}(t) &= \phi_{a,b}(EVAL_{m,s}(P; \ell_{a,b}(t))) \\ &= \left(\sum_{\mathbf{i}, wt(\mathbf{i})=j} P^{(\mathbf{i})}(a+bt) \cdot b^{\mathbf{i}} \right)_j \\ &= \left(Q^{(j)}(t)\right)_j \in EVAL(RS(d,s)). \end{aligned}$$

where in the last equality we have used Lemma 2.11.

We now prove the other direction, i.e that every f which passes all the local tests, must be a member of $MRM(m,d,s)$. Assume that we are given as input $f \in (\Sigma_{m,s})^{q^m}$. As before let

$$f_{a,b}(t) \quad = \quad \phi_{a,b}(f(\ell_{a,b}(t))).$$

Assume for every $a,b \in \mathbb{F}^m$, $f_{a,b} \in MRS(d,s)$. This means that for every $a,b \in \mathbb{F}_q^m$ there exists a uni-variate polynomial $M_{a,b} \in \mathbb{F}_q^{\leq d}[X]$ such that $EVAL(M_{a,b}) = f_{a,b}$. We need to show the existence of a polynomial $P \in \mathbb{F}_q^{\leq d}[\mathbf{X}]$ such that $EVAL(P) = f$. We define P as follows. We let

$$P(x) \quad = \quad f_{\mathbf{0}}(x).$$

Claim 5.3. $\deg(P) \leq d$ *and* $M_{a,b} = P_{|\ell_{a,b}}$.

Proof. Fix $a,b \in \mathbb{F}^m$. Then, $P_{|\ell}(t) = P(a+bt) = f_{\mathbf{0}}(a+bt) = M_{a,b}(t)$. Thus, for every $a,b \in \mathbb{F}_q^m$, $P_{|\ell_{a,b}}$ is a degree polynomial. By Theorem 5.1, $P \in \mathbb{F}_q^{\leq d}[\mathbf{X}]$. Since $P_{|\ell_{a,b}}$ and $M_{(a,b)}$ are two univariate polynomials of degree $\leqslant d$, which agree on $q > d$ points (the whole space $\mathbb{F}_q$), they must be equal as polynomials. □

We are left to show,

Lemma 5.4. *For every* $0 \leq j < s$ *and every* $\mathbf{i}$ *with* $wt(\mathbf{i}) = j$ *we have* $P^{(\mathbf{i})} = f_{\mathbf{i}}$.

Proof. Fix $0 \leqslant j < s$. For $a,b \in \mathbb{F}^m$ let $\ell = \ell_{a,b}$ and

$$P_{|\ell}(t) = P(a+bt)$$

By Lemma 2.11

$$P_{|\ell}^{(j)}(t) = \sum_{\mathbf{i}, wt(\mathbf{i})=j} P^{(\mathbf{i})}(a+bt)b^{\mathbf{i}}$$

Also, by our assumption, $EVAL(M_{a,b}) = \phi_{a,b}(f(\ell_{a,b}(t)))$ and so

$$M_{a,b}^{(j)}(t) \quad = \quad \sum_{\mathbf{i}, wt(\mathbf{i})=j} f_{(\mathbf{i})}(a+bt)b^{\mathbf{i}}$$

As $P_{|\ell_{a,b}} = M_{a,b}$ we conclude that

$$(b^{\mathbf{i}})_{wt(\mathbf{i})=j} \cdot \left(f_{\mathbf{i}}(a+bt) - P^{(\mathbf{i})}(a+bt)\right)_{wt(\mathbf{i})=j} = 0, \tag{5.2}$$

and for every $a, b \in \mathbb{F}_q^m$ we have such an equation.

Fix $0 \leq j < s$ and $z \in \mathbb{F}_q^m$. Define a vector $Diff \in \mathbb{F}^{w(j)}$ by

$$Diff(\mathbf{i}) = f_{\mathbf{i}}(z) - P^{(\mathbf{i})}(z)$$

Define a $q^m \times w(j)$ matrix B_j by $B_j(b, \mathbf{i}) = b^{\mathbf{i}}$.

In this terminology we see that $B_j Diff = \overline{0}$.

