Electronic Colloquium on Computational Complexity, Report No. 28 (2022)

The plane test is a local tester for Multiplicity Codes

Dan Karliner *[1], Roie Salama†[1], and Amnon Ta-Shma‡[1]

[1] *Department of Computer Science, Tel Aviv University, Tel Aviv, Israel.*

Abstract

Multiplicity codes are a generalization of RS and RM codes where for each evaluation point we output the evaluation of a low-degree polynomial and all of its directional derivatives up to order s. Multi-variate multiplicity codes are *locally decodable* with the natural local decoding algorithm that reads values on a random line and corrects to the closest uni-variate multiplicity code. However, it was not known whether multiplicity codes are *locally testable*, and this question has been posed since the introduction of these codes with no progress up to date. In fact, it has been also open whether multiplicity codes can be *characterized* by local constraints, i.e., if there exists a subset $\mathcal{B}$ such that c is in the code iff $c \cdot z = 0$ for any $z \in \mathcal{B}$, and, every $z \in \mathcal{B}$ has small Hamming weight, i.e., few non-zero symbols.

We begin by giving a simple example showing the line test *does not* give local characterization when $d > q$. Surprisingly, we then show the *plane test* is a *local characterization* when $s < q$ and $d < qs - 1$ for prime q. In addition, we show the k-dimensional test is a *local tester* for multiplicity codes, when $s < q$ and k is at least $\lceil \frac{d+1}{q-1} \rceil$. [1] Combining the two results, we show that the *plane test* is a local tester for multiplicity codes, with constant rejection probability for constant s.

Our technique is new. We represent the given input as a possibly very high-degree polynomial, and we show that for some choice of plane, the restriction of the polynomial to the plane is a high-degree bi-variate polynomial. The argument has to work modulo the appropriate kernels, and for that we use Grobner theory, the Combinatorial Nullstellensatz theorem and its generalization to multiplicities. Even given that, the argument is delicate and requires choosing a non-standard monomial order for the argument to work.

*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. Email: dankarliner@gmail.com.

†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. Email: roiesalama@mail.tau.ac.il.

‡The research leading to these results was supported by the Israel Science Foundation grant number 952/18. Email: amnon@tauex.tau.ac.il.

[1] For a prime power $q = p^r$ the correct bounds are $d < q(s - \frac{1}{p}) - 1$ and $\lceil \frac{d+1}{q - \frac{q}{p}} \rceil$

ISSN 1433-8092

1 Introduction

Multiplicity codes were defined in [GW13, KSY14] and are a generalization of RS and RM codes. The code $\mathrm{MRM}(q, m, d, s)$ has a codeword for each degree d m-variate polynomial p, and the codeword consists of the evaluation of p *and all of its directional derivatives up to order* s on $\mathbb{F}_q^m$. Thus, the length of the code is q^m (one coordinate per each evaluation point) and the alphabet size is $q^{\binom{m+s-1}{s-1}}$, consisting of one $\mathbb{F}_q$ value for each m-directional derivative of order up to s. Choosing $s = 1$ gives us the familiar RS code (when $m = 1$) and RM code (for general m). This work studies the *local* structure of multiplicity codes.

Let us begin with three (informal) definitions:

- A code $\mathcal{C}$ has a *local characterization* with t queries if there exists a subset $\mathcal{B}$ such that: $c \in \mathcal{C}$ iff $c \cdot z = 0$ for every $z \in \mathcal{B}$, and, every $z \in \mathcal{B}$ has Hamming weight at most t.[2]
- A code $\mathcal{C}$ is *locally correctable* with t queries if there exists a randomized algorithm A that for any string w close to a codeword $c \in \mathcal{C}$, and any coordinate i, $A(w, i) = c_i$, while making at most t queries to w.[3]
- A code $\mathcal{C}$ is *locally testable* with t queries if there exists a randomized algorithm A that given a string w, decides whether w is a codeword of $\mathcal{C}$, or far away from any codeword of $\mathcal{C}$, while making at most t queries to w. Being a bit more precise, we require that the rejection probability of the algorithm on words w that are δ far from the code is at least $\min\{\alpha\delta, c\}$, for some constants $\alpha, c > 0$, and is zero on codewords.

Local characterization is a necessary, but not sufficient, condition for local testability. In both, all codewords c pass all tests, i.e., for every $z \in \mathcal{B}$ it holds that $c \cdot z = 0$. Also, in both, any non-codeword w fails some test, i.e., for some $z \in \mathcal{B}$, $w \cdot z \neq 0$. However, in local testability there is an additional requirement that the rejection probability is linked to the distance from the code, and words far away from the code should have significant rejection probability.

While at first it seems local correctability is stronger requirement than local testability, this is not the case because local correctability only imposes conditions on the behavior of A on words close to the code $\mathcal{C}$, while local testability also imposes conditions on the behavior of A on words w that are far away from the code $\mathcal{C}$. As a result, local correctability does not imply local testability.

Before we discuss how multiplicity codes fare with these local properties, let us first survey the extensive research done on local properties of RM codes.

Over large enough fields, RM codes have a natural and simple local characterization: A multi-variate polynomial is degree d iff for every line, its restriction to the line is a univariate degree d polynomial. We call this the line test characterization. The if direction is simple, while the only-if direction is more subtle and was proved in a sequence of works [GLR+91, RS92, RS96, FS95]. Formally, when q is prime and $d < q - 1$, a multi-variate

[2] The notion of local characterization is equivalent to the notion of an LDPC code. A code $\mathcal{C}$ is *LDPC* (Low density parity check) if there exists a subset $\mathcal{B}$ of the dual code $\mathcal{C}^\perp$ such that $\mathrm{Span}(\mathcal{B}) = \mathcal{C}^\perp$ and each $z \in \mathcal{B}$ has small Hamming weight.

[3] We say $A(w, i) = b$ if $A(w, i)$ is b with probability at least $2/3$ over the internal random coins of A.

polynomial is degree d iff its restriction to all lines is a degree d polynomial. When $d = q-1$ the assertion is clearly false, as any function from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be interpolated by a degree $q-1$ polynomial. For non-prime fields $\mathbb{F}_q$ with characteristic p, it was shown that when $d < q(1-\frac{1}{p})$ the line test is a characterization, whereas for $d = q(1-\frac{1}{p})$ it is not.

The small field case also attracted a lot of attention [AKK+05, KR06, JPRZ04, BKS+10, HSS13]. When q is prime and $q \leq d+1$ the line test is not a characterization, and the next natural candidate is the *plane* test, or more generally the k-dimensional test, where one chooses a random k dimensional affine space and tests whether the restriction of the function to it agrees with a degree d polynomial. Roughly speaking, the bottom line is that characterization by (affine) subspaces happens as soon as it makes sense. For example, when $d = q-1$ characterization by lines does not make sense, because every function on the line can be explained by a degree $q-1$ polynomials, whereas not all functions over $\mathbb{F}_q^m$ can be explained by a degree $q-1$ polynomial. Similarly, if $d \geq k(q-1)$ the k-dimensional test contains no information, because every function on a k dimensional space can be explained by a degree $k(q-1)$ polynomial. Consequently, we may define two quantities:

- The *naive characterization dimension* $nc_{q,d} = \lceil \frac{d+1}{q-1} \rceil$, and,
- The *characterization dimension* $c_{q,d}$ which is the lowest k such that the k dimensional test locally characterizes $\mathrm{RM}(q,m,d)$.

By the reasoning above, clearly, $c_{q,d} \geq nc_{q,d}$. The line of work cited above shows that in fact when q is prime characterization happens as soon as it is possible, namely that $c_{q,d} = nc_{q,d}$.

When q is a prime p power, a similar phenomenon exits, but the characterization dimension should be adjusted to $c_{q,d} = \lceil \frac{d+1}{q-\frac{q}{p}} \rceil$. More precisely, the $c_{q,d}$ dimension test is a characterization, and,

Theorem 1.1. *([KR06], Theorem 4) Let d be an integer and $q = p^n$ a prime power. If $k < \left\lceil \frac{d+1}{q-q/p} \right\rceil$ there exists a function f such that:*

- *f is not a degree d polynomial, but,*
- *The restriction of f to any k dimensional subspace can be explained by a degree d polynomial.*

We now move on testing. We may define the *RM testing dimension* $t_{q,d}$ to be the lowest k such that $\mathrm{RM}(q,m,d)$ is locally testable by the k-dimensional test. Roughly speaking, [KR06, HSS13] show that $t_{q,d} = c_{q,d}$, though here we need to mention the parameters that are associated with the rejection probability of the test. Being more precise:

Theorem 1.2. *([KR06])* *Let $k = \left\lceil \frac{d+1}{q-q/p} \right\rceil$. Given $f : \mathbb{F}_q^m \to \mathbb{F}_q$ let:*

- $\mathrm{REJ}_{k,d}(f)$ *denotes the rejection probability of the test, namely, the probability over a random k dimensional affine space, that f restricted to the space cannot be explained by a degree k polynomial, and,*
- $\delta(f, \mathrm{RM}(q,m,d))$ *be the distance of f from the code* $\mathrm{RM}(q,m,d)$.

Then

$$\mathrm{REJ}_{k,d}(f) \geq \min\left\{\alpha_0 \cdot \delta(f, \mathrm{RM}(q,m,d)), c_0\right\}.$$

where $\alpha_0 = \frac{q^k}{2}$ *and* $c_0 = \frac{1}{2(k+1)q^{k+1}}$.

RM codes over large enough fields are also locally decodable with q queries [STV01]. A simple and natural local correction procedure is the following: Randomly choose a line in $\mathbb{F}_q^m$, read all the evaluations on points lying on the line, and answer according to the closest degree d univariate polynomial. Other variants exist, e.g., one may replace the line with a low-degree curve to handle larger error, but all variants use the crucial observation that the restriction of a multi-variate degree d polynomial to a line is a degree d uni-variate polynomial.

Having said all that we turn our attention back to multiplicity codes, that are a natural generalization of RM codes. Which of the local properties of RM code are preserved in multiplicity codes?

Multi-variate multiplicity codes are locally decodable [KSY14]. The local correction procedure is simple and natural: Choose a random line in $\mathbb{F}_q^m$, read all the evaluations on points lying on the line and answer according to the closest degree d univariate polynomial. For correctness, we first notice that $\mathcal{C}$ restricted to a line can be associated with a uni-variate $\mathrm{MRM}(q,1,d,s)$ code (see Lemma 2.8 for details). Also, since the points on a random line form a pairwise independent sample space, and since w is close to a codeword $c \in \mathcal{C}$, with a good probability w restricted to the line is close to c restricted on the line. Together, this implies that c is the unique codeword closest to w on the line, and the algorithm outputs (with a good probability) the correct answer c_i. Indeed, in [KMRZS17] multiplicity codes serve as a building block for the construction of the state of the art high-rate locally decodable codes.

The situation with regard to *local characterization* and *local testability* is different. The question whether multiplicity codes are locally testable is already mentioned in [Kop13], and without local characterization there is no hope for local testability. To appreciate the problem let us try to imitate the successful line of thought attacking the RM case. Given q, m, d and s what is the trivial k for which there is no hope of characterizing the $\mathrm{MRM}(q,m,d,s)$ code by dimension k affine spaces? Stated differently, given k, for what d every table on $\mathbb{F}_q^k$ giving evaluations for the function and all directional derivatives, can be explained by a degree d polynomial? We will see that the answer to that is $d = (s-1)q + k(q-1)$. This allows for degrees d that are significantly larger than q. For example, for $k = 1$ (i.e., the line test) it allows d to go up to $sq - 2$. However, as we shall see soon, for $k = 1$ even $d = q + 1$ is too large.

In this paper we study local characterization and local testing of $\mathrm{MRM}(q,m,d,s)$ codes. The starting point is a simple example that local characterization by lines is not possible (except for extreme cases). We find what comes next very surprising. We show that local characterization by *planes* works as long as $s \leq q$ and $d < sq - \frac{q}{p}$. I.e., for a very large set of parameters (containing the parameters that are often used in multiplicity codes) the MRM characterization dimension is 2, regardless of q, m and d. Given this, the next natural goal is understanding the MRM testing dimension. Our first result here is that if k is above the RM testing dimension, then k-dimensional tests give a local MRM test. Said

differently, the MRM testing dimension is no larger than the RM testing dimension. Having that it is natural to ask: Can it actually be smaller? Our second result shows that it indeed can be smaller. We show that if $d < q(s - \frac{1}{p})$ (and notice that d may get very close to qs) then the plane test is a local test (with parameters that depend on q and s). We devote the rest of the introduction to explaining our results, and discussing the new techniques developed to obtaining them. While we do not give applications of the new results, we believe our results give us new basic understandings on this important class of codes, extending the vast literature surveyed before on the corresponding question for RM codes (e.g. [AKK+05, KR06, JPRZ04, BKS+10, HSS13]).

1.1 Our results - I

1.1.1 The line test

We begin our journey by analyzing a natural candidate test for characterizing multiplicity codes: *the line test*. The line test adapts the standard, well known local testing algorithm for RM and checks whether a restriction to a line is a uni-variate $\mathrm{MRM}(q, 1, d, s)$ code. Specifically:

- We are given as input an evaluation table $T : \mathbb{F}_q^m \to \Sigma_{m,s}$ where for every point $x \in \mathbb{F}_q^m$ and every directional derivative I of order up to s, we get a value in $\mathbb{F}_q$ and therefore $\Sigma_{m,s}$ is vector of $\binom{m+s-1}{s-1}$ values from $\mathbb{F}_q$, one value per each directional derivative.
- The test chooses a random line, i.e., we choose $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^m$ uniformly at random and we define $\ell_{a,b} : \mathbb{F}_q \to \mathbb{F}_q^m$ by $\ell_{a,b}(t) = t \cdot \mathbf{a} + \mathbf{b}$.
- We then query the table T at the q points of $\mathbb{F}_q^m$ that lie on the line $\ell_{a,b}$, and we learn the function $T_{\mathbf{a},\mathbf{b}} : \mathbb{F}_q \to \Sigma_{m,s}$ defined by $T \circ \ell_{a,b}$.

Informally, we want to test whether $T_{\mathbf{a},\mathbf{b}}$ is the evaluation table of some degree $\leq d$ uni-variate polynomial and its derivatives up to order s. Formally, we should first apply a transformation $\phi_{\mathbf{a},\mathbf{b}}$ that converts multi-variate derivatives to uni-variate derivatives over the line (see Lemma 2.8). With this transformation at hand we test whether $\phi_{\mathbf{a},\mathbf{b}} \circ T \circ \ell_{\mathbf{a},\mathbf{b}}$ is a codeword of $\mathrm{MRM}(q, 1, d, s)$.

It is straight forward to check completeness, i.e., that the restriction to a line of an m-variate multiplicity codeword is indeed a uni-variate multiplicity codeword, and therefore an m-variate codeword passes all tests. However, it turns out soundness sometimes fails:

Theorem 1.3. *(informal) Fix a prime power $q = p^r$, m and $s \leq d$. Let $\mathcal{C} = \mathrm{MRM}(q, m, d, s)$.*

- *When $q \leqslant d$ the line test is* NOT *a local characterization for $\mathcal{C}$.*
- *When $q - \frac{q}{p} \geqslant d + 1$ the line test is a local characterization for $\mathcal{C}$.*

Formal statements appear in Theorem 4.1 and Corollary 5.3.

The first item states that the line test fails when $q \leq d$. To see that let us look at an example. Set $Q(x, y) = (x^q - x)y - x(y^q - y) = x^q y - xy^q$. Q is a degree $q + 1$ homogeneous polynomial that vanishes on $\mathbb{F}_q^m$. When we restrict to the line $\ell_{\mathbf{a},\mathbf{b}}$ we get the polynomial

$$Q \circ \ell_{\mathbf{a},\mathbf{b}}(t) = Q(\mathbf{a}t + \mathbf{b}) = Q(a_1 t + b_1, a_2 t + b_2),$$

which is a degree q polynomial rather then a degree $q+1$ polynomial, because the coefficient of t^{q+1} is $Q(a_1, a_2) = 0$ because Q vanishes on $\mathbb{F}_q^2$. It therefore follows that the restriction of Q to lines behaves as a degree q polynomial, whereas Q itself is not degree q and the line test wrongly accepts Q.

We now turn to the second item. In the terminology of this paper, the case of $s = 1$ and $q \geq d+2$ was proved in [FS95] and we generalize the $q \geq d+2$ case to larger s. The second item is a special case of a more general claim, that we discuss next.

