CS 860 Topics in Coding Theory Nov. 10, 2025

Lecture 18

Lecturer: Elena Grigorescu *Scribe: Enver Aman*

1 Overview

We introduce derivatives of polynomials over $\mathbb{F}_q$. Particularly, we define Hasse derivatives and generalize the notion of multiplicity to multivariate polynomials. Then, we give a generalization of the Schwartz-Zippel lemma, which bounds the sum of the multiplicity of roots of a given polynomial as opposed to the usual statement bounding the number of roots.

Finally, we apply these ideas to form "bivariate multiplicty codes", which are bivariate Reed-Muller codes with extra information about derivatives attached to each symbol. These admit a randomized local correction algorithm with $O(\sqrt{n})$ many queires, where n is the block length of such codes. Furthermore, these codes have constant rate and relative distance as $n \to \infty$.

2 Recap: Reed-Muller Codes

We recall some results given in previous lectures.

Definition 1 (Reed-Muller Codes)**.** Let $m, k > 0$ be integers, $q > 0$ a prime power, and $n := q^m$. The *Reed-Muller Code* $\mathrm{RM}_q(m,k) \subseteq \mathbb{F}_q^n$ is the code defined by

$$\mathrm{RM}_q(m,k) := \Big\{ (f(\alpha) : \alpha \in \mathbb{F}_q^m) : f \in \mathbb{F}_q[x_1, \ldots, x_m], \deg(f) < k \Big\}.$$

A codeword $c \in \mathrm{RM}_q(m,k)$ will often be indexed by $c = (c_\alpha)_\alpha = (c_\alpha)_{\alpha \in \mathbb{F}_q^m}$. (Note that $|\mathbb{F}_q^m| = q^m = n$.)

Proposition 2 (Parameters of $\mathrm{RM}_q(m,k)$)**.** *For m, k, q, n as above with the additional assumption $k < 2q$,*

$$\mathsf{R}\big(\mathrm{RM}_q(m,k)\big) = \frac{k}{n} = \frac{k}{q^m} \quad \textit{and} \quad \delta\big(\mathrm{RM}_q(m,k)\big) \geq 1 - \frac{k}{q}.$$

Proof (Sketch) The distance bound follows from Schwartz-Zippel. The rate follows since each codeword is unique because the degree k is small enough. ■

The Schwartz-Zippel lemma mentioned above is this.

Lemma 3 (Schwartz-Zippel)**.** *Let $S \subseteq \mathbb{F}_q$ and $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ with degree $d > 0$. Then,*

$$\#\{\alpha \in S^m : f(\alpha) = 0\} \leq d|S|^{m-1}.$$

3 Derivatives of Polynomials in $\mathbb{F}_q$

Let's first introduce the usual notion of derivative of polynomials over $\mathbb{F}_q$. These behave in nearly the exact same way as derivatives of polynomials over $\mathbb{R}$. They are also easier to compute and it turns out that the majority of the results in this lecture can be expressed using only these derivatives. (One requires a fancier definition (see next section) to generalize some results in later sections.)

Definition 4 (Differentiation in $\mathbb{F}_q$)**.** Let $bx_1^{a_1}\cdots x_m^{a_m} \in \mathbb{F}_q[x_1,\ldots,x_m]$ be a monomial. (That is, $b \in \mathbb{F}_q$ and each $a_i \geq 0$.) It's *derivative with respect to x_i* is

$$\partial_{x_i}(bx_1^{a_1}\cdots x_m^{a_m}) = ba_i x_i^{a_i-1}\prod_{\substack{j=1\\ j\neq i}}^{m} x_j^{a_j}.$$

(Note ba_i is well-defined here since a_i is a nonnegative integer. When $a_i = 0$, the above is just 0.) In general, $\partial_{x_i}(f)$ is defined as the sum of the derivatives of the monomials that appear in f. We often write $\partial_{x_i} f$ instead of $\partial_{x_i}(f)$.

As a concrete example, $\partial_{x_i}(x_i^n) = nx_i^{n-1}$ for $n \geq 0$.