B_j is the generating matrix of the code of degree j homogeneous polynomials over $\mathbb{F}_q^m$. As the code has positive distance by 2.3, the matrix has full rank. Thus, $B_j Diff = \overline{0}$ implies $Diff = 0$. Thus, for every z and $\mathbf{i}$ we have $f_{\mathbf{i}}(z) = P^{(\mathbf{i})}(z)$ and $f = EVAL(P)$. □

□

6 *Restriction to lines is a local characterisation for* $MRM(m, d, 2)$ *when* $\deg_{local} < q$

In this section we would like to prove that the line test stays sound for the case $s = 2$, when considering polynomials of restricted local degree, even when the total degree is greater than q. Formally :

Theorem 6.1. *Assume $d < 2q - 1$. Let $P \in \mathbb{F}[\mathbf{X}]^{loc \leqslant q-1}$ be a polynomial which passes all the tests in 5.2. Then $P \in MRM_q(m, d, 2)$.*

Given some P which passes the line tests, we can write

$$P(\mathbf{X}) \quad = \quad \sum_{I : I_i < q} \alpha_I \mathbf{X}^I. \tag{6.1}$$

Notice that while this assumption implies P is reduced modulo $I_{m,1}$, the total degree of P might be as large as $m(q-1)$, and therefore restriction to lines is *not* reduced modulo $I_{1,2}$. We nevertheless show that the line test is still a characterization. The restriction of P to the line $\ell_{\mathbf{a},\mathbf{b}}$ (where $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$) is $P_{\mathbf{a},\mathbf{b}}(t) = P(\mathbf{a}t + \mathbf{b})$. We write $P_{\mathbf{a},\mathbf{b}}(t)$ explicitly as

$$P_{\mathbf{a},\mathbf{b}}(t) \;=\; \sum_{\substack{I\\ I_i<q}} \alpha_I(\mathbf{a}t+\mathbf{b})^I = \sum_{I:I_i<q} \alpha_I \sum_{I_a+I_b=I} \binom{I}{I_a} \mathbf{a}^{I_a}\mathbf{b}^{I_b} t^{wt(I_a)}.$$

Arranging by monomials of t we write $P_{\mathbf{a},\mathbf{b}}(t) = \sum_j A_j(\mathbf{a},\mathbf{b})t^j$ where

$$A_j(\mathbf{a},\mathbf{b}) = \sum_{I:I_i<q} \alpha_I \sum_{\substack{I_a+I_b=I\\ wt(I_a)=j}} \binom{I}{I_a} \mathbf{a}^{I_a}\mathbf{b}^{I_b}. \tag{6.2}$$

Notice that $A_j(\mathbf{a},\mathbf{b})$ is reduced modolu $I_{2m,1}$. We divide the proof to two cases: in the first (simple) case we further assume $\deg(P) < 2q$, which in particular implies $P_{\mathbf{a},\mathbf{b}}$ is reduced modulo $I_{1,2}$. We then do the general case.

6.1 When $\deg(P) < 2q$

Let $\mathbf{I}_{\max}$ be a term I in Eq (6.1) of maximal weight such that $\alpha_{\mathbf{I}_{\max}} \neq 0$. Since $\mathbf{I}_{\max}$ is maximal, $d < wt(\mathbf{I}_{\max}) = \deg(P) < 2q$. The monomial $\mathbf{a}^{\mathbf{I}_{\max}}$ appears in $A_{\deg(P)}(\mathbf{a},\mathbf{b})$ and therefore $A_{\deg(P)}(\mathbf{a},\mathbf{b})$ does not vanish on ${\mathbb{F}_q}^{2m}$ (because it is a non-zero polynomial and it is reduced modulo $I_{2m,1}$). Fix $\mathbf{a},\mathbf{b} \in {\mathbb{F}_q}^m$ such that $A_{\deg(P)}(\mathbf{a},\mathbf{b}) \neq 0$. Then $P_{\mathbf{a},\mathbf{b}}(t)$ is a degree $deg(P) > d$ uni-variate polynomial (because $A_{\deg(P)}(\mathbf{a},\mathbf{b}) \neq 0$) reduced modulo $I_{1,2}$, and therefore it does not pass the line test by our criteria in Lemma 3.13. A contradiction.

6.2 The general case

As before, let $\mathbf{I}_{\max}$ be a term I in Eq (6.1) of maximal weight such that $\alpha_{\mathbf{I}_{\max}} \neq 0$. Since $\mathbf{I}_{\max}$ is maximal, $d < wt(\mathbf{I}_{\max}) = \deg(P)$. However, unlike before, it is possible that $wt(\mathbf{I}_{\max})$ is as large as $m(q-1)$ and that $P_{\mathbf{a},\mathbf{b}}(t)$ is not reduced modulo $I_{1,2}$. For $f \in \mathbb{F}_q(\mathbf{X})$ let $\overline{f} = f \bmod I_{1,2}$. Then:

$$\overline{P_{\mathbf{a},\mathbf{b}}}(t) \;=\; \sum_j A_j(\mathbf{a},\mathbf{b})\overline{t^j} \;=\; \sum_{j=0}^{2q-1} B_j(\mathbf{a},\mathbf{b})t^j \tag{6.3}$$