1.1.2 The k-dimensional test

We next consider the k-dimensional test, that tests whether the restriction to k-dimensional affine spaces reduces the the m-variate multiplicity code to a k-variate multiplicity code. More formally, we are given as input a table $T : \mathbb{F}_q^m \to \Sigma_{2,s}$. We choose $\mathbf{h} = (\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_k)$ with each $\mathbf{h}_i$ uniformly at random from $\mathbb{F}_q^m$ conditioned on $\mathbf{h}_1, \ldots, \mathbf{h}_k$ being independent and define the k-dimensional affine space $\ell_{\mathbf{h}} : \mathbb{F}_q \to \mathbb{F}_q^m$ by

$$\ell_{\mathbf{h}}(y_1, \ldots, y_k) = \mathbf{h}_0 + \sum_{i=1}^{k} y_i \mathbf{h}_i.$$

We check whether the restriction $T \circ \ell_{\mathbf{h}}$ is a k-dimensional multiplicity code, when applying the appropriate conversion $\phi_{\mathbf{h}}$ (see Lemma 2.10), i.e., we check whether $\phi_{\mathbf{h}} \circ T \circ \ell_{\mathbf{h}} : \mathbb{F}_q^k \to \Sigma_{k,s}$ is a codeword of $\mathrm{MRM}(q, k, d, s)$. As before completeness is easy, and the big question is whether soundness holds. In Section 5 we prove:

Theorem 1.4. *Let $\mathbb{F}_q$ be a field of size q, 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*

$$\mathrm{REJ}_{k,d}^{\mathrm{RM}}(f) \geq \min\left\{\alpha \cdot \delta(f, \mathrm{RM}(q, m, d)), c_0\right\}. \tag{1.1}$$

Then, for every T we have

$$\mathrm{REJ}_{k,d}^{\mathrm{MRM}}(T) \geq \min\left\{\alpha' \cdot \delta(T, \mathrm{MRM}(q, m, d, s)), c_0\right\} \tag{1.2}$$

for

$$\alpha' = \frac{q-(s-1)}{q} \frac{1}{1 + q^{d/(q-1)\frac{1}{\alpha}}} \tag{1.3}$$

We have used $\mathrm{REJ}_{k,d}^{\mathrm{RM}}(f)$ to denote the rejection probability of the RM k-dimensional test on f, and $\mathrm{REJ}_{k,d}^{\mathrm{MRM}}(T)$ to denote the rejection probability of the MRM k-dimensional test on T.

A consequence of the theorem is that if k is above the RM testing dimension, then, automatically, the k dimensional MRM test gives local testing for MRM codes. For example, if q is prime and $d < 2(q-1)$, the RM testing dimension is 2 and by Theorem 1.2 the plane test satisfies Equation (1.1) with $\alpha = \frac{q^2}{2}$ and $c_0 = \frac{1}{6q^3}$. Hence, by the theorem, the plane test is a local testing procedure for $\mathrm{MRM}(q, m, d, s)$, for any $s < q$, with $\alpha' \geq \frac{1}{3q}$ in

Equation (1.2), as $d/(q-1) < 2$. If $s \leq \frac{q}{2}$ we have $\alpha' \geq \frac{1}{6}$. In essence this means that if k is above the Reed Muller testing dimension, then the k-dimensional test is also a local testing algorithm for $\mathrm{MRM}(q, m, d, s)$ for any s as large as $q-1$, and if, say, $s < q/2$ we even get constant α'. Generally, if $d < k(q-1)$, the k-dimensional test is a local testing procedure for $\mathrm{MRM}(q, m, d, s)$ for s up to $q-1$. Item 2 in the previous subsection is the special case of this theorem when we pick $k = 1$ (i.e., we consider the line test) and we replace the testing property with the weaker characterization property.

The proof idea is as follows. Let us first consider characterization. When k is above the testing dimension, the evaluation of the function itself that are given in the input T, without the evaluations of the derivatives that are given in T, suffice to uniquely characterize the function. More precisely, if all the line tests pass the MRM test, then in particular the restriction of the function to all lines is a degree d polynomial. Then, by Theorem 1.2 the function itself is a degree d polynomial (because k is above the testing dimension). Let us call this polynomial P. This polynomial is the only possible candidate for a MRM explanation of the given input. What remains to show is that the given values of the derivatives in the input T are consistent with the derivatives of the global function P. To explain the problem, notice that every successful dimension k test gives us information about k-variate derivatives in P and T, while we need to claim about m-variate derivatives in P and T. The crux of the solution is the fact that the k-variate derivatives in a point are a *linear* combination of the m-variate derivatives at the point. We then show that the set of linear equations form a good code. Thus, if a point $x \in \mathbb{F}_q^m$ is good in the sense that many of the tests passing through it are good, then we get a codeword with many zeroes in it, and when the number of zeroes is larger than the distance then it must be the zero codeword, which implies the m-variate derivatives given in P and T coincide. A similar (but technically more complicated) approach proves the local testing version, giving the theorem.

The theorem is satisfying in that it gives a local testing procedure for multiplicity codes. However, a natural question arises: Claim 3.5 shows every table $T : \mathbb{F}_q^k \to \Sigma_{k,s}$ can be explained by a degree $(s-1)q + k(q-1)$ polynomial P (meaning that $\mathrm{EVAL}(P) = T$). Thus, if our strategy is to use the k-dimensional test to restrict a $\mathrm{MRM}(q, m, d, s)$ code to a $\mathrm{MRM}(q, k, d, s)$ code, then this approach breaks down when $d \geq (s-1)q + k(q-1)$. Thus, we can define the *naive MRM characterization dimension* to be $\lceil \frac{d+1-(s-1)q}{q-1} \rceil$, which is the minimal k needed for this approach to have chances to work. We have seen that the $\lceil \frac{d+1}{q-q/p} \rceil$-dimensional test is a local testing procedure for $\mathrm{MRM}(q, d, m, s)$, but considering the naive bound we must consider whether this is, perhaps, a gross overkill. After all, as far as the naive bound is concerned even the line test might have worked. True, we have already seen that the line test does not give a characterization. Yet, is it possible that the plane test already gives a characterization, or, perhaps, even a local test?

1.1.3 The plane test

So next we analyse the *plane* test, that tests whether the restriction to two-dimensional planes reduces the the m-variate multiplicity code to a two-dimensional multiplicity code. More formally, we are given as input a table $T : \mathbb{F}_q^m \to \Sigma_{2,s}$. We choose $\mathbf{a}, \mathbf{b}, \mathbf{c}$ uniformly at random from $\mathbb{F}_q^m$ conditioned on $\mathbf{a}, \mathbf{b}$ being linearly independent and define the plane $\ell_{\mathbf{a},\mathbf{b},\mathbf{c}} : \mathbb{F}_q \to \mathbb{F}_q^m$ by $\ell_{\mathbf{a},\mathbf{b},\mathbf{c}}(t, r) = t \cdot \mathbf{a} + r \cdot \mathbf{b} + \mathbf{c}$. We check whether the restriction $T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}}$ is a two-dimensional

multiplicity code, when applying the appropriate conversion $\phi_{\mathbf{a},\mathbf{b},\mathbf{c}}$ (see Lemma 2.9), i.e., we check whether $\phi_{\mathbf{a},\mathbf{b},\mathbf{c}} \circ T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}} : \mathbb{F}_q^2 \to \Sigma_{2,s}$ is a codeword of $\mathrm{MRM}(q,2,d,s)$. As before completeness is easy, and the big question is whether soundness holds. Our main result is the surprising:

Theorem 1.5. *(The plane test - informal) Fix q, m, d, s such that q is a power of the prime p and $s \leq q$. Suppose $d < (s - \frac{1}{p})q$. Let $\mathcal{C} = \mathrm{MRM}(q,m,d,s)$. Then, the plane test is a local characterization for $\mathcal{C}$.*

See Section 6 for a formal statement. We mention that we do not know if the condition $s \leq q$ is redundant or not. We devote the next part of the introduction for an informal explanation of our approach and technique for proving the theorem.

1.2 A warm-up proof for RM codes

As a warm-up towards the proof we first prove the line test is a characterization for RM codes (i.e., when $s = 1$) and q is prime. This claim is well known. It appears as a well known claim in Rubinfeld Sudan [RS96] but only for the case $q \geq 2d+1$. In [FS95] another proof is given that holds for all fields $\mathbb{F}_q$ of characteristic p, as long as $(1 - \frac{1}{p})q \geq d+1$. In particular, when q is prime, the proof works for all $q \geq d+2$. As mentioned above, [FS95] also show the bound is tight, i.e., that if d is such that $d+1 > (1-\frac{1}{p})q$, then the line test is not a characterization. Here, when q is prime we give yet another proof of the claim that is somewhat simpler than the one in [FS95] and will be easier to generalize to larger s. Other proofs exist, see, e.g., [JPRZ04, Section 1.4].

The starting point is the same as in [FS95]. Suppose $T : \mathbb{F}_q^m \to \mathbb{F}_q$ is some function. There exists a polynomial $P : \mathbb{F}_q^m \to \mathbb{F}_q$ in $\mathbb{F}_q[X_1, \ldots, X_m]$ that agrees with T on $\mathbb{F}_q^m$. The polynomial P is not unique, but it is unique modulo $\mathcal{I}_{m,1}$ which is the ideal of all polynomials in $\mathbb{F}_q[X_1, \ldots, X_m]$ that vanish on $\mathbb{F}_q^m$. If we choose P to be the polynomial of minimal degree agreeing with T, then from the Combinatorial Nullstellensatz (see Theorem 2.20) we see that we can represent P as

$$P(x_1, \ldots, x_m) = \sum_{0 \leq i_1, \ldots, i_m < q} \alpha_{i_1,\ldots,i_m} x_1^{i_1} \ldots x_m^{i_m}.$$

For ease of notation let us denote $\mathbf{I} = (i_1, \ldots, i_m)$ and $\mathbf{X}^{\mathbf{I}} = x_1^{i_1} \ldots x_m^{i_m}$. Before we go on notice that while the individual degree of P in each of the m variables is smaller than q, the total degree of P,$\deg(P)$, may be as large as $m(q-1)$ and in particular much larger than q.

When we restrict P to the line $\ell_{\mathbf{a},\mathbf{b}}(t)$ we see that:

$$P_{\mathbf{a},\mathbf{b}}(t) \stackrel{\text{def}}{=} P \circ \ell_{\mathbf{a},\mathbf{b}}(t) \; = P(\mathbf{a}t + \mathbf{b}) \; = \sum_{\mathbf{I}} \alpha_{\mathbf{I}} (\mathbf{a}t + \mathbf{b})^{\mathbf{I}}$$

and we can express

$$P_{\mathbf{a},\mathbf{b}}(t) \; = \sum_{k=0}^{\deg(P)} A_k(\mathbf{a},\mathbf{b}) t^k,$$

where $A_k \in \mathbb{F}_q[a_1, \ldots, a_m, b_1, \ldots, b_m]$.

At first it seems our task is to show that if $\deg(P) > d$, then $A_{\deg(P)}(\mathbf{a}, \mathbf{b})$ is non-zero, and therefore for some $\mathbf{a}, \mathbf{b} \in {\mathbb{F}_q}^m$we have $P_{\deg(P)}(\mathbf{a}, \mathbf{b}) \neq 0$. Then, when we test the line $\ell_{\mathbf{a},\mathbf{b}}$, the restricted function $P \circ \ell_{\mathbf{a},\mathbf{b}}$ is a degree $\deg(P) > d$ uni-variate polynomial, and therefore fails the line test. This argument is, however, flawed in two essential points:

1. First, we should look not at $P_{\mathbf{a},\mathbf{b}}$ but rather at $P_{\mathbf{a},\mathbf{b}}$ mod $\mathcal{I}_{1,1}$, i.e., modulo the ideal of functions that vanish on $\mathbb{F}_q$. This is because from our point of view a table can be associated with a degree d polynomial iff there exists a degree d polynomial with such an evaluation table, and two polynomials that differ by an element from $\mathcal{I}_{1,1}$ have the same valuation table. The ideal $\mathcal{I}_{1,1}$ is generated by $g(t) = t^q - t$ and so we need to look at $P_{\mathbf{a},\mathbf{b}}(t)$ mod $(t^q - t)$.

2. It is not enough to show that A_k is non-zero in $\mathbb{F}_q[a_1, \ldots, a_m, b_1, \ldots, b_m]$ but rather that A_k has a non-zero evaluation point in $\mathbb{F}_q^{2m}$. By the Combinatorial Nullstellensatz this is equivalent to A_k mod $\mathcal{I}_{2m,1}$ being non-zero.

The way we fix these two issues is different than [FS95]. We say $\mathbf{I}$ is a *maximal monomial* of P if $\deg(\mathbf{X}^{\mathbf{I}}) = \deg(P)$. We say $(\mathbf{I}_0, \mathbf{I}_1)$ is a *partition* of $\mathbf{I}$ if $\mathbf{I}_0 + \mathbf{I}_1 = \mathbf{I}$ and $\mathbf{I}_0, \mathbf{I}_1 \geq 0$, where $\mathbf{I}_0, \mathbf{I}_1 \in \mathbb{Z}^m$ and the addition and inequality are in each of the m coordinates. We also let $w(\mathbf{I})$, the *weight* of $\mathbf{I}$, be $\sum_{j=1}^{m} i_j$. We claim:

Lemma 1.6. *Assume q is prime. Let $\mathbf{I}$ be a monomial of P of weight at least $d+1$ and $\mathbf{I}_0, \mathbf{I}_1$ a partition of $\mathbf{I}$ with $w(\mathbf{I}_0) = d+1$. Then $A_{d+1}(\mathbf{a}, \mathbf{b})$ is a non-zero polynomial in $\mathbb{F}_q[a_1, \ldots, b_m]$ and furthermore $\mathbf{a}^{\mathbf{I}_0}\mathbf{b}^{\mathbf{I}_1}$ appears in it as a non-zero monomial.*

To see why the lemma is true first notice that the coefficient of $\mathbf{a}^{\mathbf{I}_0}\mathbf{b}^{\mathbf{I}_1}$ in $(\mathbf{a}t + \mathbf{b})^{\mathbf{I}}$ is $\binom{\mathbf{I}}{\mathbf{I}_0}$ which is non-zero if q is prime (see Section 2.1 for the notation $\binom{\mathbf{I}}{\mathbf{I}_0}$)[4] and it appears as a coefficient of $t^{w(\mathbf{I}_0)}$ mod $(t^q - t) = t^{d+1}$ mod $(t^q - t) = t^{d+1}$. In general, other terms may contribute to the coefficient of t^{d+1}, and we should make sure none of these terms cancel the monomial $\mathbf{a}^{\mathbf{I}_0}\mathbf{b}^{\mathbf{I}_1}$. For this, we notice that from $\mathbf{a}^{\mathbf{I}_0}\mathbf{b}^{\mathbf{I}_1}$ we can recover $\mathbf{I}_0, \mathbf{I}_1$, and therefore $\mathbf{I} = \mathbf{I}_0 + \mathbf{I}_1$. Hence, for all $\mathbf{J} \neq \mathbf{I}$, $\mathbf{a}^{\mathbf{I}_0}\mathbf{b}^{\mathbf{I}_1}$ is not obtained in $(\mathbf{a}t + \mathbf{b})^{\mathbf{J}}$. Thus, there is a *unique* way to obtain $\mathbf{a}^{\mathbf{I}_0}\mathbf{b}^{\mathbf{I}_1}$, and it appears with a non-zero coefficient and therefore $A_{d+1}(\mathbf{a}, \mathbf{b})$ has the monomial $\mathbf{a}^{\mathbf{I}_0}\mathbf{b}^{\mathbf{I}_1}$ with a non-zero coefficient, and the lemma follows.

For the second issue we notice that for every k, $A_k(\mathbf{a}, \mathbf{b})$ is a polynomial in $\mathbb{F}_q[a_1, \ldots, b_m]$ with individual degree at most $q-1$, and therefore it is already reduced modulo $\mathcal{I}_{m,1}$. We can therefore conclude that for some $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^m$ the polynomial $P_{\mathbf{a},\mathbf{b}}(t)$ mod $(t^q - t)$ is a non-zero polynomial of degree at least $d+1$, and therefore the line test fails for this choice of $\mathbf{a}, \mathbf{b}$.

1.3 The general case

We now want to explore whether we can generalize the argument to show the plane test is a characterization for $s > 1$. Suppose we are given a table T of function and derivative evaluations, $T : \mathbb{F}_q^m \to \Sigma_{m,s}$. Every table T has some (possibly high degree) polynomial P such that

[4] One can give an analogous argument for a prime power q, and we indeed do that for later on, but we skip it here because this is just a warm-up exercise.

T is the codeword of P. The functions whose table is identically zero are those polynomials that vanish on $\mathbb{F}_q^m$ with multiplicity s. Let $\mathcal{I}_{m,s}$ denote the set of m-variate polynomials that vanish on $\mathbb{F}_q^m$ with multiplicity s. $\mathcal{I}_{m,s}$ is an ideal of the ring $\mathbb{F}_q[X_1,\ldots,X_m]$. $\mathcal{I}_{1,1}$ is the ideal of all uni-variate functions that vanish on $\mathbb{F}_q$, and is generated by $g(x)=\Pi_{\alpha\in\mathbb{F}_q}(x-\alpha)=x^q-x$. Similarly, $\mathcal{I}_{1,s}$ is generated by $g(x)^s$ (and $\mathcal{I}_{1,s}=\mathcal{I}_{1,1}^s$). From the combinatorial nullstellensatz [Alo99] one can deduce that $\mathcal{I}_{m,1}$ is generated by $\{g(x_1),\ldots,g(x_m)\}$ and a further generalization [BS09] shows that $\mathcal{I}_{m,s}=\mathcal{I}_{m,1}^s$ and is therefore generated by

$$\mathcal{G}_{m,s}=\left\{g(\mathbf{X})^{\mathbf{I}}\mid w(\mathbf{I})=s\right\},$$

where we use the notation $g(\mathbf{X})^{\mathbf{I}}=g(x_1)^{i_1}\cdot\ldots\cdot g(x_m)^{i_m}$. It turns out that $\mathcal{G}_{m,s}$ is a Grobner basis for $\mathcal{I}_{m,s}$ (see Section 2.3). This implies that a basis for $\mathbb{F}_q[X_1,\ldots,X_m]$ mod $\mathcal{I}_{m,s}$ (as a vector space) is

$$\mathcal{B}_{m,s}=\left\{g(\mathbf{X})^{\mathbf{I}}\cdot\mathbf{X}^{\mathbf{J}}\mid(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}\right\}.$$

Where $(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}$ iff $w(\mathbf{I})<s$ and $j_1,\ldots,j_m<q$. Notice that there are basis elements in $\mathcal{B}_{m,s}$ whose degree is as large as $m(q-1)+(s-1)q\gg sq$. For more details see Section 3.