Derivatives of polynomials in $\mathbb{F}_q[x_1,\ldots,x_m]$ are analogous to derivatives of polynomials in $\mathbb{R}[x_1,\ldots,x_m]$, and nearly all properties of partial differentiation over $\mathbb{R}$ hold over to differentiation in $\mathbb{F}_q$. (The proofs of all of these are the same as that for polynomials over $\mathbb{R}$.)

Proposition 5 (Properties of ∂_{x_i})**.** *For all $i \in [m]$, let $\partial_{x_i} : \mathbb{F}_q[x_1,\ldots,x_m] \to \mathbb{F}_q[x_1,\ldots,x_m]$ be as above. Denote $\overline{x} := (x_1,\ldots,x_m)$, and let $f, g \in \mathbb{F}_q[\overline{x}]$.*

1. *∂_{x_i} is $\mathbb{F}_q$-linear,*
2. (Product rule) $\partial_{x_i}(fg) = g\partial_{x_i} f + f\partial_{x_i} g$,
3. (Clairaut's theorem) $\partial_{x_i}\partial_{x_j} = \partial_{x_j}\partial_{x_i}$ *for all $i, j \in [m]$.*

Remark For nonzero $f \in \mathbb{F}_q[x]$, note that $\partial_x(f) = 0$ **does not imply** that $\deg(f) = 0$. In particular, if $q = p^k$ for prime $p > 0$ (note q must be a prime power for $\mathbb{F}_q$ to be defined), then $p = 0$ in $\mathbb{F}_q$, $x^p \in \mathbb{F}_q[x]$ is nonzero, and

$$\partial_x(x^p) = px^{p-1} = 0.$$

Actually, something even worse is true: for *any* $f \in \mathbb{F}_q[x]$, $\partial_x^p(f) = 0$. This is in contrast to the situation in $\mathbb{Q}[x]$, where $\partial_x(x^n) = 0$ iff $n = 0$. The p above is the *characteristic* of $\mathbb{F}_q$, written $\mathrm{char}(\mathbb{F}_q)$. We'll see a way around this via something called *Hasse derivatives.*

4 Hasse Derivatives

Definition 6 (Hasse Derivatives)**.** Let $f \in \mathbb{F}_q[x_1, \ldots, x_m] =: \mathbb{F}_q[\overline{x}]$, and let $\overline{z} := (z_1, \ldots, z_m)$ be a new set of variables. For $i = (i_1, \ldots, i_m) \in \mathbb{Z}^m_{\geq 0}$, the *ith Hasse derivative* of f is the coefficient of $\overline{z}^i$ in $f(\overline{x} + \overline{z}) \in (\mathbb{F}_q[\overline{x}])[\overline{z}]$. Namely,

$$f(\overline{x} + \overline{z}) = \sum_{i \in \mathbb{Z}^m_{\geq 0}} f^{(i)}(\overline{x})\overline{z}^i.$$

For the same concrete example $f(\overline{x}) := x_i^n$ as in the previous section,

$$f(\overline{x} + \overline{z}) = (x_i + z_i)^n = \sum_{j=0}^{n} \binom{n}{j} x_i^{n-j} z_i^j,$$

so that $f^{(e_i)} = (x_i^n)^{(e_i)} = n x_i^n$. When $n = 0$, we will have $f^{(e_i)} = 0$, but we can still "detect" that $f(\overline{x}) = x_i^p$ is nonzero by noticing that

$$f(\overline{x} + \overline{z}) = (x_i + z_i)^p = x_i^p + z_i^p,$$

implying $f^{(pe_i)} = 1$. (So there's at least one Hasse derivative which is nonzero.)

These Hasse derivatives enjoy the same properties of the typical definition of derivatives. (Compare with Proposition 5.)