Fix a partition $\mathbf{I}_{\max} = {\mathbf{I}_{\max}}^a + {\mathbf{I}_{\max}}^b$, with $wt({\mathbf{I}_{\max}}^a) = 2q-1$. The monomial $\mathbf{a}^{{\mathbf{I}_{\max}}^a}\mathbf{b}^{{\mathbf{I}_{\max}}^b}$ appears in $A_{2q-1}(\mathbf{a},\mathbf{b})$ and therefore $A_{2q-1}(\mathbf{a},\mathbf{b})$ is a

non-zero polynomial. Furthermore, $\mathbf{a}^{\mathbf{I}_{\max}{}^a}\mathbf{b}^{\mathbf{I}_{\max}{}^b}$ *does not* appear in $A_{j'}(\mathbf{a},\mathbf{b})$, for any other $j' \neq j$ (because the monomial is multiplied by $t^{wt(\mathbf{I}_{\max}{}^a)} = t^{2q-1}$). Hence $B_{2q-1}(\mathbf{a},\mathbf{b})$ is non-zero (because only A_{2q-1} contributes the monomial $\mathbf{a}^{\mathbf{I}_{\max}{}^a}\mathbf{b}^{\mathbf{I}_{\max}{}^b}$, and therefore the monomial is not cancelled out, and B_{2q-1} is a non-zero polynomial) and reduced modulo $I_{1,2}$. Fix $\mathbf{a},\mathbf{b} \in \mathbb{F}_q{}^m$ such that $B_{2q-1}(\mathbf{a},\mathbf{b}) \neq 0$. Then $\overline{P_{\mathbf{a},\mathbf{b}}}(t)$ is a degree $2q-1 > d$ uni-variate polynomial reduced modulo $I_{1,2}$, and therefore it does not pass the line test. A contradiction.

7 *Restriction to lines is not a local characterisation for* $MRM(m,d,s)$ *when the field size is small*

In this section we consider the code $Mult(m,d,s,q)$ in the case where $q \leqslant d < sq$. We would like to show that in this case, the line test fails. More precisely

Theorem 7.1. *Assume $q \leqslant d < sq-1$, and assume $m \geqslant 2$. Then there exists a table $T \in \Sigma_{m,s}^q$ which passes the test in 5.2 . However, no polynomial $P \in \mathbb{F}_q[X_1,\ldots,X_m]^{\leqslant d}$ satisfies $EVAL_{m,s}(P) = T$.*

Proof. We will construct the desired table as $EVAL(Q)$ for some polynomial $Q \in \mathbb{F}[X_1,\ldots,X_m]$, with $deg(Q) = d+1 < sq$. Note that by 3.7, there cannot be a polynomial P with $deg(P) < deg(Q)$ having the same table. Thus, if such Q passes the line test (for every line), we are done. Define

$$\hat{Q} = (X_1^q - X_1)X_2 - (X_2^q - X_2)X_1 = X_1^q X_2 - X_2^q X_1$$

and $Q = X_1^{d-q} \cdot \hat{Q}$. First note that $\hat{Q}$ is a homogeneous polynomial of degree $q+1$, and thus Q is homogeneous of degree $d' = d+1$ .Note that $Q(\alpha) = 0$ for every $\alpha \in \mathbb{F}_q{}^m$ (since $Q \in I_{m,1}$). Write

$$Q = \sum_{\mathbf{i}, wt(\mathbf{i})=d'} c_{\mathbf{i}} X^{\mathbf{i}}$$

and look at the restriction

$$Q_{|\ell_{a,b}} \quad = \quad Q(a+bt) = \sum_{\mathbf{i}, wt(\mathbf{i})=d'} c_{\mathbf{i}}(a+bt)^{\mathbf{i}},$$

for $a, b \in {\mathbb{F}_q}^m$. note that the coefficient of $t^{d'}$ in $Q_{|\ell_{a,b}}$ is

$$\sum_{wt(\mathbf{i})=d'} c_{\mathbf{i}} b^{\mathbf{i}} = Q(b) = 0,$$

since Q vanishes on ${\mathbb{F}_q}^m$. Thus $deg(Q_{|\ell_{a,b}}) \leqslant d' - 1 = d$. Of course, this means that Q passes the test for the line $\ell_{a,b}$. Since this is true for every line, we are done.

□

8 *Restriction to planes is a local characterisation for* $MRM_q(m, d, 2)$ *when the field size is small*

In this section we consider the case $s = 2$. We would like to show that the multiplicity code $MRM_q(m, d, 2)$ can be characterized by restrictions to planes,even when the field size is small. In this section we assume q is prime.