We will occasionally abuse notation and refer to members of $\mathcal{B}_{m,s}$ as "monomials".

Going back to the plane test, we are given a table $T:\mathbb{F}_q^m\to\Sigma_{m,s}$ and we want to check whether the polynomial P that represents T is a degree d polynomial or not. W.l.o.g., we can assume P is reduced modulo $\mathcal{I}_{m,s}$ and we express $P(X_1,\ldots,X_m)\in\mathbb{F}_q[X_1,\ldots,X_m]$ mod $\mathcal{I}_{m,s}$ in the basis $\mathcal{B}_{m,s}$:

$$P(\mathbf{X})=\sum_{(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}}\alpha_{\mathbf{I},\mathbf{J}}\cdot g(\mathbf{X})^{\mathbf{I}}\mathbf{X}^{\mathbf{J}}.$$

We let $P_{\mathbf{a},\mathbf{b},\mathbf{c}}$ be P restricted to the plane $\ell_{\mathbf{a},\mathbf{b},\mathbf{c}}$, i.e., $P_{\mathbf{a},\mathbf{b},\mathbf{c}}\stackrel{\text{def}}{=}P\circ\ell_{\mathbf{a},\mathbf{b},\mathbf{c}}\in\mathbb{F}_q[t,r]$. We want to check whether $P_{\mathbf{a},\mathbf{b},\mathbf{c}}$ belongs to $\mathrm{MRM}(q,2,d,s)$ and we therefore take $P_{\mathbf{a},\mathbf{b},\mathbf{c}}$ modulo $\mathcal{I}_{2,s}$. We express

$$P_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r)\bmod\mathcal{I}_{2,s}=\sum_{i+j<s,k,\ell<q}A_{i,j,k,\ell}(\mathbf{a},\mathbf{b},\mathbf{c})\cdot g(t)^i g(r)^j t^k r^\ell$$

Our plan is to show that if P has degree larger than d, then for some $\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0\in\mathbb{F}_q^m$ it must be that $P_{\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0}(t,r)$ mod $\mathcal{I}_{2,s}$ is a polynomial of degree larger than d, and therefore the test $\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0$ fails. Equivalently, we want to show that for some i_0,j_0,k_0,ℓ_0 with $i_0+j_0<s$ and $k_0,\ell_0<q$ it holds that:

- $A_{i_0,j_0,k_0,\ell_0}(\mathbf{a},\mathbf{b},\mathbf{c})$ mod $\mathcal{I}_{3m,1}$ is non-zero, and therefore for some $\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0\in\mathbb{F}_q^m$ we have $A_{i_0,j_0,k_0,\ell_0}(\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0)\neq 0$ and the monomial $g(t)^{i_0}g(r)^{j_0}t^{k_0}r^{\ell_0}$ survives, and,
- $q\cdot(i_0+j_0)+k_0+\ell_0>d$ and therefore $\deg(P_{\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0})>d$.

The crux of the proof is finding an order on monomials under which the following lemma is true:

Lemma 1.7. *If* $(\mathbf{I}_{\max}, \mathbf{J}_{\max})$ *is such that* $g(\mathbf{X})^{\mathbf{I}_{\max}} X^{\mathbf{J}_{\max}}$ *is a maximal monomial in* P *in the monomial order, then for any partition of* $\mathbf{J}_{\max}$ *to* $\mathbf{J}^b_{\max}+\mathbf{J}^c_{\max}$ *such that* $q \cdot w(\mathbf{I}_{\max})+w(\mathbf{J}^b_{\max}) < qs$ *and* $\binom{\mathbf{J}_{\max}}{\mathbf{J}^b_{\max}} \neq 0 \bmod p$*, the monomial* $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ *appears with a non-zero coefficient at*

$$A_{w(\mathbf{I}_{\max}),\lfloor \frac{w(\mathbf{J}^b_{\max})}{q} \rfloor, 0, w(\mathbf{J}^b_{\max}) \bmod q}(\mathbf{a}, \mathbf{b}, \mathbf{c}) \bmod \mathcal{I}_{3m,1}.$$

See Lemma 6.3 for a formal statement. There is no requirement for this order to be a monomial ordering in the sense usually used for Grobner bases. The proof is much more delicate than the one we presented before for the RM case (where $s = 1$) and we give some essential ideas below. We omit some of the technical details, and, as a result, we do not see, e.g., why in the proof we also need the assumption $q \geq s$. The full proof appears in Section 6.

$P_{\mathbf{a},\mathbf{b},\mathbf{c}}(t, r) = p(\mathbf{a}t + \mathbf{b}r + bc)$ is a polynomial in $a_1, \ldots, a_m, b_1, \ldots, b_m, c_1, \ldots, c_m$, t and r. We first note that (recalling that $g(x) = x^q - x$)

$$g(at + br + c) = (at + br + c)^q - (at + br + c) = ag(t) + bg(r),$$

and so $g(at+br+c)$ behaves as a total degree q polynomial in t, r, and as a *linear* polynomial in $\mathbf{a} = a_1, \ldots, a_m$ and $\mathbf{b} = b_1, \ldots, b_m$. In particular $g(\mathbf{X})^{\mathbf{I}}\mathbf{X}^{\mathbf{J}}(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$ has total degree $w(\mathbf{I}) + w(\mathbf{J})$ in $\mathbf{a}, \mathbf{b}$, where by $P(\mathbf{X})(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$ we mean $P(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$.

One crucial difference between the $s = 1$ and $s > 1$ case is that now we may get monomials $\mathbf{a}^{\mathbf{I}_1}\mathbf{b}^{\mathbf{I}_2}\mathbf{c}^{\mathbf{I}_3}$ that are *not* reduced modulo $\mathcal{I}_{3m}$, e.g., $a_1^q = a_1$ is a monomial that appears in $g(X_1)X_1^{q-1}(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$. In general, if for some coordinate $j \in [m]$ we have $\mathbf{I}_j + \mathbf{J}_j \geq q$, we get (among other things) a monomial in $\mathbf{a}, \mathbf{b}, \mathbf{c}$ that gets reduced. This complicates things for us, because a monomial that has more then one "source" may cancel out.

To solve this problem we do two things:

- First, we choose a monomial order that first order monomials $g(\mathbf{X})^{\mathbf{I}}\mathbf{X}^{\mathbf{J}}$ by $w(\mathbf{I})+w(\mathbf{J})$, and then orders monomials by $w(\mathbf{I})$.
- Second, we focus on special monomials in $\mathbf{a}, \mathbf{b}, \mathbf{c}$ and degrees of t, r. We fix $(\mathbf{I}_{\max}, \mathbf{J}_{\max})$ with maximal $w(\mathbf{I}_{\max})+w(\mathbf{J}_{\max})$ in P, and we take some partition $\mathbf{J}^b_{\max}+\mathbf{J}^c_{\max}$ of $\mathbf{J}_{\max}$. We look at the monomial $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$.

We observe that the monomial $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ (which is reduced modulo $\mathcal{I}_{3m,1}$) is always obtained in a reduced $\mathcal{I}_{3m,1}$ form, i.e., it cannot appear as a reduction from $g(\mathbf{X})^{\mathbf{I}}\mathbf{X}^{\mathbf{J}}$ for some $(\mathbf{I}, \mathbf{J}) \neq (\mathbf{I}_{\max}, \mathbf{J}_{\max})$. This is because it has maximal $w(\mathbf{I}_{\max}) + w(\mathbf{J}_{\max})$ weight, and if it was to appear as reduction from $(\mathbf{I}, \mathbf{J})$, then those $(\mathbf{I}, \mathbf{J})$ would have a higher $w(\mathbf{I}) + w(\mathbf{J})$ weight.

The monomial $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ is obtained from $g(\mathbf{X})^{\mathbf{I}_{\max}}\mathbf{X}^{\mathbf{J}_{\max}}(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$ as a coefficient of $t^{qw(\mathbf{I}_{\max})}r^{w(\mathbf{J}^b_{\max})}$. We claim that this is the only way to obtain $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ as a coefficient of $t^{qw(\mathbf{I}_{\max})}r^{w(\mathbf{J}^b_{\max})}$. To see that suppose $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ is obtained as a coefficient of $t^{qw(\mathbf{I}_{\max})}r^{w(\mathbf{J}^b_{\max})}$ from some $g(\mathbf{X})^{\mathbf{I}}\mathbf{X}^{\mathbf{J}}(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$. Since the degree in t is $qw(\mathbf{I}_{\max})$, i.e., q times the total degree in $\mathbf{a}$, it must be that the $\mathbf{a}$ part is obtained from $g(\mathbf{X})^{\mathbf{I}}(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$, because only the g part behaves as a linear function in $a \in \mathbb{F}_q$ and a degree q polynomial in t. Furthermore $w(\mathbf{I}) \geq w(\mathbf{I}_{\max})$. Since $(\mathbf{I}_{\max}, \mathbf{J}_{\max})$ is maximal and monomials that have the

maximal $w(\mathbf{I}) + w(\mathbf{J})$ are then ordered by $w(\mathbf{I})$, we must have $w(\mathbf{I}) = w(\mathbf{I}_{\max})$. From that it is easy to conclude that $(\mathbf{I}, \mathbf{J}) = (\mathbf{I}_{\max}, \mathbf{J}_{\max})$.

Next, we need to force the monomial in t, r to have degree $d+1$ when taken modulo $\mathcal{I}_{2,s}$. We take advantage of the fact that our claims work for any partition of a maximal monomial, and therefore we can shift weight from $\mathbf{c}$ to $\mathbf{b}$ in the partition of the maximal monomial. Each time we shift weight one from $\mathbf{c}$ to $\mathbf{b}$ we change the degree in t, r by one, and this is true even when working modulo $\mathcal{I}_{2,s}$. If the degree of P is larger than d, then there is a way to put just the right weight on $\mathbf{b}$ such that the resulting polynomial in t, r is degree at least $d+1$ even when taken modulo $\mathcal{I}_{2,s}$. In fact, one can calculate explicitly how the weight should be partitioned (see Lemma 6.4). This concludes the proof of Lemma 1.7.

Having the lemma, there exist some $\mathbf{a}_0, \mathbf{b}_0, \mathbf{c}_0 \in \mathbb{F}_q^{3m}$ such that P restricted to the plane $\mathbf{a}_0 t + \mathbf{b}_0 r + \mathbf{c}_0$ is degree larger than d, even after doing the reduction modulo $\mathcal{I}_{2,s}$, because the corresponding coefficient polynomial in $\mathbf{a}, \mathbf{b}, \mathbf{c}$ is non-zero modulo $\mathcal{I}_{3m,1}$. Hence the test $\mathbf{a}_0, \mathbf{b}_0, \mathbf{c}_0$ fails!

1.4 Our results - II

We have seen two results so far:

- The k-dimensional test, for k above the RM testing dimension gives a MRM local tester, and,
- The planes test gives a MRM local characterization,

where for both results we assume $s < q$. We now combine the two results to show that the plane test gives a MRM local tester, with constant parameters when s is constant. We prove:

Theorem 1.8. *Suppose q is a prime power, $s \leq q$ and $d < q(s - \frac{1}{p})$. Let $T : \mathbb{F}_q^m \to \Sigma_{m,s}$ be a table and let $\delta = \delta(T, \mathrm{MRM}(q, m, d, s))$. Then*

$$\mathrm{REJ}_{2,d}^{\mathrm{MRM}}(T) \geq \min\{\alpha\delta, c\}$$

with $\alpha = \Omega(q^{-6s+5})$ and $c = \Omega(q^{-8s+4})$.

The proof idea is follows. Suppose T is far from $\mathrm{MRM}(q, m, d, s)$. By the first result mentioned above, a random k dimensional affine space H (for k above the RM testing dimension) cannot be explained a $\mathrm{MRM}(q, k, d, s)$ polynomial. Then, by the second result, some plane in H cannot be explained by a $\mathrm{MRM}(q, 2, d, s)$ polynomial. Hence, that plane rejects. The number of planes in k dimensional space is about q^{3k}, and so, intuitively, the rejection probability should be about q^{-3s} times the rejection probability of the k-dimensional test, which we already saw is quite good. We give the details in Section 7.

1.5 Organization and open problems

In Section 2 we introduce notation, recall multiplicity codes and some basic results about ideals in polynomial rings (Grobner theory and combinatorial nullstellensatz). 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 nullstellensatz [Alo99] and a generalization of the combinatorial nullstellensatz for multiplicities higher than one [BS09]. In Section 4 we prove the line test is not a characterization when $d > q + 1$. In Section 5 we prove the k-dimensional test is a MRM local tester when k is above the RM testing dimension. In Section 6 we prove the plane test is a local characterization of the MRM code, and in Section 7 we combine the two results to show the plane test is a local tester for MRM codes.

Finally, we state some open problems:

- A self-evident open problem that arises from our work is whether the parameters of the plane test in Section 7 can be made better.
- Another intriguing question is whether the condition $s \leq q$ is necessary or not. We remark that in the usual setting of the parameters $q \gg s$. Nevertheless, we think it is interesting to know whether the condition is required, and this is likely to improve our understanding of the code.
- In Theorem 4.1 we show that for $d \geq q+1$ the line test is not a local characterization for $\mathrm{MRM}(q, m, d, s)$ for any $s > 1$. When $s > 1$ and $d < q(1 - \frac{1}{p})$ it follows from Section 5 that the line test is a local characterization. An open problem is pinning down where in the range $q(1 - \frac{1}{p}) \leq d < q + 1$ the line test stops being a local characterization.
- Similarly, in Claim 3.5 we show that the plane test has no hope of being a local characterization for $\mathrm{MRM}(q, m, d, s)$ when $d \geq q(s-1) + 2(q-1) = qs + q - 2$. When $d < q(s - \frac{1}{p})$ Theorem 6.2 tells us that the plane test is a local characterization. The same question can be asked about where in the range $q(s - \frac{1}{p}) \leq d < qs + q - 2$ the plane test stops being a local characterization.
- Another natural open problem, pointed to us by Tali Kaufman, is understanding the $d \gg (s - \frac{1}{p})q$ case. As we mentioned before, For RM codes (where $s = 1$) the problem attracted a lot of attention, see, e.g., [AKK+05, KR06, JPRZ04, BKS+10, HSS13] and it is natural to ask what happens to multiplicity codes over such small fields.

1.6 Acknowledgements

We would like to thank Tali Kaufman and Noga Ron-Zewi for a stimulating discussion on the paper. In particular, we thank them for suggesting to utilize the approach for giving a new analysis of the RM characterization.

2 Preliminaries

2.1 Notation

We denote vectors by bold letters. 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 individual degree at most d , and by $\mathbb{F}[\mathbf{X}]^{loc \leqslant d}$ the set of polynomials of individual degree

at most d (i.e degree in each variable). Given a vector $\mathbf{I} = (i_1, \ldots, i_m) \in \mathbb{N}^m$, we use the notation

$$\mathbf{X}^{\mathbf{I}} \stackrel{\text{def}}{=} \prod_{k=1}^{m} X_k^{i_k}.$$

For a vector $\mathbf{I} \in \mathbb{N}^m$, and a set $S \subseteq [m]$, 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 multinomial coefficients for natural numbers:

$$\binom{a}{b} \stackrel{\text{def}}{=} \frac{a!}{b!(a-b)!}$$
$$\binom{a}{b_1, \ldots, b_\ell} = \frac{a!}{b_1! \cdots b_\ell!}$$

where $\sum b_i = a$. We extend this definition to $I, I_1, J, J_1, \ldots, J_\ell \in \mathbb{N}^m$ where $J = J_1 + \ldots + J_\ell$ by

$$\binom{I}{I_1} \stackrel{\text{def}}{=} \prod_{k=1}^{m} \binom{I_k}{(I_1)_k}$$
$$\binom{J}{J_1, \ldots, J_\ell} \stackrel{\text{def}}{=} \prod_{k=1}^{m} \binom{J_k}{(J_1)_k, \cdots, (J_\ell)_k}.$$

We mention Lucas theorem, that if p is prime, $q = p^w$ for $w \in \mathbb{N}$, and $a, b \in \mathbb{N}$ have base p representation $a = \sum_{\ell=0}^{w} a_\ell p^\ell$, $b = \sum_{\ell=0}^{w} b_\ell p^\ell$ with $0 \leq a_\ell, b_\ell < p$, then

$$\binom{a}{b} \bmod p = \Pi_{\ell=0}^{w} \binom{a_\ell}{b_\ell}, \tag{2.1}$$

where we use the convention that $\binom{c}{d} = 0$ when $d > c$. Thus, $\binom{a}{b} \bmod p \neq 0$ iff $a_\ell \geq b_\ell$ for all $\ell = 0, \ldots, w-1$.