Proposition 7 (Properties of $f^{(i)}(\overline{x})$)**.** *For any $f, g \in \mathbb{F}_q[\overline{x}]$, the following hold.*

1. $f \in \mathbb{F}_q[\overline{x}] \mapsto f^{(i)} \in \mathbb{F}_q[\overline{x}]$ *is $\mathbb{F}_q$-linear for all $i \in \mathbb{Z}^m_{\geq 0}$,*
2. (Product rule) *For any $i \in \mathbb{Z}^m_{\geq 0}$,*

$$(fg)^{(i)} = \sum_{\substack{j,k \in \mathbb{Z}^m_{\geq 0} \\ j+k=i}} f^{(j)} g^{(k)}.$$

Proof (1) Let $a \in \mathbb{F}_q$, then

$$\sum_{i \in \mathbb{Z}^m_{\geq 0}} (f + ag)^{(i)}(\overline{x})\overline{z}^i = (f + ag)(\overline{x} + \overline{z}),$$

$$= f(\overline{x} + \overline{z}) + ag(\overline{x} + \overline{z}) = \sum_{i \in \mathbb{Z}^m_{\geq 0}} (f^{(i)}(\overline{x}) + ag^{(i)}(\overline{x}))\overline{z}^i$$

Equating coefficients of $\overline{z}^i$ on both sides yields the result.

(2) This follows from equating coefficients in the below.

$$(fg)(\overline{x} + \overline{z}) = \sum_{j \in \mathbb{Z}^m_{\geq 0}} f^{(j)}(\overline{x})\overline{z}^j \sum_{k \in \mathbb{Z}^m_{\geq 0}} g^{(k)}(\overline{x})\overline{z}^j = \sum_{i \in \mathbb{Z}^m_{\geq 0}} \overline{z}^i \left(\sum_{\substack{j,k \in \mathbb{Z}^m_{\geq 0} \\ j+k=i}} f^{(j)}(\overline{x}) g^{(k)}(\overline{x}) \right).$$

■

Next, we generalize the notion of multiplicity from univarite polynomials to multivariate polynomials. In one variable, the multiplicity of $\lambda \in \mathbb{F}_q$ of $f(x) \in \mathbb{F}_q[x]$ is the largest k such that $(x - \lambda)^k$ divides $f(x)$.

Definition 8 (Multiplicities)**.** Suppose $f \in \mathbb{F}_q[\overline{x}]$ is nonzero and $\alpha \in \mathbb{F}_q^m$. The *multiplicity of f at α* is the smallest integer $k \geq 0$ such that there exists $i = (i_1, \ldots, i_m) \in \mathbb{Z}_{\geq 0}^m$ with $i_1 + \cdots + i_m = k$ and $f^{(i)}(\alpha) \neq 0$. Denote this quantity $\operatorname{mult}(f, \alpha)$. We put $\operatorname{mult}(0, \alpha) := \infty$ for all $\alpha \in \mathbb{F}_q^m$.

Alternatively, $\operatorname{mult}(f, \alpha)$ is the minimum degree of a monomial that appears in $f(\overline{z}+\alpha)$. Further, $\operatorname{mult}(f, \alpha) > 0$ iff $f(\alpha) = 0$. The typical Schwartz-Zippel lemma stated above can be rewritten as

$$\sum_{\alpha \in S^m} \min\{1, \operatorname{mult}(f, \alpha)\} \leq d|S|^{m-1}$$

for $S \subseteq \mathbb{F}_q$ and $f \in \mathbb{F}_q[\overline{x}]$ of degree d. This can be generalized to take multiplicities into consideration.

Lemma 9 (Schwartz-Zippel with Multiplicity)**.** *Let $S \subseteq \mathbb{F}_q$ and $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ with degree $d > 0$. Then,*

$$\sum_{\alpha \in S^m} \operatorname{mult}(f, \alpha) \leq d|S|^{m-1}.$$

Proof Use induction on m. When $m = 1$, we have that $g := \prod_{\alpha \in S}(x - \alpha)^{\operatorname{mult}(f,\alpha)}$ divides f. Since f has degree d, we must have $\deg(g) = \sum_{\alpha \in S} \operatorname{mult}(f, \alpha) \leq d$.