Let $\mathbb{F}$ be a field of size q, and let m be a positive integer. For $\mathbf{a}, \mathbf{b} \in {\mathbb{F}_q}^m$ define:

- $\ell_{\mathbf{a},\mathbf{b},\mathbf{c}} : \mathbb{F}_q^2 \to \mathbb{F}_q^m$ by:

$$\ell_{\mathbf{a},\mathbf{b},\mathbf{c}}(t, r) \quad = \quad \mathbf{a}t + \mathbf{b}r + \mathbf{c}.$$

- $\phi_{(\mathbf{a},\mathbf{b})} : \Sigma_{m,2} \to \Sigma_{2,2}$ by:

$$\left(\phi_{(\mathbf{a},\mathbf{b})})(z)\right)_{\mathbf{j}=(j_1,j_2)} \quad = \quad \sum_{\mathbf{i}\in\mathbb{N}^m} z_{\mathbf{i}} \cdot \sum_{k=0}^{m} \sum_{\substack{S\subset[m] \\ |S|=k \\ wt(\mathbf{i}_S)=j_1, wt(\mathbf{i}_{\bar{S}})=j_2}} \mathbf{a}^{\mathbf{i}_S}\mathbf{b}^{\mathbf{i}_{\bar{S}}}.$$

From Lemma 2.12 we see that:

Theorem 8.1. *(Completeness) Suppose $q > 2$, $d < 2q - 1$. Then if a table $T \in \Sigma_{m,s}^{q^m}$ satisfies $T \in MRM_q(m, d, 2)$ then for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}^m$,*

$$\phi_{(\mathbf{a},\mathbf{b})} \circ T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}} \in MRM_q(2, d, 2).$$

The main challenge is proving the converse:

Theorem 8.2. *(Soundness) Suppose $q > 2$, $d < 2q - 1$. If a table $T \in \Sigma_{m,2}^{q^m}$ satisfies that for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}^m$, $\phi_{(\mathbf{a},\mathbf{b})} \circ T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}} \in MRM_q(2, d, 2)$ then $T \in MRM_q(m, d, 2)$.*

In this section, when saying "multidegree", we mean with respect to the total degree lexicographic order (see 2.2), unless stated otherwise. Note that every polynomial has a unique monomial of maximal multidegree (as opposed to standard total degree). We define vector space of tables which pass the test:

$$V_{m,d} = \left\{ T \in \Sigma_{m,s}^{q^m} \mid \phi_{(\mathbf{a},\mathbf{b})} \circ T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}} \in MRM_q(2, d, 2) \text{ for every } \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}^m \right\} \tag{8.1}$$

We denote by $C_{m,d} = V_{m,d} \setminus MRM_{q,d,2}$, the set of tables which cheat the test. We would like to show that $C_{m,d} = \emptyset$. Assume towards contradiction that we have some table $T \in C_{m,d}$. By 3.8, T can be realised (uniquely) as an element of the quotient space $P \in \mathbb{F}[\mathbf{X}] \Big/ I_{m,s}$.

let $g \in \mathbb{F}[X]$ be the univariate polynomial defined by $g(X) = X^q - X$, and denote for $J \in \mathbb{N}^m$, the polynomial $g_J(X) = \prod_{i=1}^m g(X_i)^{J_i}$. We use the basis $\mathcal{B}_{m,2}$ from 3.11 to write P in the form

$$P(\mathbf{X}) = \sum_{\substack{J, wt(J)<2 \\ I, I_i<q}} \alpha_{I,J} g_J(\mathbf{X}) \mathbf{X}^I \tag{8.2}$$

Since $T \in C_{m,d}$, we have $deg(P) > d$ by 3.13. This means that there must be some J and I such that $\alpha_{I,j} \neq 0$ and

$$wt(J)q + wt(I) > d \tag{8.3}$$

Note that we may assume that every I, J which for which $\alpha_{I,J} \neq 0$, satisfy

8.3. This is since the test is linear, and any degree $\leqslant d$ will have no effect on whether P passes the test or not. Moreover, we may assume there exists some J with $wt(J) = 1$, i.e, that some element of the form $g_i(X) = X_i^q - X_i$ appears in P. Otherwise, P is of local degree $< p$, and in Section 6 we showed that in this case even the line test is a good characterization. So, from now on we assume there is atleast one J with $wt(J) = 1$. Let $\mathbf{I}_{\max}$ be of maximal total degree such that $\alpha_{\mathbf{I}_{\max},\mathbf{J}_{\max}} \neq 0$ for some $\mathbf{J}_{\max}$ with $wt(\mathbf{J}_{\max}) = 1$ (and fix this $\mathbf{J}_{\max}$).

For $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}^m$ the restriction of P to the plane defined by $\mathbf{a}, \mathbf{b}, \mathbf{c}$ is $P_{\mathbf{a},\mathbf{b},\mathbf{c}}(t, r) = P(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$. By Claim 4.1 we can write $P_{\mathbf{a},\mathbf{b},\mathbf{c}}$ as

$$P_{\mathbf{a},\mathbf{b},\mathbf{c}}(t, r) = \sum_{\substack{i,j\in\mathbb{N} \\ k<q}} A_{i,j,k}(\mathbf{a}, \mathbf{b}, \mathbf{c}) g(t)^i r^j t^k$$

We view $A_{i,j,k}(\mathbf{a}, \mathbf{b}, \mathbf{c})$ as a polynomial in the variables $\mathbf{a}, \mathbf{b}, \mathbf{c}$.