Finally, we let $g \in \mathbb{F}_q[X]$ denote the polynomial $g(X) = X^q - X$. For $\mathbf{X} = (X_1, \ldots, X_m)$ and $\mathbf{I} = (i_1, \ldots, i_m) \in \mathbb{N}^m$ we let $g(\mathbf{X})^{\mathbf{I}}$ denote $\Pi_{k=1}^{m} (g(X_k))^{i_k}$.

2.2 Reed Muller and Multiplicity codes

Definition 2.1. *Let d, m be non-negative integers, 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 $\mathbb{F}_q^m$, namely,*

$$RM(q, m, d) = \left\{ (f(\alpha))_{\alpha \in \mathbb{F}_q^m} \mid f \in \mathbb{F}_q[\mathbf{X}]^{\leqslant d} \right\}.$$

We will make use of the following lemma:

Lemma 2.2. *[HSS13, Lemma 3.2] Let $\delta^{\mathrm{RM}}_{q,m,d}$ be the relative distance of the code $\mathrm{RM}(q,m,d)$. Then $\delta^{\mathrm{RM}}_{q,m,d} \geq q^{-d/(q-1)}$.*

Definition 2.3. *(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 $P^{(\mathbf{I})}(\mathbf{X})$, 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 $\lambda \in \mathbb{F}$, $(\lambda P)^{(\mathbf{I})}(\mathbf{X}) = \lambda P^{(\mathbf{I})}(\mathbf{X})$ and $P^{(\mathbf{I})}(\mathbf{X}) + Q^{(\mathbf{I})}(\mathbf{X}) = (P+Q)^{(\mathbf{I})}(\mathbf{X})$. The product rule shows $(PQ)^{(\mathbf{I})}(\mathbf{X}) = \sum_{\mathbf{I}_0+\mathbf{I}_1=\mathbf{I}} P^{(\mathbf{I}_0)}(\mathbf{X}) \cdot Q^{\mathbf{I}_1}(\mathbf{X})$.

Definition 2.4 (Weight)**.** *If $\mathbf{I} = (i_1, \ldots, i_m) \in \mathbb{N}^m$ then $w(\mathbf{I}) = \sum_{j=1}^m i_j$.*

Definition 2.5 (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 $mult(P, \mathbf{a})$, is the largest integer s such that for every non-negative vector $\mathbf{I}$ with $w(\mathbf{I}) < s$ we have $P^{(\mathbf{I})}(\mathbf{a}) = 0$. If s 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 2.6. *[DKSS13] Let $P \in \mathbb{F}[\mathbf{X}]$ be a non-zero polynomial of total degree at most d. Then for any finite $A \subseteq \mathbb{F}$,*

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

Definition 2.7 (Multiplicity code)**.** *Let $m, d \geq s$ be non-negative integers, and let q be a prime power. Let*

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

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

We also let $\mathrm{MRS}(q, d, s) \coloneqq Mult(q, 1, d, s)$ stand for Reed-Solomon multiplicity code.

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

Lemma 2.8. *[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 $PL_{\mathbf{a},\mathbf{b}}(t) = P(\mathbf{a}t + \mathbf{b})$. Then*

$$PL^{(j)}_{\mathbf{a},\mathbf{b}}(t) = \sum_{\mathbf{I}: w(\mathbf{I}) = j} P^{(\mathbf{I})}(\mathbf{a}t + \mathbf{b}) \cdot \mathbf{a}^{\mathbf{I}}.$$

We also derive a formula for the derivative of a restriction to a two dimensional plane.

Lemma 2.9. *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 $PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) = P(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$. Then for $(j_1, j_2) \in \mathbb{N}^2$:*

$$PP^{(j_1,j_2)}_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) = \sum_{\mathbf{I}\in\mathbb{N}^m} P^{(\mathbf{I})}(\mathbf{a}t + \mathbf{b}r + \mathbf{c}) \cdot \sum_{\substack{\mathbf{I}_1+\mathbf{I}_2=\mathbf{I} \\ w(\mathbf{I}_1)=j_1, w(\mathbf{I}_2)=j_2}} \binom{\mathbf{I}}{\mathbf{I}_1} \mathbf{a}^{\mathbf{I}_1}\mathbf{b}^{\mathbf{I}_2}.$$

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. On the one hand,

$$\begin{aligned} P(\mathbf{a}(t + R_1) + \mathbf{b}(r + R_2) + \mathbf{c}) &= PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t + R_1, r + R_2) = PP_{\mathbf{a},\mathbf{b},\mathbf{c}}((t,r) + (R_1, R_2)) \\ &= \sum_{j_1,j_2\in\mathbb{N}} PP^{(j_1,j_2)}_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) R_1^{j_1} R_2^{j_2}. \end{aligned}$$

On the other hand,

$$\begin{aligned} P(\mathbf{a}(t + R_1) + \mathbf{b}(r + R_2) + \mathbf{c}) &= P(\mathbf{a}t + \mathbf{b}r + c + R_1\mathbf{a} + R_2\mathbf{b}) \\ &= \sum_{\mathbf{I}\in\mathbb{N}^m} P^{(\mathbf{I})}(\mathbf{a}t + \mathbf{b}r + c) \cdot (R_1\mathbf{a} + R_2\mathbf{b})^{\mathbf{I}} \\ &= \sum_{\mathbf{I}\in\mathbb{N}^m} P^{(\mathbf{I})}(\mathbf{a}t + \mathbf{b}r + c) \cdot \prod_{k=1}^{m} (a_k R_1 + b_k R_2)^{i_k} \\ &= \sum_{\mathbf{I}\in\mathbb{N}^m} P^{(\mathbf{I})}(\mathbf{a}t + \mathbf{b}r + c) \cdot \sum_{\substack{\mathbf{I}_1+\mathbf{I}_2=\mathbf{I} \\ w(\mathbf{I}_1)=j_1, w(\mathbf{I}_2)=j_2}} \binom{\mathbf{I}}{\mathbf{I}_1} \mathbf{a}^{\mathbf{I}_1}\mathbf{b}^{\mathbf{I}_2} R_1^{j_1} R_2^{j_2}. \end{aligned}$$

Comparing coefficients of $R_1^{j_1} R_2^{j_2}$ for every $\mathbf{J} = (j_1, j_2) \in \mathbb{N}^2$ we get the result. □

We will also be interested in the restrictions of polynomials to general k-dimensional subspaces. Let $PP_{\mathbf{h}_0,\mathbf{h}_1,\ldots,\mathbf{h}_k}(\mathbf{Y}) = P(\mathbf{h}_0 + \sum_{i=1}^{k} \mathbf{h}_i Y_i)$. Then, similarly to Lemma 2.9,

Lemma 2.10.

$$PP^{\mathbf{J}}_{\mathbf{h}_0,\mathbf{h}_1,\ldots,\mathbf{h}_k}(\mathbf{Y}) = \sum_{\mathbf{I}\in\mathbb{N}^m} P^{(\mathbf{I})}(\mathbf{h}_0 + \sum_{i=1}^{k} \mathbf{h}_i Y_i) \cdot \sum_{\substack{\mathbf{I}_1+\cdots+\mathbf{I}_k=\mathbf{I} \\ w(\mathbf{I}_r)=j_r}} \binom{\mathbf{I}}{\mathbf{I}_1, \ldots, \mathbf{I}_k} \prod_{i=1}^{k} \mathbf{h}_k^{\mathbf{I}_k}.$$

The proof is identical to the proof of Lemma 2.9.

2.3 Grobner bases and Nullstellensatz

The theory of Grobner bases describes the structure of ideals in the ring $R = \mathbb{F}[\mathbf{X}]$ and we briefly explain some of the essential concepts of this theory. We refer to [CLO13] for a thorough treatment of this theory.

Definition 2.11. *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 $w(\alpha) = \sum \alpha_i > w(\beta) = \sum \beta_i$ or, $w(\alpha) = w(\beta)$ and $\alpha \succ_{lex} \beta$.*

Definition 2.12. *Let $f(\mathbf{X}) = \sum_{\mathbf{I}} a_{\mathbf{I}} \mathbf{X}^{\mathbf{I}}$ and $\succ$ a monomial order.*

1. *The multi-degree of f is $multideg(f) = \max\{\mathbf{I} \mid a_{\mathbf{I}} \neq 0\}$ where the 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 $LT(f) = LC(f) \cdot LM(f)$.*

Definition 2.13 (Multivariate polynomial division)**.** *Let $\succ$ be a monomial order on $\mathbb{Z}^m_{\geqslant 0}$, and let $F = \{f_1, \ldots, f_k\}$ be a set of k polynomials in $\mathbb{F}[\mathbf{X}]$. Then every $f \in \mathbb{F}[\mathbf{X}]$ can be written as*

$$f = q_1 f_1 + \cdots + q_k f_k + r,$$

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 $LT(f_1), \ldots, LT(f_k)$. We call r a remainder of the division by F. Moreover, $multideg(q_i f_i) \leqslant multideg(f)$ for every $i \in [s]$. The remainder r is not necessarily unique, and might depend on the order of division.

Definition 2.14. *Let $\{0\} \neq I \subseteq \mathbb{F}[\mathbf{X}]$ 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 in I.*

$$LT(I) = \{LT(f) \mid f \in I \setminus \{0\}\}$$

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

Definition 2.15. *Let $\{0\} \neq I \subseteq \mathbb{F}[\mathbf{X}]$ be an ideal. Fix a monomial order 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 has a Grobner basis.*

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

Theorem 2.16. *[CLO13, Section 2, Proposition 1] Let $I \subset \mathbb{F}[X_1, \ldots, X_m]$ be an ideal and $G = \{g_1, \ldots, g_k\}$ a Grobner basis. Then given $f \in \mathbb{F}[\mathbf{X}]$ there is a **unique** $r \in \mathbb{F}[\mathbf{X}]$ such that there is a $g \in I$ such that $f = g + r$ and no term of r is divisible by any of $LT(g_1), \ldots, LT(g_k)$. 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, the theorem gives us a natural way of choosing representatives modulo I.

Theorem 2.17. *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*

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

is a basis for R / I .

The following criterion determines whether G is a Grobner basis.

Definition 2.18 (LCM and S polynomials)**.** *Let $f, g \in \mathbb{F}[\mathbf{X}]$ be non-zero polynomials. Let $\alpha = multideg(f)$ and $\beta = multideg(g)$.*

1. *The least common multiple of $LM(f)$ and $LM(g)$, denoted $LCM(LM(f), LM(g))$, 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*

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

Theorem 2.19. *(Buchberger's Criterion) [CLO13, Sec 6] Let $I \subset \mathbb{F}[\mathbf{X}]$ be an ideal. Then a basis $G = \{g_1, \ldots, g_k\}$ of I is a Grobner basis of I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero .*

Note that we always have $S = S(g_i, g_j) \in I$ by the definition of S. When saying the remainder 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 2.13).

Theorem 2.20. *(Combinatorial 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

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

Also, let $\mathcal{I}_m$ denote the ideal $\mathcal{I}_m = \left\{ f \in \mathbb{F}_q[\mathbf{X}] \mid \forall \alpha \in \mathbb{F}_q^m \;\; f(\alpha) = 0 \right\}$.

Corollary 2.21. $\mathcal{I}_m = \langle g(X_1), \ldots, g(X_m) \rangle$.

Proof. Let $f \in \mathcal{I}_m$. By Theorem 2.20, taking $S_i = \mathbb{F}_q$ for every i, we get that $f = \sum h_i g_i$ for some $\{h_i\}$ and so $f \in \langle g_k \rangle_{k \in [m]}$. The other inclusion is trivial since $g(X_i) = X_i^q - X_i$ vanishes on $\mathbb{F}_q^m$ for every i. □

Using Theorem 2.19 it can be easily proved that:

Claim 2.22. *$G = \{g(X_k)\}_{k=1}^m$ is a Grobner basis for $\mathcal{I}_m$ relative to the total degree lexicographic order.*

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

$$\mathcal{I}_{m,s} = \{ f \in \mathbb{F}_q[\mathbf{X}] \mid \forall \alpha \in {\mathbb{F}_q}^m \;\; Mult(f; \alpha) \geq s \}.$$

In this notation, $\mathcal{I}_{m,1} = \mathcal{I}_m$ defined before. For every $\mathbf{I} = (I_1, \ldots, I_m) \in \mathbb{N}^m$ define

$$g(\mathbf{X})^{\mathbf{I}} = \prod_{k=1}^{m} g(X_k)^{I_k}.$$

Theorem 2.23. *(Combinatorial Nullstellensatz with multiplicity) [BS09, Sec 3] $\mathcal{I}_{m,s} = \langle g(\mathbf{X})^{\mathbf{I}} \rangle_{w(\mathbf{I})=s}$. Furthermore, the set $\mathcal{G}_{m,s} = \left\{ g(\mathbf{X})^{\mathbf{I}} \right\}_{w(\mathbf{I})=s}$ is a Grobner basis for $\mathcal{I}_{m,s}$.*

Proof. To see that $\mathcal{I}_{m,s}$ is indeed an ideal, fix $f \in \mathcal{I}_{m,s}$ and $h \in \mathbb{F}[\mathbf{X}]$. Then for $r < s$: $(hf)^{(r)} = \sum_{i=0}^{r} f^{(i)} \cdot h^{(r-i)} = 0$ and so $hf \in \mathcal{I}_{m,s}$. Also, clearly, $g(\mathbf{X})^{\mathbf{I}} \in \mathcal{I}_{m,s}$ for every $\mathbf{I}$ with $w(\mathbf{I}) = s$. We need to show $\mathcal{G}_{m,s}$ is a Grobner basis for $\mathcal{I}_{m,s}$,

[BS09, Section 3] show $\mathcal{G}_{m,s}$ generates $\mathcal{I}_{m,s}$ and, furthermore, $f = \sum_{\mathbf{b}: w(\mathbf{I})=s} g(\mathbf{X})^{\mathbf{I}} h_{\mathbf{I}}$ for some $h_{\mathbf{I}}$ with $deg(h_{\mathbf{I}}) \leqslant deg(f) - s \deg(g)$. In particular, this is true for the S polynomials in Theorem 2.19. I.e, every such S polynomial can be expressed as $S = \sum g(\mathbf{X})^{\mathbf{I}} h_{\mathbf{I}}$ where $deg(g(\mathbf{X})^{\mathbf{I}} h_{\mathbf{I}}) \leqslant deg(S)$. By Buchberger's criterion $\left\{ g(\mathbf{X})^{\mathbf{I}} \right\}$ is a Grobner basis. □

Finally, we look at equality modulo $\mathcal{I}_{m,1}$.

Definition 2.24. *For $n_1, n_2 \in \mathbb{N}$ we say $n_1 =_{\mathbb{F}_q} n_2$ iff $x^{n_1} = x^{n_2} \bmod \mathcal{I}_{1,1}$. Equivalently, $n_1 =_{\mathbb{F}_q} n_2$ iff*

- *$n_1 = n_2$, or,*
- *$\min(n_1, n_2) > 0$ and $n_1 = n_2 \bmod (q-1)$.*

Definition 2.25. *Let $A, B \in \mathbb{N}^m$. We say $A =_{\mathbb{F}_q} B$ for iff $A_k =_{\mathbb{F}_q} B_k$ for every $1 \leq k \leq m$.*

We also record:

Claim 2.26. *Let $a, b \in \mathbb{N}$. If $a =_{\mathbb{F}_q} b$ and $a < q$ then $a \leq b$.*

Proof. If $b < q$ then $a =_{\mathbb{F}_q} b$ implies $a = b$. Otherwise $a < q \leq b$. □

3 Polynomials and tables

A *table* is an element of $\Sigma_{m,s}^{q^m}$, i.e., a function mapping every evaluation point in $\mathbb{F}_q^m$ to an element in $\Sigma_{m,s}$. EVAL takes a multi-variate polynomial and returns its table of evaluations. More precisely,

Definition 3.1. *We define* $\mathrm{EVAL}_{m,s} : \mathbb{F}_q[\mathbf{X}] \times \mathbb{F}_q^m \to \Sigma_{m,s}$ *by*

$$\mathrm{EVAL}_{m,s}(P; \mathbf{a}) = \left(P^{(\mathbf{I})}(a)\right)_{w(\mathbf{I})<s}.$$

Similarly, we define $\mathrm{EVAL}_{m,s} : \mathbb{F}_q[\mathbf{X}] \to (\Sigma_{m,s})^{q^m}$ *by*

$$\mathrm{EVAL}_{m,s}(P) = \left(\mathrm{EVAL}(P; \mathbf{a})\right)_{\mathbf{a}\in\mathbb{F}_q^m}.$$

We say $T \in (\Sigma_{m,s})^{q^m}$ *is the* table *of* $P \in \mathbb{F}_q[\mathbf{X}]$ *if* $\mathrm{EVAL}(P) = T$.