Assume $m > 1$. Denote $\overline{x}' := (x_1, \ldots, x_{m-1})$ and define the polynomial

$$g_s(\overline{x}') := f(\overline{x}', s) = f(x_1, \ldots, x_{m-1}, s) \in \mathbb{F}_q[\overline{x}'],$$

for each $s \in S$. We claim that, for every $\beta \in S^{m-1}$ and $s \in S$,

$$\operatorname{mult}(f, (\beta, s)) \leq \operatorname{mult}(g_s, \beta).$$

Upon proving this claim, use induction on each g_s to obtain

$$\begin{aligned}\sum_{\alpha \in S^m} \operatorname{mult}(f, \alpha) = \sum_{s \in S} \sum_{\beta \in S^{m-1}} \operatorname{mult}(f, (\beta, s)) &\leq \sum_{s \in S} \sum_{\beta \in S^{m-1}} \operatorname{mult}(g_s, \beta), \\ &\leq \sum_{s \in S} d|S|^{m-2} = d|S|^{m-1}.\end{aligned}$$

OK, back to proving the claim. Note that $\operatorname{mult}(f, (\beta, s))$ is the smallest degree of a monomial appearing in $P_1(\overline{x}) := f(\overline{x}' + \beta, x_m + s)$; on the other hand, $\operatorname{mult}(g_s, \beta)$ is the smallest degree of a monomial appearing in $P_2(\overline{x}') := g_s(\overline{x}' + \beta) = f(\overline{x}' + \beta, s)$. We have that $P_2(\overline{x}')$ is equal to $P_1(\overline{x})$ with x_m set to zero. So, the minimum degree monomials in P_2 also appear in P_1. Hence, the claim holds.

■

Note that the proof above can be adjusted to work with $\mathbb{F}_q$ replaced by any domain R.

5 Bivariate Multiplicity Codes of Order-2

Of particular interest for us here are a modified bivariate Reed-Muller codes (i.e. of the form $\mathrm{RM}_q(2,k)$). These "multiplicity codes" were first introduced by Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin in 2010.

Definition 10 (Bivariate Multiplicity Code of Order-2)**.** Let $d > 0$ and q a prime power. The *order-2 multiplicity codeword* of a polynomial $f \in \mathbb{F}_q[x,y]$ with $\deg(f) < d$ is

$$c^{(2)}(f) := \Big(\Big(f(\alpha), (\partial_x f)(\alpha), (\partial_y f)(\alpha)\Big) : \alpha \in \mathbb{F}_q^2\Big) \in (\mathbb{F}_q^3)^{q^2}.$$

(Note: We are treating $c^{(2)}(f)$ as a codeword over the alphabet $\mathbb{F}_q^3$ with block length $|\mathbb{F}_q^2| = q^2$.) The corresponding *bivariate multiplicity code of order-2* is the collection of all these $c(f)$'s, and is denoted

$$\mathrm{RM}_q^{(2)}(2,d) := \Big\{c(f) \in (\mathbb{F}_q^3)^{q^2} : f \in \mathbb{F}_q[x,y],\ \deg(f) < d\Big\}.$$

Compare $\mathrm{RM}_q(2,d)$ to the above: for each $f \in \mathbb{F}_q[x,y]$ with $\deg(f) < d$ and $\alpha \in \mathbb{F}_q^2$, the αth entry of the corresponding codeword in $\mathrm{RM}_q(2,d)$ and in $\mathrm{RM}_q^{(2)}(2,d)$ is

$$f(\alpha) \in \mathbb{F}_q \qquad \text{and} \qquad (f(\alpha), \partial_x f(\alpha), \partial_y f(\alpha)) \in \mathbb{F}_q^3,$$

respectively. Intuitively, $\mathrm{RM}_q^{(2)}(m,d)$ is obtained from $\mathrm{RM}_q(2,d)$ by replacing each $f(\alpha)$ with the 3-tuple $(f(\alpha), \partial_x f(\alpha), \partial_y f(\alpha))$.