Claim 8.3. *For every partition* $\mathbf{I}_{\max} = {\mathbf{I}_{\max}}^b + {\mathbf{I}_{\max}}^c$*, the monomial* $\mathbf{a}^{\mathbf{J}_{\max}} \mathbf{b}^{{\mathbf{I}_{\max}}^b} \mathbf{c}^{{\mathbf{I}_{\max}}^c}$ *appears at* $A_{1,wt({\mathbf{I}_{\max}}^b),0}$ *and does not appear at any* $A_{1,j,0}$ *for any* $j \neq wt({\mathbf{I}_{\max}}^b)$.

Intuitively, terms of $A_{1,j,0}$ come with t-degree q and $wt(\mathbf{a}) = 1$. The only way to achieve a q-ratio between the t-degree and the a-total degree, is to take a terms only from g_J part. This, essentially, forces the lemma. We now give a rigorous proof.

Proof. We expand $P_{\mathbf{a},\mathbf{b},\mathbf{c}}(t, r)$. First, $P(\mathbf{X}) = \sum_{\substack{J:wt(J)<2 \\ I:I_i<q}} \alpha_{I,J} g_J(\mathbf{X}) \mathbf{X}^I$. Thus

$$\begin{aligned}
P_{\mathbf{a},\mathbf{b},\mathbf{c}}(t, r) &= \sum_{\substack{J:wt(J)<2 \\ I:I_i<q}} \alpha_{I,J} g_J(\mathbf{a}t + \mathbf{b}r + \mathbf{c})(\mathbf{a}t + \mathbf{b}r + \mathbf{c})^I \\
&= \sum_{\substack{J:wt(J)<2 \\ I:I_i<q}} \alpha_{I,J} \cdot \prod_{i=1}^{m} (g(a_i t + b_i r + c_i))^{J_i} \cdot \Pi_{i=1}^m (a_i t + b_i r + c_i)^{I_i} \\
&= \sum_{\substack{J:wt(J)<2 \\ I:I_i<q}} \alpha_{I,J} \sum_{\substack{J_a+J_b=J \\ I_a+I_b+I_c=I}} \binom{I}{I_a I_b} \binom{J}{J_a} \mathbf{a}^{J_a+I_a} \mathbf{b}^{J_b+I_b} \mathbf{c}^{I_c} g(t)^{wt(J_a)} g(r)^{wt(J_b)} t^{wt(I_a)} r^{wt(I_b)},
\end{aligned}$$

where we have used

$$g_J(\mathbf{a}t + \mathbf{b}r + c) \;=\; \prod_{i=1}^{m}(g(a_i t + b_i r + c_i))^{J_i} = \prod_{i=1}^{m}(a_i g(t) + b_i g(r))^{J_i}.$$

By claim 4.1, every element of the form t^ℓ, can be expressed as

$$t^\ell = \sum_{i_1,i_2:i_1 q+i_2\leqslant \ell, i_2<q} \beta_{i_1,i_2} g(t)^{i_1} t^{i_2}. \tag{8.4}$$

Plugging into Eq (8.4) we get

$$P_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) = \sum_{\substack{J:wt(J)<2\\ I:I_i<q}} \alpha_{I,J} \sum_{\substack{J_a+J_b=J\\ I_a+I_b+I_c=I}} \sum_{\substack{i_1,i_2\\ i_1 q+i_2\leqslant wt(I_a)\\ i_2<q}} \beta_{i_1,i_2} \binom{I}{I_a I_b} \binom{J}{J_a} \mathbf{a}^{J_a+I_a}\mathbf{b}^{J_b+I_b}\mathbf{c}^{I_c} g(t)^{wt(J_a)+i_1} t^{i_2} Q_{J_b,I_b}$$

(8.5)

where $Q_{J_b,I_b}(r) = g(r)^{wt(J_b)} r^{wt(I_b)}$. We now have a representation as in the basis defined at claim 4.1.

We wish to see, for which choice of values $I_a, I_b, I_c, J_a, J_b, i_1, i_2$ in Eq (8.5), $\mathbf{a}^{\mathbf{J}_{\max}}\mathbf{b}^{\mathbf{I}_{\max}{}^b}\mathbf{c}^{\mathbf{I}_{\max}{}^c}$ appears as a coefficient of $A_{1,j,0}$. We must have

$$\begin{array}{rcll}
\mathbf{J}_{\max} & = & J_a + I_a & \text{By comparing the powers of } \mathbf{a}\ , \\
\mathbf{I}_{\max}{}^b & = & J_b + I_b & \text{By comparing the powers of } \mathbf{b}\ , \\
\mathbf{I}_{\max}{}^c & = & I_c & \text{By comparing the powers of } \mathbf{c}\ , \\
wt(J_a) + i_1 & = & 1 & \text{By comparing the powers of } g(t)) \\
i_2 & = & 0 & \text{By comparing the } < q \text{ power of } t
\end{array}$$