An element in $\Sigma_{m,s}$ contains information about all the derivatives of order up to s. Sometimes we would like to focus on a certain directional derivative. If $\sigma \in \Sigma_{m,s}$ and $\mathbf{I} \in \mathbb{N}^m$ with $w(\mathbf{I}) < s$, then $\sigma_{(\mathbf{I})} \in \mathbb{F}_q$ is the entry of σ that encodes the $\mathbf{I}$'th derivative. Similarly, if $f \in \Sigma_{m,s}^{q^m}$ is a table, i.e., $f : \mathbb{F}_q^m \to \Sigma_{m,s}$, then $f_{(\mathbf{I})} : \mathbb{F}_q^m \to \mathbb{F}_q$ is defined by letting $f_{(\mathbf{I})}(x)$ be the $\mathbf{I}$'th entry of $f(x) \in \Sigma_{m,s}$.

Note that every polynomial determines its table $\mathrm{EVAL}(P)$. However, two different polynomials might have the same table if their difference is the zero table on $\mathbb{F}_q^m$. From Theorem 2.23,

$$\mathrm{Ker}(\mathrm{EVAL}_{m,s}) = \mathcal{I}_{m,s} \;=\; \langle g(\mathbf{X})^{\mathbf{I}} \rangle_{w(\mathbf{I})=s}.$$

Since $\mathcal{I}_{m,s}$ does not contain any non-zero polynomial of total degree less than sq, we conclude that:

Corollary 3.2. $\mathrm{EVAL}_{m,s}$ *is injective on polynomials of total degree less than* sq.

Claim 3.3. $\mathrm{EVAL}_{m,s}$ *is onto* $\Sigma_{m,s}^{q^m}$.

Proof. We will show that

$$\dim\left(\mathbb{F}_q[X_1,\ldots,X_m] \Big/ \mathcal{I}_{m,s}\right) \geq \dim\left((\Sigma_{m,s})^{q^m}\right) = q^m \cdot \binom{m+s-1}{m},$$

where the dimension is over $\mathbb{F}_q$. This implies that the image of $\mathrm{EVAL}_{m,s}$ is everything, and the mapping is injective.

To see that consider the set

$$\mathcal{B}_{m,s} = \left\{ g(\mathbf{X})^{\mathbf{I}} \cdot \prod_{k=1}^{m} X_k^{j_k} \mid w(\mathbf{I}) < s, 0 \leqslant j_k < q \right\}. \tag{3.1}$$

The elements in $\mathcal{B}_{m,s}$ have different multi degree and therefore are independent. Also elements in $\mathcal{B}_{m,s}$ are monomials of degree smaller than sq, and therefore are $\mathcal{I}_{m,s}$ reduced. Thus,

$$\begin{aligned}\dim\left(\mathbb{F}_q[\mathbf{X}]\Big/\mathcal{I}_{m,s}\right) &\geq \dim\ \mathrm{Span}(\mathcal{B}_{m,s})\\ &= \mid \{(\mathbf{I},\mathbf{J}) \in \mathbb{N}^m \times \mathbb{N}^m \mid w(\mathbf{I}) < s, 0 \leqslant j_k < q\} \mid \\ &= \binom{m+s-1}{m} \cdot q^m,\end{aligned}$$

as desired. □

Corollary 3.4. *The set $\mathcal{B}_{m,s}$ is a basis for $\mathbb{F}[\mathbf{X}]\Big/\mathcal{I}_{m,s}$.*

Example 3.1. *When $m = 1$ the set $\{g(x)^i x^j \mid i \in \mathbb{N}, j < q\}$ is a basis of $\mathbb{F}[\mathbf{X}]$. Thus, for every $\ell \in \mathbb{N}$ there are $\beta_{\ell,i,j}$ such that*

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

By comparing coefficients of x^ℓ we see that $\beta_{\ell,\lfloor \frac{\ell}{q} \rfloor,\ell \bmod q} = 1$.

Claim 3.5. *For every table $T : {\mathbb{F}_q}^m \to \Sigma_{m,s}$ there exists a degree $q(s-1)+(q-1)m$ polynomial such that $\mathrm{EVAL}(P) = T$.*

Proof. By Claim 3.3, T may be written as $\mathrm{EVAL}(P)$, where P is an $\mathbb{F}_q$-combination of basis elements in $\mathcal{B}_{m,s}$. By the definition of $\mathcal{B}_{m,s}$, any basis element is of the form $g(\mathbf{X})^{\mathbf{I}} \cdot \prod_{k=1}^m X_k^{j_k}$ where $w(\mathbf{I}) < s$ and $0 \leqslant j_k < q$. As such, $\deg(P) \leq \deg(g(X)^{\mathbf{I}}) + \deg(\prod_{k=1}^m X_k^{j_k}) \leq q(s-1)+(q-1)m$. □

We will later need:

Lemma 3.6. *Let $A \in \mathbb{F}_q[t]$ and $B \in \mathbb{F}_q[r]$. Then,*

$$\deg_t(A(t)B(r) \bmod \mathcal{I}_{2,s}) \leq \deg_t(A).$$

Proof. Express A in the basis $\{g(t)^i t^j\}_{i \in \mathbb{N}, j<q}$,

$$A(t) = \sum_{(i,j)\in\mathcal{A}} \alpha_{i,j} g(t)^i t^j,$$

and similarly for B,

$$B(r) = \sum_{(k,\ell)\in\mathcal{B}} \beta_{k,\ell} g(r)^k r^\ell,$$

for some sets $\mathcal{A}, \mathcal{B}$, $\alpha_{i,j}, \beta_{k,\ell} \in \mathbb{F}_q$. Then,

$$A(t)B(r) \mod \mathcal{I}_{2,s} = \sum_{(i,j)\in\mathcal{A},(k,\ell)\in\mathcal{B}: i+k<s} \alpha_{i,j}\beta_{k,\ell} g(t)^i g(r)^k t^j r^\ell.$$

Suppose $\deg_t(A(t)B(r) \bmod \mathcal{I}_{2,s})$ is achieved on the monomial of $(i,j) \in \mathcal{A}, (k,\ell) \in \mathcal{B}$. In particular, this degree in t is already achieved in A for the monomial (i,j). Thus, $\deg_t(AB) \leq \deg_t(A)$. □

Next, we would like to give a purely algebraic criteria, which states when exactly a table belongs to the code $\mathrm{MRM}(q, m, d, s)$.

Definition 3.7. *Let $T \in \Sigma_{m,s}^{q^m}$ be a table. By Corollary 3.2 and Claim 3.3 there is a unique element $P_T \in \mathbb{F}[\mathbf{X}] \Big/ \mathcal{I}_{m,s}$ such that $\mathrm{EVAL}_{m,s}(P_T) = T$. We call P_T the* representing polynomial *of T.*

Lemma 3.8. *Assume $d < sq$. Let $T \in \Sigma_{m,s}^{q^m}$ be a table, and P_T its representing polynomial. Then*

$$T \in \mathrm{MRM}(q, m, d, s) \iff deg(P_T) \leqslant d.$$

Proof. First, assume $deg(P_T) \leqslant d$. Then, by definition, since $\mathrm{EVAL}_{m,s}(P_T) = T$, we have $T \in \mathrm{MRM}(q, m, d, s)$. For the other direction, assume $T \in \mathrm{MRM}(q, m, d, s)$. Then there is some $Q \in \mathbb{F}[\mathbf{X}]$ of total degree $\leqslant d$ such that $\mathrm{EVAL}_{m,s}(Q) = T$. As $\deg(Q) \leq d < sq$, Q is $\mathcal{I}_{m,s}$ reduced and by Corollary 3.2 Q is the representing polynomial of T. □

To understand the low-dimensional tests on tables, we need to define the restriction of tables to subspaces. If T is a table $T : \mathbb{F}_q^m \to \Sigma_{m,s}$ and we want to restrict to the plane $\mathbf{a}t + \mathbf{b}r + c$ the restriction $T_{\mathbf{a},\mathbf{b},\mathbf{c}}$ should be a table $\mathbb{F}_q^2 \to \Sigma_{2,s}$. To this end we define the alphabet reduction map $\phi_{(\mathbf{a},\mathbf{b})} : \Sigma_{m,s} \to \Sigma_{2,s}$ by

Definition 3.9.

$$\left(\phi_{(\mathbf{a},\mathbf{b})}(z)\right)_{\mathbf{J}=(j_1,j_2)} = \sum_{\mathbf{I}\in\mathbb{N}^m} z_{\mathbf{I}} \cdot \sum_{\substack{\mathbf{I}_1+\mathbf{I}_2=\mathbf{I} \\ w(\mathbf{I}_1)=j_1, w(\mathbf{I}_2)=j_2}} \binom{\mathbf{I}}{\mathbf{I}_1} \mathbf{a}^{\mathbf{I}_1}\mathbf{b}^{\mathbf{I}_2}$$

This map applies the "chain rule" to an element in $\Sigma_{m,s}$, in accordance with Lemma 2.9. We may then define

$$T_{\mathbf{a},\mathbf{b},\mathbf{c}} = \phi_{(\mathbf{a},\mathbf{b})} \circ T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}}$$

.

Similarly, for $\mathbf{h} = (\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_k)$ we define $\phi_{\mathbf{h}}$ and $T_{\mathbf{h}}$ by:

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

$$T_{\mathbf{h}}(\mathbf{Y}) = \phi_{(\mathbf{h})} \circ T(\mathbf{h}_0 + \sum_{i=1}^{k} Y_i \mathbf{h}_i)$$

4 The line test is not a characterization when $d \geq q$

We now show that when the field size is smaller than the degree d, the line test fails.

Theorem 4.1. *Assume q is a prime power, $q \leqslant d < sq - 1$ and $m \geqslant 2$. There exists a table $T \in \Sigma_{m,s}^{q}$ which passes all the tests of the line test, but there is no polynomial $P \in \mathbb{F}_q[X_1, \ldots, X_m]^{\leqslant d}$ that satisfies $\mathrm{EVAL}_{m,s}(P) = T$.*

Proof. Define

$$\begin{aligned} Q &= X_1^{d-q} \cdot (g(X_1)X_2 - g(X_2)X_1) \\ &= X_1^{d-q} \cdot (X_1^q X_2 - X_2^q X_1). \end{aligned}$$

Note that Q is homogeneous of degree $d+1$. Fix $\mathbf{a}, \mathbf{b} \in {\mathbb{F}_q}^m$ and let $QL_{\mathbf{a},\mathbf{b}}(t) = Q(\mathbf{a}t+\mathbf{b})$. Since Q is homogeneous of degree $d+1$, the coefficient of t^{d+1} in $QL_{\mathbf{a},\mathbf{b}}(t)$ is $Q(\mathbf{a})$. However, $Q \in \langle g(X_1), g(X_2)\rangle \subseteq \mathcal{I}_{m,1}$ and therefore $Q(\alpha) = 0$ for every $\alpha \in \mathbb{F}_q^m$. In particular $Q(\mathbf{a}) = 0$. Thus, $\deg(QL_{\mathbf{a},\mathbf{b}}) \leq d$ and Q passes the degree d line test for the line $\ell_{\mathbf{a},\mathbf{b}}$. Thus, Q passes the degree d line test for all lines.

Now take the table $T = \mathrm{EVAL}(Q)$. By Corollary 3.2, there cannot be a polynomial P with $deg(P) \leq d < deg(Q) = d+1 < sq$ having the same table. However, we saw T passes all line tests. Thus, T wrongly passes the line test. □

5 Local testing above the RM testing dimension

In this section we look at the local characterization and local testing of $\mathrm{MRM}(q,m,d,s)$ by dimension k tests, when k is above the RM testing dimension $t_{q,d} = \lceil \frac{d+1}{q-\frac{q}{p}} \rceil$ of $\mathrm{RM}(q,m,d)$. By Theorem 1.2 dimension k subspaces give a local test (and hence also a local characterization) for $\mathrm{RM}(q,m,d)$. We show they also give a local test (and hence also a local characterization) for $\mathrm{MRM}(q,m,d,s)$ for $s < q$. There is, however, some parameter loss in the reduction as we next explain. To formally state the result we need some notation. For $x \in \mathbb{F}_q^m$ let

$$\begin{aligned} H_k &= \left\{\mathbf{h} = (\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_k) \mid \mathbf{h}_0, \ldots, \mathbf{h}_k \in \mathbb{F}_q^m, \dim(\mathrm{span}\{\mathbf{h}_1, \ldots, \mathbf{h}_k\}) = k\right\}, \text{and,} \\ H_{k,x} &= \left\{\mathbf{h} \in H_k \mid x \in \mathbf{h}_0 + \mathrm{Span}\left\{\mathbf{h}_1, \ldots, \mathbf{h}_k\right\}\right\}. \end{aligned}$$

By $\mathbf{h} \sim_k H$ (resp. $H_{k,x}$) we mean a choosing $\mathbf{h}$ uniformly at random from H_k (resp. $H_{k,x}$). We let $A_{\mathbf{h}} = \mathbf{h}_0 + \mathrm{Span}\left\{\mathbf{h}_1, \ldots, \mathbf{h}_k\right\}$ be the k-dimensional affine space defined by $\mathbf{h}$. We also recall the distance and rejection function from the introduction:

Definition 5.1. *Let $T : \mathbb{F}_q^m \to \Sigma_{m,s}$ be a table. Then*

- *$\delta(T, \mathrm{MRM}(q,m,d,s))$ is the distance between T and the closest evaluation table of a degree d polynomial, i.e., $\delta(T, \mathrm{MRM}(q,m,d,s)) = \min_{G \in \mathrm{MRM}(q,m,d,s)}\{\delta(T,G)\}$, and,*
- *$\mathrm{REJ}_{k,d}^{\mathrm{MRM}}(T)$ is the probability a dimension-k test demonstrates that T is not a degree d polynomial.*

With this notation we prove:

Theorem 5.2. *Let $\mathbb{F}_q$ be a field of size q, 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*

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

Then, for every $s < q$, for every T we have

$$\mathrm{REJ}_{k,d}^{\mathrm{MRM}}(T) \geq \min\left\{\alpha' \cdot \delta(T, \mathrm{MRM}(q,m,d,s)), c_0\right\} \tag{5.1}$$

for

$$\alpha' = \left(1 - \frac{s-1}{q}\right) \frac{1}{1 + q^{d/(q-1)\frac{1}{\alpha}}} \tag{5.2}$$

For example, assume q is prime. If $d+1 \leq q-1$ the testing dimension is 1, meaning that lines are a good local test for $\mathrm{RM}(q,m,d)$. Then, Theorem 5.2 says that lines are also a good test for $\mathrm{MRM}(q,m,d,s)$, alas, with a larger coefficient. Similarly, if $q < d \leq 2(q-1)$ the RM testing dimension is 2 and therefore planes are a good local test for $\mathrm{RM}(q,m,d)$. Then, Theorem 5.2 says that planes are also a good test for $\mathrm{MRM}(q,m,d,s)$, with a larger coefficient. In the same vein 3-dimensional planes are a good local test for $\mathrm{MRM}(q,m,d,s)$ when $d \leq 3(q-1)$.

To explain the intuition behind the theorem we first consider the characterization aspect of it. Suppose k is above the RM testing dimension, and that the table T passes all $\mathrm{MRM}(q,m,d,s)$ k-dimensional tests $\mathbf{h}$. Specifically, this means that for every $\mathbf{h} \in H_k$, the table T restricted to the k-dimensional affine space $A_{\mathbf{h}}$ is consistent with a degree d polynomial $P_{\mathbf{h}}$. Now, let $T_{(0)}$ be the table T where at each entry we keep only the evaluation of the function itself and remove the evaluations that are associated with higher derivatives. Then, in particular, for every $\mathbf{h} \in H_k$, the table $T_{(0)}$ restricted to the k-dimensional space $A_{\mathbf{h}}$ is still consistent with the degree d polynomial $P_{\mathbf{h}}$. As k is above the RM testing dimension, there must be a unique degree d polynomial P that is consistent with $P_{\mathbf{h}}$ (and the table $T_{(0)}$) for every $\mathbf{h} \in H_k$. This P is the only possible candidate for a low-degree explanation of the table T. What we need to check, and is indeed correct, is that since T passes all dimension k tests, P is indeed consistent with T.

The testing case requires more technical details but is similar in spirit. We first, again, look at $T_{(0)}$ that contains only the function evaluations, and not the higher derivatives evaluations. If T passes the test with high enough probability, then so does $T_{(0)}$, and this ensures the existence of a global degree-d polynomial P that agrees with most values of $T_{(0)}$. Again, what remains to be shown is that P agrees with most values of T, which we indeed prove.