We'll focus mostly on the order-2 multiplicity codes defined above, but Kopparty-Saraf-Yekhanin generalize the above codes to higher order multiplicities by attaching Hasse derivatives of order up to s to each symbol. (The above is with $s = 2$.)

Let's compute the parameters of $\mathrm{RM}_q^{(2)}(2,d)$. If d is too large, then it could be that $c^{(2)}(f) = c^{(2)}(g)$ for some distinct $f, g \in \mathbb{F}_q[x,y]$ with $\deg(f), \deg(g) < d$. We claim that this cannot happen when $d < 2q$. First, a lemma about relating multiplicities and derivatives, which is a slightly more specific result of $f(\alpha) = 0$ iff $\mathrm{mult}(f,\alpha) \geq 1$.

Lemma 11. *Let $f \in \mathbb{F}_q[x,y]$ and suppose $\alpha = (a,b) \in \mathbb{F}_q^2$ is such that*

$$f(\alpha) = \partial_x f(\alpha) = \partial_y f(\alpha) = 0.$$

Then, $\mathrm{mult}(f,\alpha) \geq 2$.

Proof By assumption, we have that all three of

$$\mathrm{mult}(f,\alpha) \geq 1, \quad \mathrm{mult}(\partial_x f,\alpha) \geq 1, \quad \mathrm{mult}(\partial_y f,\alpha) \geq 1.$$

Correspondingly, there exists $r, s \in \mathbb{F}_q$ such that

$$f(x+a, y+b) = rx + sy + (\text{degree} \geq 2 \text{ terms}).$$

Compute ∂_x of the above:

$$\partial_x\Big(f(x+a,y+b)\Big) = (\partial_x f)(x+a,y+b) = r + (\text{degree} \geq 1 \text{ terms}).$$

But, $\text{mult}(\partial_x f, \alpha) \geq 1$, so $r = 0$. Similarly, $s = 0$. Hence, all monomials in $f(x+a, y+b)$ are of degree ≥ 2. ■

Now, we prove the claimed bound on k.

Lemma 12. *Let $f, g \in \mathbb{F}_q[x,y]$. Assume f, g are zero or $\deg(f), \deg(g) < 2q$ and*

$$f(\alpha) = g(\alpha), \quad \partial_x f(\alpha) = \partial_x g(\alpha), \quad \partial_y f(\alpha) = \partial_y g(\alpha)$$

for all $\alpha \in \mathbb{F}_q^2$. Then, $f = g$.

Proof It suffices to show the statement with $g = 0$. Assume f is nonzero and $d := \deg(f) < 2q$. From Lemma 11, we have that $\text{mult}(f, \alpha) \geq 2$ for all $\alpha \in \mathbb{F}_q^2$. Use Schwartz-Zippel with multiplicity (Lemma 9) with $S = \mathbb{F}_q$ to obtain

$$2q^2 = \sum_{\alpha \in \mathbb{F}_q^2} \text{mult}(f, \alpha) \leq dq.$$

Correspondingly, $d \geq 2q$, a contradiction. ■

As a result, for $f, g \in \mathbb{F}_q[x,y]$ with $\deg(f), \deg(g) < 2q$,

$$c^{(2)}(f) = c^{(2)}(g) \qquad \text{implies} \qquad f = g.$$

Proposition 13 (Parameters of $\text{RM}_q^{(2)}(2,d)$)**.** *Let q a prime power and $d < 2q$. Then,*

$$\mathsf{R}\Big(\text{RM}_q^{(2)}(2,d)\Big) = \frac{1}{3q^2}\binom{d+1}{2} \quad \textit{and} \quad \delta\Big(\text{RM}_q^{(2)}(2,d)\Big) \geq 1 - \frac{d}{2q}.$$

Proof The mapping $f \mapsto c^{(2)}(f)$ over $f \in \mathbb{F}_q[x,y]$ with $\deg(f) < d$ is injective, by the previous lemma. There are $\binom{d+1}{2}$ monomials in x, y of degree $< d$. So,

$$|\text{RM}_q^{(2)}(2,d)| = \#\{f \in \mathbb{F}_q[x,y] : \deg(f) < d\} = q^{\binom{d+1}{2}} = (q^3)^{\frac{1}{3}\binom{d+1}{2}}.$$