As $wt(\mathbf{J}_{\max}) = 1$ we have $wt(J_a) + wt(I_a) = 1$. Together with the fourth equation we get $wt(I_a) = i_1$. However, $wt(I_a) \geqslant i_1 q + i_2 \geq i_1 q$, and so $i_1 \geqslant i_1 q$, which implies $i_1 = 0$. Thus $wt(I_a) = 0$ and $I_a = \emptyset$. Thus $J_a = \mathbf{J}_{\max}$. However, $1 \geq wt(J) = wt(J_a) + wt(J_b) = wt(\mathbf{J}_{\max}) + wt(J_b) = 1 + wt(J_b)$. Thus $J_b = \emptyset$. From the second equation $I_b = \mathbf{I}_{\max}{}^b$. Thus the only possible solution is $J_a = \mathbf{J}_{\max}, J_b = \emptyset, I_a = \emptyset, I_b = \mathbf{I}_{\max}{}^b, I_c = \mathbf{I}_{\max}{}^c, i_1 = i_2 = 0$. This parameter setting gives the coefficient $\alpha_{\mathbf{I}_{\max},\mathbf{J}_{\max}} \cdot \binom{\mathbf{I}_{\max}}{\mathbf{I}_{\max}{}^b}$ which is non-zero, since $\mathbf{I}_{\max i} < q$ for every $1 \leq i \leq m$ (here we use the fact that q is prime). Thus, this setting is the unique solution giving the monomial

$\mathbf{a}^{\mathbf{J}_{\max}}\mathbf{b}^{\mathbf{I}_{\max}{}^b}\mathbf{c}^{\mathbf{I}_{\max}{}^c}$. Thus, it cannot cancel and the claim follows. □

Next we would like to understand $P_{\mathbf{a},\mathbf{b},\mathbf{c}} \bmod I_{2,2}$. We adopt the notation $f_{i,j,k} = g(t)^i r^j t^k$ and the notation $\overline{\text{mod}}$ from section 4, and we use the properties in claim 4.2. For $f \in \mathbb{F}_q(X_1, X_2)$ let $\overline{f} = f \bmod I_{2,2}$. Denote the expansion in the $I_{2,2}$ basis in equation 4.4 by:

$$\overline{P_{\mathbf{a},\mathbf{b},\mathbf{c}}}(t,r) = \sum_{i' \le 1, j' < 2q-i, k' < q} B_{i',j',k'}(\mathbf{a},\mathbf{b},\mathbf{c})(g(t))^{i'} r^{j'} t^{k'}$$

We have:

$$\begin{aligned}\overline{P_{\mathbf{a},\mathbf{b},\mathbf{c}}}(t,r) &= \sum_{i\in\mathbb{N}, j\in\mathbb{N}, k<q} A_{i,j,k}(\mathbf{a},\mathbf{b},\mathbf{c})\overline{f_{i,j,k}} \\ &= \sum_{i\le 1, j\in\mathbb{N}, k<q} A_{i,j,k}(\mathbf{a},\mathbf{b},\mathbf{c})\overline{f_{i,j,k}}, \end{aligned} \tag{8.6}$$

where the equality holds because it is taken modulo $I_{2,2}$. Note that j may be as large as $q + m(q-1)$.

Lemma 8.4. *For any partition* $\mathbf{I}_{\max} = \mathbf{I}_{\max}{}^b + \mathbf{I}_{\max}{}^c$, $B_{1,wt(\mathbf{I}_{\max}{}^b)\overline{mod}(q-1),0} \in \mathbb{F}[\mathbf{a},\mathbf{b},\mathbf{c}]$ *is not the zero polynomial. Moreover, the monomial* $\mathbf{a}^{\mathbf{J}_{\max}}\mathbf{b}^{\mathbf{I}_{\max}{}^a}\mathbf{c}^{\mathbf{I}_{\max}{}^b}$ *appears in it.*

Proof. We divide the expression in Eq (8.6) to:

$$\overline{P_{\mathbf{a},\mathbf{b},\mathbf{c}}}(t,r) = \sum_{j\in\mathbb{N}, k<q} A_{0,j,k}(\mathbf{a},\mathbf{b},\mathbf{c})\overline{f_{0,j,k}} + \sum_{j\in\mathbb{N}, k<q} A_{1,j,k}(\mathbf{a},\mathbf{b},\mathbf{c}) f_{1,j\,\overline{\text{mod}}\,(q-1),k}.$$