In short, one can informally say that Theorem 5.2 shows that the MRM testing dimension is not larger than the RM testing dimension, and that above the RM testing dimension one can get *local testing* for MRM codes. A natural question is whether the MRM testing dimension is equal to the RM testing dimension, or not. In Section 4 we saw that when the RM testing dimension is larger than 1, so is the MRM testing dimension, and lines do not characterize the MRM code. One might be drawn to the conjecture that the RM and MRM testing dimensions coincide. However, surprisingly, in Section 6 we show that no matter what the RM testing dimension is, when $d < sq$ the MRM testing dimension is at most two (for a precise statement see Theorem 6.2). For example, for $\mathrm{MRM}(q,d,m,s)$ with $2q < d < 3(q-1)$, the RM testing dimension is (roughly) 3 while the MRM testing dimension is still 2.

Combining the result with Theorem 1.2 we get:

Corollary 5.3. *Let $d, q, s < q$ be positive integers and let $t = t_{q,d} = \lceil \frac{d+1}{q-\frac{q}{p}} \rceil$ be the RM testing*

dimension. Then,

$$\mathrm{REJ}^{\mathrm{MRM}}_{t,d}(T) \geq \min\left\{\frac{1}{3}\cdot(1-\frac{s-1}{q})\cdot\delta(T,\mathrm{MRM}(q,m,d,s)),\frac{1}{2(t+1)q^{t+1}}\right\}$$

Proof. Theorem 1.2 from [KR06] ensures that

$$\mathrm{REJ}_{t,d}(f) \geq \min\left\{\frac{q^t}{2}\cdot\delta(f,\mathrm{RM}(q,m,d)),\frac{1}{2(t+1)q^{t+1}}\right\}$$

Using Theorem 5.2 we see that

$$\alpha' \geq \left(1-\frac{s-1}{q}\right)\frac{1}{1+q^{d/(q-1)}\frac{1}{\alpha}} \geq \frac{1}{3}(1-\frac{s-1}{q}).$$

using the fact that $\frac{d}{q-1} \leq t$ and $\frac{q^{d/(q-1)}}{\alpha} \leq 2$. □

In particular, for $d < (q - \frac{q}{p})$ the line test is a local characterization, as $t_{q,d} = 1$.

We note that the assumption $s \leq d$ is quite natural, as derivatives with order higher than the degree must be identically zero. In contrast, it is not clear whether the assumption $s < q$ is indeed required, and we leave it for future study.

5.1 The proof

Proof. Let $T : \mathbb{F}_q^m \to \Sigma_{m,s}$ be a table. Let

$$\rho = \mathrm{REJ}^{\mathrm{MRM}}_{k,d}(T)$$

be the k-dimensional MRM test rejection probability. If $\rho \geq c_0$ we are done. Therefore, we assume $\rho < c_0$. We first utilize what we know at the zero level.

Claim 5.4. *Let $\delta^{\mathrm{RM}} = \delta^{\mathrm{RM}}_{q,m,d}$ be the distance of the $\mathrm{RM}(q,m,d)$ code. There exists a degree d polynomial P such that*

$$\Pr_{\mathbf{h}\in H_k}\left[(\phi_{\mathbf{h}}\circ T)|_{A_{\mathbf{h}}} \neq \mathrm{EVAL}(P|_{A_h})\right] \stackrel{\mathrm{def}}{=} \varepsilon_0 \leq \rho(1+\frac{1}{\alpha\cdot\delta^{\mathrm{RM}}}).$$

We call **h** good *if* $(\phi_{\mathbf{h}}\circ T)|_{A_{\mathbf{h}}} = \mathrm{EVAL}(P|_{A_h})$ *and* bad *otherwise. In this terminology,* $\varepsilon_0 = \Pr_{\mathbf{h}\in H_k}[\mathbf{h}$ *is bad*$]$.

Proof. Let $T_{(\mathbf{0})} : \mathbb{F}_q^m \to \mathbb{F}_q$ be as in Section 3, i.e., the table where we keep only the entries of the function evaluations and ignore the evaluations of higher order derivatives. For a given affine space A we have that $(T|_A)_{(\mathbf{0})} = T_{(\mathbf{0})}\big|_A$, and so if the former agrees with a degree d polynomial, so does the latter. It follows that

$$\mathrm{REJ}^{\mathrm{RM}}_{k,d}(T_{(\mathbf{0})}) \leq \rho.$$

By the hypothesis regarding $\mathrm{RM}(q,m,d)$ and using $\rho < c_0$ there exists a unique degree d polynomial $P \in \mathbb{F}_q[\mathbf{X}]$ such that

$$\delta_{(0)} \stackrel{\mathrm{def}}{=} \delta(T_{(\mathbf{0})},P) \leq \frac{\rho}{\alpha}.$$

We notice that

$$\mathbb{E}_{\mathbf{h}\sim H_k}\ \delta(T_{(\mathbf{0})}\big|_{A_\mathbf{h}}, P|_{A_\mathbf{h}}) = \Pr_{x\sim\mathbb{F}_q^m}(T_{(\mathbf{0})}(x)\neq P(x)) = \delta(T_{(\mathbf{0})}, P) = \delta_{(0)},$$

because the subspaces in $A_\mathbf{h}$ for $\mathbf{h}\in H_k$, cover every point an equal number of times. Therefore, by Markov's inequality,

$$\Pr_{\mathbf{h}\sim H_k}\left(\delta(T_{(\mathbf{0})}\big|_{A_\mathbf{h}}, P|_{A_\mathbf{h}}) \geq \delta^{\mathrm{RM}}\right) \leq \frac{\delta_{(0)}}{\delta^{\mathrm{RM}}} \tag{5.3}$$

Also, by assumption,

$$\Pr_{\mathbf{h}\in H_k}\left((\phi_\mathbf{h}\circ T)|_{A_\mathbf{h}} \notin \mathrm{MRM}(q,k,d,s)\right) \leq \rho. \tag{5.4}$$

This means that except for probability ρ over $\mathbf{h}$, $(\phi_\mathbf{h}\circ T)|_{A_\mathbf{h}}$ agrees with $\mathrm{EVAL}(P_\mathbf{h})$ for some k-variate degree d polynomial $P_\mathbf{h}$. When this happens it also holds that $T_{(\mathbf{0})}$ agrees with $P_\mathbf{h}$ over $A_\mathbf{h}$ (because $\phi_\mathbf{h}$ does not change the zero level).

Thus, Equations (5.3) and (5.4) together imply that except for probability $\rho+\frac{\delta_0}{\delta^{\mathrm{RM}}} \leq \rho(1+\frac{1}{\alpha\delta^{\mathrm{RM}}})$ over $\mathbf{h}$, we simultaneously have that $T_{(\mathbf{0})} = P_\mathbf{h}$ over $A_\mathbf{h}$ and that $\delta(T_{(\mathbf{0})}\big|_{A_\mathbf{h}}, P|_{A_\mathbf{h}}) < \delta^{\mathrm{RM}}$. When both events happen we conclude that

$$\delta(P_\mathbf{h}, P|_{A_\mathbf{h}}) < \delta^{\mathrm{RM}}$$

As $P_\mathbf{h}$ and $P|_{A_\mathbf{h}}$ are degree d polynomials on $A_\mathbf{h}$ and are closer than δ^{RM}, it must be the that in fact $P_\mathbf{h} = P|_{A_\mathbf{h}}$. Thus, $(\phi_\mathbf{h}\circ T)|_{A_\mathbf{h}}$ is a valid $\mathrm{MRM}(q,k,d,s)$ table, and it is the table of the polynomial $P|_{A_\mathbf{h}}$, i.e., $(\phi_\mathbf{h}\circ T)|_{A_\mathbf{h}} = \mathrm{EVAL}(P|_{A_\mathbf{h}})$ as desired. □

Our goal is to bound $\delta(\mathrm{EVAL}(P), T)$. This means that at most $x\in\mathbb{F}_q^m$ we should have $T(x) = \mathrm{EVAL}(P;x)$. $T(x)$ and $\mathrm{EVAL}(P;x)$ contains values for all the m-variate directional derivatives of order up to s. Our handle on these values is Claim 5.4, that shows that most $\mathbf{h}$ are good, meaning that the k-variate derivatives of $P|_{A_\mathbf{h}}$ and $\phi_\mathbf{h}\circ T|_{A_\mathbf{h}}$ are the same. We notice that every such k-variate derivative is a linear combination (dependent on $\mathbf{h}$) of the m-variate derivatives. If x is such that for many $\mathbf{h}\in H_{k,x}$, $\mathbf{h}$ is good, then for that x we get many linear equations on the m-variate derivatives. Our task is to prove that for many x there are enough good $\mathbf{h}\in H_{k,x}$ to force the underlying m-variate derivatives of P and T to agree.

Claim 5.5. *We say $x\in\mathbb{F}_q^m$ is* bad *if $\Pr_{\mathbf{h}\in H_{k,x}}[\mathbf{h}\ \textit{is bad}] \geq 1-\frac{s-1}{q}$ and* good *otherwise. Then*

$$\Pr_{x\in\mathbb{F}_q^m}[x\ \textit{is bad}] \leq \frac{q}{q-(s-1)}\cdot\Pr_{\mathbf{h}\in H_k}[\mathbf{h}\ \textit{is bad}].$$

Proof. We have

$$\mathbb{E}_{x\in\mathbb{F}_q^m}\left[\Pr_{\mathbf{h}\in H_{k,x}}(\ \mathbf{h}\text{ is bad})\right] = \Pr_{\mathbf{h}\in H_k}(\ \mathbf{h}\text{ is bad}) = \varepsilon_0,$$

where ε_0 is as in Claim 5.4. This is because choosing a uniform $\mathbf{h} \in H_k$ is the same as first choosing a uniform $x \in \mathbb{F}_q^m$ and then choosing a uniform $\mathbf{h} \in H_{k,x}$. Therefore, for every $c > 1$, by Markov's inequality,

$$\Pr_{x \in \mathbb{F}_q^m}\left[\Pr_{h \in H_{k,x}}(\mathbf{h} \text{ is bad}) \geq c \cdot \varepsilon_0\right] \leq \frac{1}{c}.$$

Choosing $c = \frac{q-(s-1)}{q \cdot \varepsilon_0}$ gives the result. □

We note that if most k-dimensional subspaces are good, then most lines are:

Claim 5.6. *For every $x \in \mathbb{F}_q^m$ and $k \geq 1$,*

$$\Pr_{\mathbf{u} \in H_{1,x}}[\mathbf{u} \textit{ is bad}] \leq \Pr_{\mathbf{h} \in H_{k,x}}[\mathbf{h} \textit{ is bad}]$$

Proof. Fix x. For every $\mathbf{h} \in H_{k,x}$, If $\mathbf{h}$ is good, then $(\phi_{\mathbf{h}} \circ T)|_{A_{\mathbf{h}}} = \text{EVAL}(P|_{A_{\mathbf{h}}})$. This implies, in particular, that for every $\mathbf{u} \in H_{1,x}$ such that $A_{\mathbf{u}} \subseteq A_{\mathbf{h}}$, we also have that $(\phi_{\mathbf{u}} \circ T)|_{A_{\mathbf{u}}} = \text{EVAL}(P|_{A_{\mathbf{u}}})$. The result then follows because we can sample $\mathbf{u} \in H_{1,x}$ by first sampling $\mathbf{h} \in A_{k,x}$ and then choosing a random $\mathbf{u} \in H_{1,x}$ such that $A_{\mathbf{u}} \subseteq A_{\mathbf{h}}$. □

We now fix any good x. We will prove:

Claim 5.7. *Suppose $x \in \mathbb{F}_q^m$ is good. Then for any m-variate direction $\mathbf{I}$ with $w(\mathbf{I}) < s$ we have*

$$T_{(\mathbf{I})}(x) = P^{(\mathbf{I})}(x) \tag{5.5}$$

Once we prove the claim we can conclude the proof of the theorem because:

$$\begin{aligned}\delta(T, \text{EVAL}(P)) &\leq \Pr_{x \in \mathbb{F}_q^m}(x \text{ is bad}) \leq \frac{q}{q-(s-1)} \cdot \varepsilon_0 \\ &\leq \frac{q}{q-(s-1)} \cdot \rho \cdot (1 + \frac{1}{\alpha \cdot \delta^{\text{RM}}}) \leq \rho \left(1 - \frac{q}{s-1}\right)^{-1} \left(1 + \frac{q^{d/(q-1)}}{\alpha}\right).\end{aligned}$$

Proof. (of Claim 5.7) Fix a good $x \in \mathbb{F}_q^m$ and let $w_0 < s$. We will show Equation (5.5) simultaneously for all m-variate directions $\mathbf{I}$ with $w(\mathbf{I}) = w_0$. We know that

$$\Pr_{\mathbf{u} \in H_{1,x}}(\mathbf{u} \text{ is bad}) \leq \Pr_{\mathbf{h} \in H_{k,x}}(\mathbf{h} \text{ is bad}) < 1 - \frac{s-1}{q}, \tag{5.6}$$

where the first inequality is by Claim 5.6 and the second because x is good.

Suppose $\mathbf{u} = (\mathbf{b}, \mathbf{a})$ is good (where $\mathbf{b}, \mathbf{a} \in \mathbb{F}_q^m$). Then, by definition, $(\phi_{\mathbf{u}} \circ T)|_{A_{\mathbf{u}}} = \text{EVAL}(P|_{A_{\mathbf{u}}})$. In particular $\phi_{\mathbf{u}}(T(x)) = \text{EVAL}(P|_{A_{\mathbf{u}}}; x)$, because $x \in A_\ell$. Now:

- By Definition 3.9 (and plugging $k = 1$)

$$(\phi_{\mathbf{u}}(T(x)))_{w_0} = \sum_{\mathbf{I}, w(\mathbf{I}) = w_0} T(x)_{(\mathbf{I})} \cdot \mathbf{a}^{\mathbf{I}},$$

- Also, by Lemma 2.8 (plugging $t = 0$),

$$(\mathrm{EVAL}(P|_{A_{\mathbf{u}}}; x))_{w_0} = \sum_{\mathbf{I}, w(\mathbf{I})=w_0} P^{\mathbf{I}}(x) \cdot \mathbf{a}^{\mathbf{I}}.$$

Thus, a good $\mathbf{u} = (\mathbf{b}, \mathbf{a})$ gives the liner equation

$$\sum_{\mathbf{I}, w(\mathbf{I})=w_0} (P^{\mathbf{I}}(x) - T(x)_{(I)}) \cdot \mathbf{a}^{\mathbf{I}} = 0,$$

where the variables are $v_{\mathbf{I}} = P^{\mathbf{I}}(x) - T(x)_{(I)}$ for every m-variate direction $\mathbf{I}$ of total weight exactly w_0. Thus, Equation (5.6) implies that

$$\Pr_{\mathbf{a} \in \mathbb{F}_q^m \setminus \{0\}} \left(\sum_{\mathbf{I}, w(\mathbf{I})=w_0} (T(x)_{(\mathbf{I})} - P^{(\mathbf{I})}(x)) \cdot \mathbf{a}^{\mathbf{I}} = 0 \right) > \frac{(s-1)}{q}.$$

Now, look at the polynomial $f_x \in \mathbb{F}_q[X_1, \ldots, X_m]$ defined by

$$f_x(\mathbf{a}) = \sum_{\mathbf{I}, w(\mathbf{I})=w_0} (T(x)_{(\mathbf{I})} - P^{(\mathbf{I})}(x)) \cdot \mathbf{a}^{\mathbf{I}}.$$

f_x is an m-variate, degree w_0 homogeneous polynomial, and it is 0 with probability larger than $\frac{(s-1)}{q} \geq \frac{w_0}{q} = \frac{\deg(f_x)}{q}$. By the Schwartz-Zippel lemma, it must be the 0 polynomial. Therefore, $T(x)_{(\mathbf{I})} - P^{(\mathbf{I})}(x)$ for all $\mathbf{I}$ with $w(\mathbf{I}) = w_0$ as desired. □

□

Remark 5.8. *Another way to view the argument, is that each $\mathbf{a} \in \mathbb{F}_q^m$ is an evaluation point of a homogeneous* $\mathrm{RM}(q, m, w_0)$ *codeword, and therefore each good $\mathbf{u} = (\mathbf{b}, \mathbf{a})$ gives a zero coordinate of the codeword. If the number of good $\mathbf{u}$ is too large, we get too many zeroes, and therefore the codeword must be the zero codeword, meaning that the values of the variables are zero as we wish.*

Remark 5.9. *The argument we use has the information that many k-dimensional restrictions are good, but then chooses to reduce this knowledge to the weaker statement that for many x, for many lines passing through x, the* linear *restrictions are good. It seems that using the stronger statement might give a better code and improve the parameters, but we have not succeeded yet in analyzing this.*

6 The plane test is a characterization

In this section we show that the multiplicity code $\mathrm{MRM}(q, m, d, s)$ can be characterized by restrictions to planes. Let $\mathbb{F}_q$ be a field and let $m, s \leq d$ be positive integers. For $\mathbf{a}, \mathbf{b}, \mathbf{c} \in {\mathbb{F}_q}^m$ [5] define:

[5] In this section, we omit the requirement that $\mathbf{a}, \mathbf{b}$ be independent. If some degenerate plane shows that a table is not a low degree polynomial, then some actual plane will too.