Note that the alphabet is $\mathbb{F}_q^3$ and of size q^3. The block length is q^2, so the rate is

$$\mathsf{R}\Big(\text{RM}_q^{(2)}(2,d)\Big) = \frac{1}{3q^2}\binom{d+1}{2}.$$

For the distance, note that $\text{RM}_q^{(2)}(2,d)$ is additive. So, it suffices to compute the minimum weight (over the alphabet $\mathbb{F}_q^3$) of a codeword $c^{(2)}(f) \in \text{RM}_q^{(2)}(2,d)$. Suppose $f \in \mathbb{F}_q[x,y]$ is such that

$$(f(\alpha), \partial_x f(\alpha), \partial_y f(\alpha)) = (0,0,0)$$

for $(1-\delta)q^2$ many $\alpha \in \mathbb{F}_q^2$. Use Lemma 11 to obtain $\mathrm{mult}(f,\alpha) \geq 2$ for δq^2 many $\alpha \in \mathbb{F}_q^2$. By Lemma 9,

$$2(1-\delta)q^2 \leq \sum_{\alpha \in \mathbb{F}_q^2} \mathrm{mult}(f,\alpha) \leq (\deg(f))q < dq.$$

Then, $\delta > 1 - d/(2q)$. Correspondingly, $\delta(\mathrm{RM}_q^{(2)}(2,d)) > 1 - d/(2q)$. ■

6 Local Correction of $\mathrm{RM}_q^{(2)}$

Throughout this section, fix $\delta > 0$, and consider the code $C_q(\delta) := \mathrm{RM}_q^{(2)}(2, 2(1-\delta)q)$. By Proposition 13,

$$\mathsf{R}\Big(C_q(\delta)\Big) = \frac{1}{3q^2}\binom{2(1-\delta)q+1}{2} \geq \frac{2}{3}(1-\delta)^2 \quad \text{and} \quad \delta\Big(C_q(\delta)\Big) > \delta.$$

We denote $c(f) := c^{(2)}(f)$ for $f \in \mathbb{F}_q[x,y]$ and treat $c(f)$ as a function $\mathbb{F}_q^2 \to \mathbb{F}_q^3$.

To be precise, we solve the following problem for to-be-determined parameters ε, ℓ. We're given as input $\alpha \in \mathbb{F}_q^2$ and functions $r, r_x, r_y \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ such that there exists $f \in \mathbb{F}_q[x,y]$ with $\deg(f) < 2(1-\delta)q$ and

$$\Big(f(\gamma), \partial_x f(\gamma), \partial_y f(\gamma)\Big) = \Big(r(\gamma), r_x(\gamma), r_y(\gamma)\Big)$$

for all but $\leq \varepsilon q^2$ many $\gamma \in \mathbb{F}_q^2$. The goal is to compute the triple $(f(\alpha), \partial_x f(\alpha), \partial_y f(\alpha))$ using at most ℓ queires to the value of (r, r_x, r_y) at points $\gamma \in \mathbb{F}_q^2$. Label $c(r) := (r, r_x, r_y) \colon \mathbb{F}_q^2 \to \mathbb{F}_q^3$. Throughout this section, we'll fix r, f, α as given here, and determine suitable values for ℓ, ε.

Loosely, the algorithm will be as follows: Pick a line in $\mathbb{F}_q^2$ through α uniformly at random. With high probability, $c(f) = c(r)$ for "most" points on the chosen line. The restriction of $c(f)$ to a line yields a univariate polynomial $h(t)$ and its derivative $h'(t)$; there are corresponding functions $H(t), H_1(t)$ involving only r, r_x, r_y such that $H(t) = h(t)$ and $H_1(t) = h'(t)$ for most $t \in \mathbb{F}_q$. Turns out, this is enough to recover the polynomials h, h'.