$B_{1,j,0}(\mathbf{a},\mathbf{b},\mathbf{c})$ does not get any contribution from $A_{0,j,k}$ (where $k < q$) because the power of t there is smaller than q. Similarly, $B_{1,j,0}$ gets a contribution from $\sum_{j\in\mathbb{N},k<q} A_{1,j,k}(\mathbf{a},\mathbf{b},\mathbf{c}) f_{1,j\,\overline{\text{mod}}\,(q-1),k}$ only when $k = 0$. Thus $B_{1,j,0}$ may get a contribution only from $A_{1,j',0}$ for some j'. However, by 8.3 the only term that can contribute $\mathbf{a}^{\mathbf{J}_{\max}}\mathbf{b}^{\mathbf{I}_{\max}{}^b}\mathbf{c}^{\mathbf{I}_{\max}{}^c}$ is $j' = wt(\mathbf{I}_{\max}{}^b)$. As this monomial is contributed exactly once, it is not cancelled out and $B_{1,wt(\mathbf{I}_{\max}{}^b)\,\overline{\text{mod}}\,q-1,0}$ is not the zero polynomial. □

Lemma 8.4, tells us that there $B_{1,wt(\mathbf{I}_{\max}{}^b)\overline{\mod}(q-1),0}(\mathbf{a},\mathbf{b},\mathbf{c})$ is a non-zero polynomial in $\mathbf{a},\mathbf{b},\mathbf{c}$. We will need the stronger property that $B_{1,wt(\mathbf{I}_{\max}{}^b)\overline{\mod}(q-1),0}(\mathbf{a},\mathbf{b},\mathbf{c})$ is non-zero modulo $I_{3m,1}$, i.e., has a non-zero evaluation on $\mathbb{F}_q{}^{3m}$. We prove it using the maximality of $\mathbf{I}_{\max}$ (notice that so far we have not used this maximality).

Lemma 8.5. *For every partition* $\mathbf{I}_{\max} = \mathbf{I}_{\max}{}^b + \mathbf{I}_{\max}{}^c$, *the monomial* $\mathbf{a}^{\mathbf{J}_{\max}}\mathbf{b}^{\mathbf{I}_{\max}{}^b}\mathbf{c}^{\mathbf{I}_{\max}{}^c}$ *appears at* $B_{1,wt(\mathbf{I}_{\max}{}^b)\overline{mod}(q-1),0}\mathrm{mod}\ I_{3m,1}$.

Proof. By Lemma 8.4, $B_{1,wt(\mathbf{I}_{\max}{}^b)\overline{\mod}(q-1),0}$ contains the monomial $\mathbf{a}^{\mathbf{J}_{\max}}\mathbf{b}^{\mathbf{I}_{\max}{}^b}\mathbf{c}^{\mathbf{I}_{\max}{}^c}$. We claim that $A_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r)$ in its entire (when we now look at it as a polynomial in $\mathbf{a},\mathbf{b},\mathbf{c}$), does not contain any monomial of the form $M(\mathbf{a},\mathbf{b},\mathbf{c})$, such that $M \neq M_0$ but $M = M_0 \mod I_{3m}$. Assume otherwise. Since $wt(J_0) = 1$, $J_0 = \vec{e_{j_0}}$ for some j_0. In other words $M_0 = a_j\mathbf{b}^{I_0^b}\mathbf{c}^{I_0^c}$. By 8.5, M is of the form $M = \mathbf{a}^{J_a+I_a}\mathbf{b}^{I_b+J_b}\mathbf{c}^{I_c}$, where $J = J_a + J_b$ satisfies $wt(J) < 2$, and $I = I_a + I_b$ satisfies $I_i < q$ for $i = 1,\ldots,m$. We see that the c^{I_c} part is already reduced mod I_{3m}, and thus $I_c = I_0^c$. Since $wt(J) < 2$, there are 3 possible cases

1. $J = \emptyset$.
2. There is some j_a such that $J = J_a = \vec{e_{j_a}}$.
3. There is some j_b such that $J = J_b = \vec{e_{j_b}}$.

In the first case, M is already reduced, and thus $M = M_0$, and we're done. In the second case, $(J_a)_i = 0$ for every $i \neq j$, and so a_i is reduced for $i \neq j$. Also, $J_b = \emptyset$, and thus $\mathbf{b}^{I_b}$ is reduced. The only possible non reduced element is $a_{j_a}^{1+(I_a)_{j_a}}$. However, if it is not reduced, we have

$$1 + (I_a)_{j_a} \geqslant (J_0)_{j_a} + q - 1.$$

This gives $wt(I_a) \geqslant q - 2 > 0$. Thus $wt(I) = wt(I_a) + wt(I_0^b) + wt(I_0^c) > wt(I_0)$. This contradicts the maximality of I_0, among the monomials which appear with J of weight 1. In the third case, I_a is reduced, and $(J_b)_i = 0$ for every $i \neq j_b$. Thus, b_i is reduced for every $i \neq j_b$. The only possible non reduced element is $b_{j_b}^{1+(I_b)_{j_b}}$. If it is not reduced, we have

$$1 + (I_b)_{j_b} \geqslant (J_0)_{j_b} + q - 1.$$

As before, we get $(I_b)_{j_b} \geqslant q - 2$. Let $\tilde{I}_b, \tilde{I}_0^b$ be the restrictions of I_b, I_0^b to the coordinates $j \neq j_b$ (respectively). Then we know from before that $\tilde{I}_b = \tilde{I}_0^b$. We get

$$wt(I) = 1 + wt(I_b) + wt(I_c) \geqslant q - 1 + wt(\tilde{I}_b) + wt(I_0^c) \geqslant wt(I_0).$$