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

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

From Lemma 2.9 and Definition 3.9 we see that:

Theorem 6.1. *(Completeness) Suppose $d < sq - 1$. If a table $T \in \Sigma_{m,s}^{q^m}$ satisfies $T \in \mathrm{MRM}(q,m,d,s)$ then for all $\mathbf{a},\mathbf{b},\mathbf{c} \in \mathbb{F}_q^m$,*

$$\phi_{(\mathbf{a},\mathbf{b})} \circ T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}} \in \mathrm{MRM}(q,2,d,s).$$

The main challenge is proving the converse:

Theorem 6.2. *(Soundness) Suppose q is a power of the prime p, $q \geq s$ and $d < q(s - \frac{1}{p})$. If a table $T \in \Sigma_{m,2}^{q^m}$ satisfies that for all $\mathbf{a},\mathbf{b},\mathbf{c} \in \mathbb{F}_q^m$, $\phi_{(\mathbf{a},\mathbf{b})} \circ T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}} \in \mathrm{MRM}(q,2,d,s)$ then $T \in \mathrm{MRM}(q,m,d,s)$.*

We define the vector space of tables which pass the test:

$$V_{m,d,s} = \left\{ T \in \Sigma_{m,s}^{q^m} \mid \forall \mathbf{a},\mathbf{b},\mathbf{c} \in \mathbb{F}_q^m \;\; \phi_{(\mathbf{a},\mathbf{b})} \circ T \circ \ell_{\mathbf{a},\mathbf{b},\mathbf{c}} \in \mathrm{MRM}(q,2,d,s) \right\} \tag{6.1}$$

We denote by $C_{m,d,s} = V_{m,d,s} \backslash \mathrm{MRM}_{m,d,s}$, the set of tables which cheat the test. We would like to show that $C_{m,d,s} = \emptyset$. Assume towards a contradiction that there is a table $T \in C_{m,d,s}$. By Claim 3.3, T can be realized (uniquely) as an element P of the quotient space $\mathbb{F}_q[\mathbf{X}] \Big/ \mathcal{I}_{m,s}$. We use the basis $\mathcal{B}_{m,s}$ from Equation (3.1) to write P in the form

$$P(\mathbf{X}) = \sum_{(\mathbf{I},\mathbf{J}) \in \mathcal{M}_{s,q}} \alpha_{\mathbf{I},\mathbf{J}} \cdot g(\mathbf{X})^{\mathbf{I}} \mathbf{X}^{\mathbf{J}},$$

where $\alpha_{\mathbf{I},\mathbf{J}} \in \mathbb{F}_q$ and $(\mathbf{I},\mathbf{J}) \in \mathcal{M}_{s,q}$ iff $w(\mathbf{I}) < s$ and $J_k < q$ for every $1 \leq k \leq m$. Since $T \notin \mathrm{MRM}_{m,d,s}$ we have $deg(P) > d$. This means there must be some $\mathbf{I}$ and $\mathbf{J}$ such that $\alpha_{\mathbf{I},\mathbf{J}} \neq 0$ and

$$w(\mathbf{I})q + w(\mathbf{J}) > d. \tag{6.2}$$

We may assume that every $\mathbf{I},\mathbf{J}$ for which $\alpha_{\mathbf{I},\mathbf{J}} \neq 0$ satisfy Equation (6.2). This is since the test is linear, and any degree $\leqslant d$ terms have no effect on whether P passes the test or not.

We use the following monomial order $\succ_w$ on $\mathcal{B}_{m,s}$:

1. First order monomials according to $w(\mathbf{I}) + w(\mathbf{J})$,
2. Then order monomials according to $w(\mathbf{I})$,
3. Finally, order monomials according to the lexicographic order on $\mathbf{I},\mathbf{J}$.

We emphasize that $\succ_w$ is not a monomial order in the sense of Grobner bases, and we make no use of it in that sense.

Let $(\mathbf{I}_{\max},\mathbf{J}_{\max})$ be s.t. $g(\mathbf{X})^{\mathbf{I}_{\max}} \cdot X^{\mathbf{J}_{\max}}$ is a maximal monomial of P according to $\succ_w$.

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 $PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) = P(\mathbf{a}t + \mathbf{b}r + \mathbf{c})$. Expressing $PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r)$ in the basis $\mathcal{B}_{2,\infty}$:

$$PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) = \sum_{i\in\mathbb{N},j\in\mathbb{N},k,\ell<q} A_{i,j,k,\ell}(\mathbf{a},\mathbf{b},\mathbf{c}) \cdot g(t)^i g(r)^j t^k r^\ell$$
$$PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) \bmod I_{2,s} = \sum_{i+j<s,k,\ell<q} A_{i,j,k,\ell}(\mathbf{a},\mathbf{b},\mathbf{c}) \cdot g(t)^i g(r)^j t^k r^\ell$$

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

Lemma 6.3. *For every partition $\mathbf{J}_{\max} = \mathbf{J}^b_{\max} + \mathbf{J}^c_{\max}$ such that:*

- $q \cdot w(\mathbf{I}_{\max}) + w(\mathbf{J}^b_{\max}) \le qs - 1$, *and,*
- $\binom{\mathbf{J}_{\max}}{\mathbf{J}^b_{\max}} \neq 0 \bmod p$,

the monomial $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ appears with a non-zero coefficient at

$$A_{w(\mathbf{I}_{\max}),\lfloor \frac{w(\mathbf{J}^b_{\max})}{q} \rfloor, 0, w(\mathbf{J}^b_{\max}) \bmod q}(\mathbf{a},\mathbf{b},\mathbf{c}) \bmod \mathcal{I}_{3m,1}.$$

Where the ideal $\mathcal{I}_{3m,1}$ above is in the variables $a_1,\ldots,a_m,b_1,\ldots,b_m,c_1,\ldots,c_m$.

Proof. We expand $PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r)$. First, $P(\mathbf{X}) = \sum_{(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}} \alpha_{\mathbf{I},\mathbf{J}} \cdot g(\mathbf{X})^{\mathbf{I}}\mathbf{X}^{\mathbf{J}}$. Thus

$$\begin{aligned}
PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) &= \sum_{(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}} \alpha_{\mathbf{I},\mathbf{J}} \cdot g(\mathbf{a}t+\mathbf{b}r+\mathbf{c})^{\mathbf{I}}(\mathbf{a}t+\mathbf{b}r+\mathbf{c})^{\mathbf{J}} \\
&= \sum_{(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}} \alpha_{\mathbf{I},\mathbf{J}} \prod_{k=1}^{m} (g(a_kt+b_kr+c_k))^{I_k} \cdot \Pi_{i=k}^{m}(a_kt+b_kr+c_k)^{J_k} \\
&= \sum_{(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}} \alpha_{\mathbf{I},\mathbf{J}} \prod_{k=1}^{m} (g(t)a_k+g(r)b_k)^{I_k} \cdot \Pi_{i=k}^{m}(a_kt+b_kr+c_k)^{J_k} \\
&= \sum_{(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}} \alpha_{\mathbf{I},\mathbf{J}} \sum_{\substack{\mathbf{I}_a+\mathbf{I}_b=\mathbf{I} \\ \mathbf{J}_a+\mathbf{J}_b+\mathbf{J}_c=\mathbf{J}}} \binom{\mathbf{I}}{\mathbf{I}_a}\binom{\mathbf{J}}{\mathbf{J}_a,\mathbf{J}_b,\mathbf{J}_c} \mathbf{a}^{\mathbf{I}_a+\mathbf{J}_a}\mathbf{b}^{\mathbf{I}_b+\mathbf{J}_b}\mathbf{c}^{\mathbf{J}_c} \cdot g(t)^{w(\mathbf{I}_a)}g(r)^{w(\mathbf{I}_b)}t^{w(\mathbf{J}_a)}r^{w(\mathbf{J}_b)}
\end{aligned} \tag{6.3}$$

We expand $t^{w(J_a)}$ and $r^{w(J_b)}$ in the basis $\mathcal{B}_{1,s}$ as in Example 3.1 to get:

$$\begin{aligned}
PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(t,r) = \sum_{(\mathbf{I},\mathbf{J})\in\mathcal{M}_{s,q}} \alpha_{\mathbf{I},\mathbf{J}} \cdot \sum_{\substack{\mathbf{I}_a+\mathbf{I}_b=\mathbf{I} \\ \mathbf{J}_a+\mathbf{J}_b+\mathbf{J}_c=\mathbf{J}}} \binom{\mathbf{I}}{\mathbf{I}_a}\binom{\mathbf{J}}{\mathbf{J}_a\mathbf{J}_b\mathbf{J}_c} \\
\sum_{\substack{i_1,i_2 \\ i_1q+i_2\le w(\mathbf{J}_a) \\ i_2<q}} \sum_{\substack{j_1,j_2 \\ j_1q+j_2\le w(\mathbf{J}_b) \\ j_2<q}} \beta_{w(\mathbf{J}_a),i_1,i_2}\beta_{w(\mathbf{J}_b),j_1,j_2} \\
\mathbf{a}^{\mathbf{I}_a+\mathbf{J}_a}\mathbf{b}^{\mathbf{I}_b+\mathbf{J}_b}\mathbf{c}^{\mathbf{J}_c} \cdot g(t)^{w(\mathbf{I}_a)+i_1}t^{i_2} \cdot g(r)^{w(\mathbf{I}_b)+j_1}r^{j_2}.
\end{aligned} \tag{6.4}$$

We now have a representation in the basis $\mathcal{B}_{2,\infty}$.

Set:

$$\begin{aligned}\Delta_{rq} &= \left\lfloor \frac{w(\mathbf{J}^b_{\max})}{q} \right\rfloor \\ \Delta_t &= 0 \\ \Delta_r &= w(\mathbf{J}^b_{\max}) \bmod q.\end{aligned} \tag{6.5}$$

We wish to see for which choice of values $\mathbf{I}, \mathbf{J}, \mathbf{I}_a, \mathbf{I}_b, \mathbf{J}_a, \mathbf{J}_b, \mathbf{J}_c, i_1, i_2, j_1, j_2$ in Equation (6.3), $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ appears as a coefficient of $A_{(w(\mathbf{I}_{\max}),\Delta_{rq},\Delta_t,\Delta_r)} \bmod \mathcal{I}_{3m,1}$. We must have

$$\begin{aligned}
\mathbf{I}_{\max} &=_{\mathbb{F}_q} \mathbf{I}_a + \mathbf{J}_a && \text{By comparing the powers of } \mathbf{a}\text{, remembering mod } \mathcal{I}_{3m,1}\ , \\
\mathbf{J}^b_{\max} &=_{\mathbb{F}_q} \mathbf{I}_b + \mathbf{J}_b && \text{By comparing the powers of } \mathbf{b}\text{, remembering mod } \mathcal{I}_{3m,1}\ , \\
\mathbf{J}^c_{\max} &=_{\mathbb{F}_q} \mathbf{J}_c && \text{By comparing the powers of } \mathbf{c}\text{, remembering mod } \mathcal{I}_{3m,1}\ ,
\end{aligned}$$

where $=_{\mathbb{F}_q}$ was defined in Definition 2.24.

By Claim 2.26 together with $s < q$ we have

$$w(\mathbf{I}_{\max}) \le w(\mathbf{I}_a) + w(\mathbf{J}_a) \tag{6.6}$$
$$w(\mathbf{J}^b_{\max}) \le w(\mathbf{I}_b) + w(\mathbf{J}_b) \tag{6.7}$$
$$\mathbf{J}^c_{\max} = \mathbf{J}_c. \tag{6.8}$$

It follows that

$$\begin{aligned}
w(\mathbf{I}_{\max}) + w(\mathbf{J}_{\max}) &= w(\mathbf{I}_{\max}) + w(\mathbf{J}^b_{\max}) + w(\mathbf{J}^c_{\max}) \\
&\le w(\mathbf{I}_a) + w(\mathbf{J}_a) + w(\mathbf{I}_b) + w(\mathbf{J}_b) + w(\mathbf{J}_c) \\
&= w(\mathbf{I}) + w(\mathbf{J}).
\end{aligned}$$

As $(\mathbf{I}_{\max}, \mathbf{J}_{\max})$ is maximal it follows that

$$w(\mathbf{I}_{\max}) + w(\mathbf{J}_{\max}) = w(\mathbf{I}) + w(\mathbf{J}). \tag{6.9}$$

This, in turn, implies that both inequalities in Equations (6.6) and (6.7) are in fact equalities, i.e.,

$$w(\mathbf{I}_{\max}) = w(\mathbf{I}_a) + w(\mathbf{J}_a) \tag{6.10}$$
$$w(\mathbf{J}^b_{\max}) = w(\mathbf{I}_b) + w(\mathbf{J}_b). \tag{6.11}$$

We now look at

$$degt \stackrel{\text{def}}{=} \deg_t(g(t\mathbf{a})^{\mathbf{I}_a} \cdot (t\mathbf{a})^{\mathbf{J}_a} \cdot g(r\mathbf{b})^{\mathbf{I}_b} \cdot (r\mathbf{b})^{\mathbf{J}_b} \cdot \mathbf{c}^{\mathbf{J}_c} \bmod \mathcal{I}_{2,s}).$$

On the one hand, we look for the monomial $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ in $A_{w(\mathbf{I}_{\max}),\Delta_{rq},\Delta_t,\Delta_r} \bmod \mathcal{I}_{3m,1}$, and so we should have $degt = q \cdot w(\mathbf{I}_{\max}) + \Delta_t$. On the other hand, by Lemma 3.6,

$$\begin{aligned}
degt &= \deg_t(g(t\mathbf{a})^{\mathbf{I}_a}(t\mathbf{a})^{\mathbf{J}_a} g(r\mathbf{b})^{\mathbf{I}_b}(r\mathbf{b})^{\mathbf{J}_b}\mathbf{c}^{\mathbf{J}_c} \bmod \mathcal{I}_{2,s}) \\
&\le \deg_t(g(t\mathbf{a})^{\mathbf{I}_a}(t\mathbf{a})^{\mathbf{J}_a}) \\
&= q \cdot w(\mathbf{I}_a) + w(\mathbf{J}_a).
\end{aligned}$$

Thus,

$$q \cdot w(\mathbf{I}_{\max}) + \Delta_t \leq q \cdot w(\mathbf{I}_a) + w(\mathbf{J}_a).$$

Together with Equation (6.10) we see that $q \cdot w(\mathbf{I}_a) + q \cdot w(\mathbf{J}_a) + \Delta_t \leq q \cdot w(\mathbf{I}_a) + w(\mathbf{J}_a)$, and therefore $q \cdot w(\mathbf{J}_a) + \Delta_t \leqslant w(\mathbf{J}_a)$ which is possible iff $w(\mathbf{J}_a) = 0$ (and $\Delta_t = 0$, which is indeed true, see Equation (6.5)). Now, $w(\mathbf{J}_a) = 0$ implies:

$$\begin{aligned} w(\mathbf{I}_a) &= w(\mathbf{I}_{\max}), \text{ and,} \\ \mathbf{J}_a &= \emptyset. \end{aligned}$$

We saw in Equation (6.9) that $w(\mathbf{I}) + w(\mathbf{J}) = w(\mathbf{I}_{\max}) + w(\mathbf{J}_{\max})$. If $\mathbf{I}_b \neq \emptyset$ then

$$\begin{aligned} w(\mathbf{I}) &= w(\mathbf{I}_a) + w(\mathbf{I}_b) \\ &> w(\mathbf{I}_a) = w(\mathbf{I}_a) + w(\mathbf{J}_a) = w(\mathbf{I}_{\max}). \end{aligned}$$

Thus, $(\mathbf{I}, \mathbf{J}) \succ_w (\mathbf{I}_{\max}, \mathbf{J}_{\max})$ in contradiction to the maximality of $(\mathbf{I}_{\max}, \mathbf{J}_{\max})$. We conclude that

$$\mathbf{I}_b = \emptyset.$$

As $(\mathbf{I}_{\max}, \mathbf{J}_{\max}) \in \mathcal{M}_{s,q}$ we have $(\mathbf{J}_{\max})_k \leq q - 1$ for every $k \in [m]$. Thus, $\mathbf{J}^b_{\max} =_{\mathbb{F}_q} \mathbf{J}_b$, $w(\mathbf{J}^b_{\max}) = w(\mathbf{J}_b)$ and $\mathbf{J}^b_{\max}$ is already reduced. Together this implies that

$$\mathbf{J}^b_{\max} = \mathbf{J}_b.$$

Finally, we use the hypothesis that $q \geq s$. We have, $(\mathbf{I}_{\max})_k < s \leq q$ for all $k \in [m]$. Thus, $\mathbf{I}_{\max} =_{\mathbb{F}_q} \mathbf{I}_a$, $w(\mathbf{I}_{\max}) = w(\mathbf{I}_a)$ and $\mathbf{I}_{\max}$ is already reduced. Together this implies that that

$$\mathbf{I}_{\max} = \mathbf{I}_a.$$

Thus,

$$\begin{aligned} \mathbf{I}_{\max} = \mathbf{I}_a &= \mathbf{I}_a + \mathbf{I}_b = \mathbf{I}, \\ \mathbf{J}^b_{\max} &= \mathbf{I}_b + \mathbf{J}_b = \mathbf{J}_b. \end{aligned}$$

Altogether,the only term that may possibly contribute $\mathbf{a}^{\mathbf{I}_{\max}} \mathbf{b}^{\mathbf{J}^b_{\max}} \mathbf{c}^{\mathbf{J}^c_{\max}}$ to $A_{w(\mathbf{I}_{\max}), \Delta_{rq}, \Delta_t, \Delta_r}$ mod $\mathcal{I}_{3m,1}$ is $(\mathbf{I}_a, \mathbf{I}_b, \mathbf{J}_a, \mathbf{J}_b, \mathbf{J}_c) = (\mathbf{I}_{\max}, \emptyset, \emptyset, \mathbf{J}^b_{\max}, \mathbf{J}^c_{\max})$. Also, the tuple $(\mathbf{I}_a, \mathbf{I}_b, \mathbf{J}_a, \mathbf{J}_b, \mathbf{J}_c) = (\mathbf{I}_{\max}, \emptyset, \emptyset, \mathbf{J}^b_{\max}, \mathbf{J}^c_{\max})$ contributes

$$\alpha_{\mathbf{I}_{\max}, \mathbf{J}_{\max}} \cdot \binom{\mathbf{J}_{\max}}{\mathbf{J}^b_{\max}} \sum_{\substack{j_1, j_2 \\ j_1 q + j_2 \leqslant w(\mathbf{J}^b_{\max}) \\ j_2 < q}} \beta_{w(\mathbf{J}^b_{\max}), j_1, j_2} \mathbf{a}^{\mathbf{I}_{\max}} \mathbf{b}^{\mathbf{J}^b_{\max}} \mathbf{c}^{\mathbf{J}^c_{\max}} \cdot g(t)^{w(\mathbf{I}_{\max})} \cdot g(r)^{j_1} r^{j_2}.$$

to the term in Equation (6.3).