First we justify the choosing of the line. Given $\beta \in \mathbb{F}_q^2$, denote $L_\beta := \{\alpha + t\beta : t \in \mathbb{F}_q\}$ by the line through α in the direction of β and denote $\mathcal{L} := \{L_\beta : \beta \in \mathbb{F}_q^2\}$. Note that $L_\beta = L_{\beta'}$ iff $\beta = \lambda\beta'$ for $\lambda \in \mathbb{F}_q$, so there are $q+1$ distinct lines in $\mathcal{L}$. (Namely, $L_{(0,1)}$ and $L_{(1,\lambda)}$ for $\lambda \in \mathbb{F}_q$.) Finally, $L_\beta \cap L_\gamma = \{\alpha\}$ whenever L_β, L_γ are distinct lines. To actually choose the line, see the following lemma.

Lemma 14. *Let $\beta \in \mathbb{F}_q^2 \setminus \{(0,0)\}$ be chosen uniformly at random, and let $L_\beta \subseteq \mathbb{F}_q^2$ be the corresponding line.*

1. *This is the same as picking a uniformly random line L_β in $\mathcal{L}$.*
2. *There are at most 100 lines $L_\gamma \in \mathcal{L}$ such that the functions $c(f)|_{L_\gamma}, c(r)|_{L_\gamma} \colon L_\gamma \to \mathbb{F}_q^3$ disagree on $\geq \varepsilon q/50$ points in L_γ.*

(The choice of 100 and 50 is arbitrary here: they could be replaced by $2c$ and c for any constant $c > 1$.)

Proof (1) For a given $\gamma \in \mathbb{F}_q^2$, the probability that $L_\beta = L_\gamma$ equals the probability that β, γ are parallel, which is equal to the probability that $\beta \in \{\lambda\gamma : \lambda \in \mathbb{F}_q \setminus \{0\}\}$. This occurs with probability $(q-1)/(q^2-1) = 1/(q+1) = 1/|\mathcal{L}|$.

(2) Let N be the number of distinct lines $L_\gamma \in \mathcal{L}$ such that $c(f)|_{L_\gamma} \neq c(r)|_{L_\gamma}$ for $\geq \varepsilon q/50$ points. The collection $\{L \setminus \{\alpha\} : L \in \mathcal{L}\}$ is a partition for $\mathbb{F}_q^2 \setminus \{\alpha\}$. So, we obtain that $c(f) \neq c(r)$ disagree on $\geq N(q-1) \cdot (\varepsilon q/50)$ points in $\mathbb{F}_q^2$. On the other hand, $c(f), c(r)$ can only disagree in at most εq^2 points in $\mathbb{F}_q^2$. So,

$$N(q-1) \cdot \frac{\varepsilon q}{50} \leq \varepsilon q^2 \qquad \text{which implies} \qquad N \leq \frac{50q}{q-1} \leq 100$$

as long as $q \geq 2$. (This always happens actually by property of finite fields.) ■

As a result, the probability that $c(f)|_{L_\beta} \neq c(r)|_{L_\beta}$ for $< \varepsilon q/50$ many points is $\geq 1 - 100/(q-1)$, which grows close to 1 as q gets large. Such lines $L_\beta \in \mathcal{L}$ (i.e. all except for the ≤ 100 that yield the behavior in (2) above) are called *good lines* from here on.

For $\beta = (b_1, b_2) \in \mathbb{F}_q^2$ chosen as above with L_β a good line, define the functions

$$H_\beta(t) := r(\alpha + t\beta) \qquad \text{and} \qquad H_\beta^*(t) := b_1 r_x(\alpha + t\beta) + b_2 r_y(\alpha + t\beta).$$

Also define the univariate polynomial $h_\beta(t) := f(\alpha + t\beta)$. If t is such that $[c(f)](\alpha + t\beta) = [c(r)](\alpha + t\beta)$, then

$$H_\beta(t) = h_\beta(t) \quad \text{and} \quad H_\beta^*(t) = \partial_t h_\beta(t) = b_1 \partial_x f(\alpha + t\beta) + b_2 \partial_y f(\alpha + t\beta).$$

Hence, if L_β is good, then the pair (H_β, H_β^*) agrees with the pair $(h_\beta, \partial_t h_\beta)$ of univariate polynomials at $\geq (1 - \varepsilon/50)q$ many points $t \in \mathbb{F}_q$. Note that

$$\deg(h_\beta) \leq \deg(f) < 2(1-\delta)q.$$

It turns out this is enough to uniquely identify h_β when $\varepsilon := 50\delta$. For the next lemma, we label $\partial_t g(t) =: g'(t)$.