By maximality of I_0 we have $I = I_0$, and thus $I_b = I_0^b$. However, since M is equivalent to M_0 , this means

$$I_b + J_b = I_b \bmod q - 1$$

(where the mod is in each coordinate). This gives $1 = (J_b)_{j_b} = 0 \bmod (q-1)$, and thus $q = 2$, which is a contradiction.

□

Lemma 8.6. *There is a partition of* $\mathbf{I}_{\max} = {\mathbf{I}_{\max}}^b + {\mathbf{I}_{\max}}^c$, *such that* $wt({\mathbf{I}_{\max}}^b)\ \overline{mod}\ (q-1) > d - q$.

Proof. If $wt(\mathbf{I}_{\max}) < q$ choose ${\mathbf{I}_{\max}}^b = \mathbf{I}_{\max}, {\mathbf{I}_{\max}}^c = \emptyset$. Then $wt({\mathbf{I}_{\max}}^b)\ \overline{\text{mod}}\ (q-1) = wt({\mathbf{I}_{\max}}^b) > d - q$ by Eq (8.3). If $j_{\max} = wt(\mathbf{I}_{\max}) \geq q$ we choose any partition $\mathbf{I}_{\max} = {\mathbf{I}_{\max}}^b + {\mathbf{I}_{\max}}^c$ with $wt({\mathbf{I}_{\max}}^b) = q - 1$ and we use the fact that $d < 2q - 1$. □

We are now ready to prove 8.2.

Proof of 8.2. by 8.6, and 8.5, we have a coefficient $B_{1,j_b,0}$ of a monomial in $\overline{A_{\mathbf{a},\mathbf{b},\mathbf{c}}}(t,r)$ of degree $> d$, which satisfies $B_{1,j_b,0} \notin I_{3m}$.We look at $EVAL_{3m,1} : \mathbb{F}[\mathbf{a},\mathbf{b},\mathbf{c}] \to q^{q^{3m}}$. It satisfies $Ker(EVAL_{3m,1}) = I_{3m}$. Thus, $EVAL_{3m,1}(B_{1,j_b,0}) \neq 0$. In other words, there are $\mathbf{a}_0, \mathbf{b}_0, \mathbf{c}_0$ such that $B_{1,j_b,0}(\mathbf{a}_0, \mathbf{b}_0, \mathbf{c}_0) \neq 0$. This means that $\overline{A_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r)}$ is of degree $> d$, and thus, by 3.13, the bivariate polynomial $P_{\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0}(t,r)$ cannot represent a table of a degree $\leqslant d$ polynomial. In other words, $EVAL_{2,s}(P_{\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0}) \notin MRM_q(2,d,s)$. By the definition of $\phi_{\mathbf{a},\mathbf{b}}$, and by 2.12, T fails the test for $(\mathbf{a},\mathbf{b},\mathbf{c})$.

□

References

[Alo99] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999.

[BS09] Simeon Ball and Oriol Serra. Punctured combinatorial nullstellensätze. *Combinatorica*, 29(5):511–522, 2009.

[CLO13] David Cox, John Little, and Donal OShea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

[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.

[Ham50] Richard W Hamming. Error detecting and error correcting codes. *The Bell system technical journal*, 29(2):147–160, 1950.

[KMRZS17] Swastik Kopparty, Or Meir, Noga Ron-Zewi, and Shubhangi Saraf. High-rate locally correctable and locally testable codes with sub-polynomial query complexity. *Journal of the ACM (JACM)*, 64(2):1–42, 2017.

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

[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.

[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.

[Sha01] Claude Elwood Shannon. A mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review*, 5(1):3–55, 2001.

תקציר

במסגרת מחקר זה, נחקרו התכונות הלוקאליות של קודים לתיקון שגיאות המבוססים על הערכה של פולינומים מרובי משתנים ונגזרותיהם. המחקר מכיל אנליזה של 2 מבחנים לוקאליים טבעיים והפרמטרים שבהם הם מהווים אפיון מלא לקודים אלה. מבחן אחד מבוסס על צמצום לישרים חד מימדיים, והשני על מישורים דו מימדיים.

אפיון מקומי של קודים לתיקון שגיאות מבוססי נגזרות

חיבור זה הוגש כעבודת מחקר לקראת התואר "מוסמך אוניברסיטה" במדעי המחשב

על ידי

רועי סלמה

העבודה נעשתה בבית הספר למדעי המחשב

בהנחיית פרופ' אמנון תא-שמע

תשפ"ב