Notice that $w(\mathbf{I}_{\max}) + j_1 < s$, for otherwise $q \cdot w(\mathbf{I}_{\max}) + w(\mathbf{J}^b_{\max}) \geq q(w(\mathbf{I}_{\max}) + j_1) \geq qs$ in contradiction to the hypothesis. Thus the term is already $\mathcal{I}_{2,s}$ reduced. The contribution

to $A_{w(\mathbf{I}_{\max}),\Delta_{rq},0,\Delta_r} \bmod \mathcal{I}_{3m,1}$ occurs for (j_1, j_2) such that $j_1 = \Delta_{rq}$ and $j_2 = \Delta_r$. Thus, in the sum in Equation (6.3) there is exactly one possible way to contribute $\mathbf{a}^{\mathbf{I}_{\max}}\mathbf{b}^{\mathbf{J}^b_{\max}}\mathbf{c}^{\mathbf{J}^c_{\max}}$ to $A_{w(\mathbf{I}_{\max}),\Delta_{rq},0,\Delta_r} \bmod \mathcal{I}_{3m,1}$, and this is when

$$\begin{aligned}(\mathbf{I}_a, \mathbf{I}_b, \mathbf{J}_a, \mathbf{J}_b, \mathbf{J}_c) &= (\mathbf{I}_{\max}, \emptyset, \emptyset, \mathbf{J}^b_{\max}, \mathbf{J}^c_{\max}), \text{ and} \\ (i_1, i_2, j_1, j_2) &= (0, 0, \Delta_{rq}, \Delta_r).\end{aligned}$$

The coefficient of this term is:

$$\alpha_{\mathbf{I}_{\max},\mathbf{J}_{\max}} \cdot \binom{\mathbf{J}_{\max}}{\mathbf{J}^b_{\max}} \cdot \beta_{w(\mathbf{J}^b_{\max}),\Delta_{rq},\Delta_r}.$$

$\alpha_{\mathbf{I}_{\max},\mathbf{J}_{\max}} \neq 0$. By assumption $\binom{\mathbf{J}_{\max}}{\mathbf{J}^b_{\max}}$ is non-zero. $\beta_{\ell,\lfloor \frac{\ell}{q} \rfloor,\ell \bmod q} = 1$ (see Example 3.1) and taking $\ell = w(\mathbf{J}^b_{\max})$ shows the coefficient is non-zero. As there is a unique term contributing the monomial with a non-zero coefficient, the monomial cannot cancel in $A_{w(\mathbf{I}_{\max}),\Delta_{rq},\Delta_t,\Delta_r} \bmod \mathcal{I}_{3m,1}$ and $A_{w(\mathbf{I}_{\max}),\Delta_{rq},\Delta_t,\Delta_r} \bmod \mathcal{I}_{3m,1}$ is non-zero. □

Lemma 6.4. *There is a partition* $\mathbf{J}_{\max} = \mathbf{J}^b_{\max} + \mathbf{J}^c_{\max}$, *such that*

$$\begin{aligned}d < \ & q \cdot w(\mathbf{I}_{\max}) + w(\mathbf{J}^b_{\max}) \leq qs - 1, \text{ and,} \\ & \binom{\mathbf{J}_{\max}}{\mathbf{J}^b_{\max}} \bmod p \neq 0.\end{aligned}$$

Proof. Suppose $q = p^w$ where p is prime (if q is prime then $p = q$ and $w = 1$). We choose $\mathbf{J}^b_{\max}$ as follows. We go over $k = 1, \ldots, m$ and find the first $k_0 \geq 0$ such that $q \cdot w(\mathbf{I}_{\max}) + \sum_{k=0}^{k_0} (\mathbf{J}_{\max})_k > d$. There must be some $k_0 \leq m$ like that since $qw(\mathbf{I}_{\max}) + w(\mathbf{J}_{\max}) > d$. We set:

- $(\mathbf{J}^b_{\max})_k = (\mathbf{J}_{\max})_k$, for $k = 1, \ldots, k_0 - 1$, and,
- $(\mathbf{J}^b_{\max})_k = 0$, for $k = k_0 + 1, \ldots, m$.

Set $v = (\mathbf{J}_{\max})_{k_0}$. There is a first value $0 < v' \leq v$ such that

$$qw(\mathbf{I}_{\max}) + \sum_{k=1}^{k_0-1} (\mathbf{J}_{\max})_k + v' > d.$$

We express $v = (\mathbf{J}_{\max})_{k_0}$ in base p: $v = \sum_{\ell=0}^{w-1} v_\ell \cdot p^\ell$. We let v'' be the first integer such that:

- $v'' \geq v'$, and,
- If we express v'' in base p as $v'' = \sum_{\ell=0}^{w-1} v''_\ell \cdot p^\ell$ then $v''_\ell \leq v_\ell$ for every ℓ.

Claim 6.5. $v' \leq v'' \leq \min\{v, v' + p^{w-1} - 1\}$.

Proof. Notice that v respects the conditions that we need, and so if $v \leq v' + p^{w-1} - 1$ the claim holds. Otherwise, $v \geq v' + p^{w-1} - 1$. Then, $v'' \leq v' + p^{w-1} - 1$ because we can increase v' by setting all the lower bits in the p-representation to 0, while increasing the most significant bit (that is multiplied by p^{w-1}) by 1. □

Thus, by Lucas theorem (see Equation (2.1))

$$\binom{v}{v''} \bmod p = \Pi_{\ell=0}^{w-1} \binom{v_\ell}{v''_\ell} \neq 0.$$

Having that, we let $(\mathbf{J}^b_{\max})_{k_0} = v''$. We have, $\mathbf{J}^b_{\max} \leq \mathbf{J}_{\max}$, $qw(\mathbf{I}_{\max}) + w(\mathbf{J}^b_{\max}) > d$ and $\binom{\mathbf{J}_{\max}}{\mathbf{J}^b_{\max}} \bmod p \neq 0$. Also,

$$qw(\mathbf{I}_{\max}) + w(\mathbf{J}^b_{\max}) \leq d + p^{w-1} \leq qs - 1,$$

because $d \leq qs - p^{w-1} - 1 = q(s - \frac{1}{p}) - 1$, completing the proof of the lemma. □

We are now ready to prove Theorem 6.2.

Proof. Fix a partition $\mathbf{J}_{\max} = \mathbf{J}^b_{\max} + \mathbf{J}^c_{\max}$ as in Lemma 6.4. Let

$$\begin{aligned} degr &= \deg_r(g(t)^{w(\mathbf{I}_{\max})} r^{w(\mathbf{J}^b_{\max})} \bmod \mathcal{I}_{2,s}) \\ &= \deg_r(g(t)^{w(\mathbf{I}_{\max})} r^{w(\mathbf{J}^b_{\max})}) = w(\mathbf{J}^b_{\max}). \end{aligned}$$

Define $\Delta_{rq} = \lfloor \frac{w(\mathbf{J}^b_{\max})}{q} \rfloor$, $\Delta_t = 0$ and $\Delta_r = w(\mathbf{J}^b_{\max}) \bmod q$. By Lemma 6.3 we know that

$$A_{w(\mathbf{I}_{\max}),\Delta_{rq},\Delta_t,\Delta_r}(\mathbf{a},\mathbf{b},\mathbf{c}) \bmod \mathcal{I}_{3m,1} \neq 0$$

Thus, there exist $\mathbf{a}_0, \mathbf{b}_0, \mathbf{c}_0$ such that

$$A_{w(\mathbf{I}_{\max}),\Delta_{rq},\Delta_t,\Delta_r}(\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0) \neq 0$$

We look at the test $\mathbf{a}_0, \mathbf{b}_0, \mathbf{c}_0$. We have

$$PP_{\mathbf{a},\mathbf{b},\mathbf{c}}(r,t) \bmod \mathcal{I}_{2,s} = \sum_{i+j<s,k,\ell<q} A_{i,j,k,\ell}(\mathbf{a},\mathbf{b},\mathbf{c}) g(t)^i g(r)^j t^k r^\ell.$$

As $A_{w(\mathbf{I}_{\max}),\Delta_{rq},\Delta_t,\Delta_r}(\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0) \neq 0$ we see that

$$\begin{aligned} \deg(PP_{\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0} \bmod \mathcal{I}_{2,s}) &\geq q \cdot w(\mathbf{I}_{\max}) + q \cdot \Delta_{rq} + \Delta_t + \Delta_r \\ &= q \cdot w(\mathbf{I}_{\max}) + w(\mathbf{J}^b_{\max}) > d. \end{aligned}$$

Thus, by Lemma 3.8, the test $(\mathbf{a}_0, \mathbf{b}_0, \mathbf{c}_0)$ rejects. □

7 Planes give a local MRM tester

We restate Theorem 1.8:

Theorem 7.1. *Suppose q is a prime power, $s \leq q$ and $d < q(s - \frac{1}{p})$. Let $T : \mathbb{F}_q^m \to \Sigma_{m,s}$ be a table and let $\delta = \delta(T, \mathrm{MRM}(q,m,d,s))$. Then*

$$\mathrm{REJ}^{\mathrm{MRM}}_{2,d}(T) \geq \min\{\alpha\delta, c\}$$

with $\alpha = \Omega(q^{-6s+5})$ and $c = \Omega(q^{-8s+4})$.

Proof. We remind the reader that

$$H_k = \left\{\mathbf{h} = (\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_k) \mid \mathbf{h}_0, \ldots, \mathbf{h}_k \in \mathbb{F}_q^m, \dim(\text{span}\{\mathbf{h}_1, \ldots, \mathbf{h}_k\}) = k\right\}$$

Let us say that $\mathbf{v} \in H_k$ is *bad*, if the k-dimensional test with $\mathbf{v}$ rejects, i.e., $(\phi_{\mathbf{v}} \circ T)|_{A_{\mathbf{v}}} \notin \text{MRM}(q, k, d, s)$. We let $t = \lceil \frac{d+1}{q-\frac{q}{p}} \rceil$ be the $\text{RM}(q, m, d, s)$ testing dimension. Selecting a uniform $\mathbf{u} \in H_2$ is the same as selecting $\mathbf{h} \sim H_t$ and then a uniform $\mathbf{u} \in H_2$ such that $A_{\mathbf{u}} \subset A_{\mathbf{h}}$. Thus,

$$\begin{aligned}\text{REJ}_{2,d}^{\text{MRM}}(T) &= \Pr_{\mathbf{u} \sim H_2}(\mathbf{u} \text{ is bad}) \\ &\geq \Pr_{\mathbf{h} \in H_t}(\mathbf{h} \text{ is bad}) \cdot \Pr_{\mathbf{u} \in H_2 : A_{\mathbf{u}} \subset A_{\mathbf{h}}}(\mathbf{u} \text{ is bad} \mid \mathbf{h} \text{ is bad}).\end{aligned}$$

- By Corollary 5.3, the probability of picking a bad $\mathbf{h} \in H_t$ is:

$$\text{REJ}_{t,d}^{\text{MRM}}(T) \geq \min\left\{\frac{\delta}{3q}, \frac{1}{2(t+1)q^{t+1}}\right\}.$$

- By Theorem 6.2 we know that for any bad $\mathbf{h} \in H_t$ there is at least one $\mathbf{u} \in H_2$ such that $A_{\mathbf{u}}$ is contained $A_{\mathbf{h}}$ and $\mathbf{u}$ is bad. Furthermore, if $A_{\mathbf{u}} = A_{\mathbf{u}'}$ then $\mathbf{u}$ is bad iff $\mathbf{u}'$ is bad. We look at $A_{\mathbf{u}}$. There are $(q^2-1)(q^2-q)q^2$ different $\mathbf{u}' \in H_2$ such that $A_{\mathbf{u}'} = A_{\mathbf{u}}$ (because there are q^2-1 choices for the first basis element, q^2-q choices for the second basis element and $|A_{\mathbf{u}}| = q^2$ choices for the offset).

Altogether,

$$\text{REJ}_{2,d}^{\text{MRM}}(T) \geq \frac{\Omega(q^6)}{q^{3t}} \cdot \min\left\{\frac{\delta}{3q}, \frac{1}{2(t+1)q^{t+1}}\right\} = \Omega(\min\left\{q^{-3t+5}\delta, \frac{q^{-4t+5}}{t}\right\}).$$

We notice that $t \leq \lceil \frac{q(s-\frac{1}{p})}{q-\frac{q}{p}} \rceil \leq \lceil \frac{s}{1-\frac{1}{p}} \rceil \leq 2s$. Thus $\alpha = \Omega(q^{-6s+5})$ and $c = \Omega(q^{-8s+4})$ as promised.

□

References

[AKK+05] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing reed-muller codes. *IEEE Transactions on Information Theory*, 51(11):4032–4039, 2005. 1, 1, 1.5

[Alo99] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999. 1.3, 1.5, 2.20

[BKS+10] Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. Optimal testing of reed-muller codes. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 488–497. IEEE, 2010. 1, 1, 1.5

[BS09] Simeon Ball and Oriol Serra. Punctured combinatorial nullstellensätze. *Combinatorica*, 29(5):511–522, 2009. 1.3, 1.5, 2.23, 2.3

[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. 1.5, 2.3, 2.16, 2.19

[DKSS13] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to kakeya sets and mergers. *SIAM Journal on Computing*, 42(6):2305–2328, 2013. 2.6

[FS95] Katalin Friedl and Madhu Sudan. Some improvements to total degree tests. In *Proceedings Third Israel Symposium on the Theory of Computing and Systems*, pages 190–198. IEEE, 1995. 1, 1.1.1, 1.2, 1.2

[GLR+91] Peter Gemmell, Richard J. Lipton, Ronitt Rubinfeld, Madhu Sudan, and Avi Wigderson. Self-testing/correcting for polynomials and for approximate functions. In Cris Koutsougeras and Jeffrey Scott Vitter, editors, *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 32–42. ACM, 1991. 1

[GW13] Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of reed–solomon codes. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013. 1

[HSS13] Elad Haramaty, Amir Shpilka, and Madhu Sudan. Optimal testing of multivariate polynomials over small prime fields. *SIAM Journal on Computing*, 42(2):536–562, 2013. 1, 1, 1, 1.5, 2.2

[JPRZ04] Charanjit S Jutla, Anindya C Patthak, Atri Rudra, and David Zuckerman. Testing low-degree polynomials over prime fields. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pages 423–432. IEEE, 2004. 1, 1, 1.2, 1.5

[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. 1

[Kop13] Swastik Kopparty. Some remarks on multiplicity codes. *Discrete Geometry and Algebraic Combinatorics*, 625:155–176, 2013. 1

[KR06] Tali Kaufman and Dana Ron. Testing polynomials over general fields. *SIAM Journal on Computing*, 36(3):779–802, 2006. 1, 1.1, 1, 1.2, 1, 1.5, 5

[KSY14] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. *Journal of the ACM (JACM)*, 61(5):1–20, 2014. 1, 1, 2.8

[RS92] Ronitt Rubinfeld and Madhu Sudan. Self-testing polynomial functions efficiently and over rational domains. In Greg N. Frederickson, editor, *Proceedings of the Third Annual ACM/SIGACT-SIAM Symposium on Discrete Algorithms, 27-29 January 1992, Orlando, Florida, USA*, pages 23–32. ACM/SIAM, 1992. 1

[RS96] Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM Journal on Computing*, 25(2):252–271, 1996. 1, 1.2

[STV01] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the xor lemma. *Journal of Computer and System Sciences*, 62(2):236–266, 2001. 1

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il