Lemma 15. *Suppose $d < q$, and let $g, h \in \mathbb{F}_q[t]$ with $\deg(g), \deg(h) < 2d$ if g, h respectively is nonzero. Assume that*

$$g(\lambda) = h(\lambda) \qquad \textit{and} \qquad g'(\lambda) = h'(\lambda)$$

for d many points $\lambda \in \mathbb{F}_q$. Then, $g = h$.

Proof It suffices to show the result with $h = 0$: so assume $g(\lambda_i) = g'(\lambda_i) = 0$ for distinct $\lambda_i \in \mathbb{F}_q$ with $i \in [d]$. This implies $(t - \lambda_i)^2$ divides $g(t)$ for each $i \in [d]$. Correspondingly,

$$g(t) = g_0(t) \prod_{i \in [d]} (t - \lambda_i)^2,$$

for another polynomial g_0. If g is nonzero, then $\deg(g) \geq 2d$, which is a contradiction. ■

The above lemma implies that if g with degree $< 2(1-\delta)q$ is such that (H_β, H_β^*) agrees with $(g, \partial_t g)$, then $g = h_\beta$. Via the Berlekamp-Welch algorithm, we can uniquely recover the polynomial $h_\beta(t)$ from the evaluations of (H_β, H_β^*) on all of $\mathbb{F}_q$. Finally, once we recover h_β, we can compute

$$h_\beta(0) = f(\alpha) \quad \text{and} \quad \partial_t h_\beta(0) = b_1 \partial_x f(\alpha) + b_2 \partial_y f(\alpha).$$

Repeat the test for a different line $L_\gamma \neq L_\beta$ for some $\gamma = (c_1, c_2) \in \mathbb{F}_q^2$. With high probability, L_γ is also a good line so that we recover a univariate polynomial $h_\gamma(t)$ such that

$$h_\gamma(0) = f(\alpha) \quad \text{and} \quad \partial_t h_\gamma(0) = c_1 \partial_x f(\alpha) + c_2 \partial_y f(\alpha).$$

Since L_β, L_γ are distinct lines, $\beta = (b_1, b_2)$ and $\gamma = (c_1, c_2)$ are linearly independent. Correspondingly, the system

$$\begin{bmatrix} b_1 & b_2 \\ c_1 & c_2 \end{bmatrix} \begin{bmatrix} \partial_x f(\alpha) \\ \partial_y f(\alpha) \end{bmatrix} = \begin{bmatrix} h_\beta(0) \\ h_\gamma(0) \end{bmatrix}$$

has a unique solution $(\partial_x f(\alpha), \partial_y f(\alpha))$. Thus, we have computed

$$[c(f)](\alpha) = (f(\alpha), \partial_x f(\alpha), \partial_y f(\alpha)).$$

The following theorem summarizes the result.

Theorem 16. *$C_q(\delta)$ is locally correctable up to a 50δ fraction of error using $2q$ queires, which is correct with probability $\geq (1 - \frac{100}{q-1})^2$.*

Proof The fraction ε of error we used was $\varepsilon := 50\delta$. The $2q$ queires came from evaluating the value of $(H_\beta, H_\beta^*)(t)$ and of $(H_\gamma, H_\gamma^*)(t)$ for each $t \in \mathbb{F}_q$: computing both of these requires the value of $c(r)$ on L_β and on L_γ. Finally, the algorithm is correct exactly when both H_β, H_γ are good lines, which occurs with probability $\geq (1 - 100/(q-1))^2$. ■