# Polynomials, Divided Differences, and Codes

**S. Venkitesh**
Tel Aviv University, Israel

## Abstract

Multiplicity codes (Kopparty et al., J. ACM 2014) are multivariate polynomial codes where the codewords are described by evaluations of polynomials (with a degree bound) and their derivatives up to some order (the multiplicity parameter), on a suitably chosen affine set of points. While efficient decoding algorithms were known in some special cases of point sets, by a reduction to univariate multiplicity codes, a general algorithm for list decoding up to the distance of the code when the point set is an arbitrary finite grid, was obtained only recently (Bhandari et al., IEEE TIT 2023). This required the characteristic of the field to be zero or larger than the degree bound, which is somewhat necessary since list decoding up to distance with small output list size is not possible when the characteristic is significantly smaller than the degree.

In this work, we present an alternative construction based on divided differences of polynomials, that conceptually resembles the classical multiplicity codes but has good list decodability "insensitive to the field characteristic". We obtain a simple algorithm that list decodes this code up to distance for arbitrary finite grids over all finite fields. Our construction can also be interpreted as a *folded Reed-Muller code*, which may be of independent interest.

**2012 ACM Subject Classification** Mathematics of computing → Coding theory; Theory of computation → Error-correcting codes

**Keywords and phrases** Error-correcting code, polynomial code, Reed-Solomon code, Reed-Muller code, folded Reed-Solomon code, folded Reed-Muller code, multiplicity code, divided difference, q-derivative, polynomial method, list decoding, list decoding capacity, linear algebraic list decoding

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2025.93

**Related Version** *Full Version*: `https://doi.org/10.48550/arXiv.2412.01755`

**Funding** A part of this work was done while the author was supported in part by BSF grant 2021683, ISF grant 735/20, and by the European Union (ERC, ECCC, 101076663).
*S. Venkitesh*: Len Blavatnik and the Blavatnik Family Foundation.

**Acknowledgements** The author thanks Dean Doron, Mrinal Kumar, Noga Ron-Zewi, Amnon Ta-Shma, and Mary Wootters for patiently listening to and giving feedback on presentations of this work at different times. A part of this work was done while the author was a postdoc at the Department of Computer Science, University of Haifa, and was participating in the program on Error Correcting Codes and Computation (2024) at the Simons Institute for the Theory of Computing, UC Berkeley.

## 1 Introduction and overview

Codes based on polynomial evaluations have found widespread applications, both implicitly and explicitly, in theoretical computer science, combinatorics, and allied areas. The prototypical univariate polynomial code is the *Reed-Solomon (RS) code* [57, 58], wherein the codewords are evaluations of degree bounded univariate polynomials on a set of points, and the prototypical multivariate polynomial code is the analogously defined *Reed-Muller (RM) code* [52, 57, 39, 68, 14]. [1] Despite several decades of research, the decodability properties of these codes are far from being well-understood.

[1] The RM code was considered over the binary field by [52, 57], and over larger fields by [39, 68, 14].

## 1.1 The list decoding problem

In this work, we are specifically interested in the *list decoding problem* [16, 69], where the aim is to output a list of close codewords for any given received word efficiently. The main parameter of interest is the *list decoding radius*, which represents the fraction of disagreements that we can decode from, and we would like it to be as large as possible.

### Unique decoding of polynomial codes

To begin with, consider the easier setting where we fix the list decoding radius to be *half the minimum distance* of the code, which is precisely the setting of the *unique decoding problem* – in this case, there could only be at most one codeword this close to any given received word, and the aim is to efficiently find it if it exists. This problem has now been solved completely for RS codes [56, 49, 67], for univariate multiplicity codes [53], for RM codes in a special case [40, 5], and quite recently for RM codes in general [41] and for multivariate multiplicity codes [8]. What is noteworthy is that all of these algorithms are *insensitive to the field characteristic*. We now move on to consider larger list decoding radius.

### List decoding of univariate polynomial codes

In the last decade of the 20th century, two classic works [65, 27] showed that all RS codes can be list decoded up to the *Johnson bound* (which is relative radius $1 - \sqrt{R}$, where $R$ is the rate of the code), and also laid an algebraic algorithmic framework that has since been exploited over and over again for several other polynomial codes. Further, we do not know of explicit RS codes that can be list decoded beyond the Johnson bound, but we do know of explicit RS codes that are not list decodable significantly beyond the Johnson bound [7]. Due to recent breakthroughs [11, 26, 2], we now know that random RS codes are list decodable *up to (information theoretic) capacity* (that is, relative radius $1 - R - \epsilon$ for arbitrarily small but fixed $\epsilon > 0$, which represents getting approximately close to the information theoretic limit of list decoding), but we neither know of an explicit construction nor know of an algorithm to achieve this.

It is in this context of list decoding up to the information theoretic capacity that a *folding* trick has been enlightening. The works of [28, 29] showed that *folded Reed-Solomon (FRS) codes* (where the bits of an RS codeword are bunched into blocks of large constant size), and univariate multiplicity codes [43] (wherein the codewords are evaluations of polynomials and their derivatives up to a large constant multiplicity) can be algorithmically list decoded up to capacity! Further improvements to the parameters have been achieved in [44, 61, 63, 12] in different settings.

### List decoding of multivariate polynomial codes

Moving on to multivariate polynomial codes, while the list decoding algorithms of [65, 27] generalize easily to RM codes, the decoding radius now worsens as a function of the number of variables, and attaining Johnson bound is no longer possible with these algorithms. While we know of a Johnson bound attaining algorithm [55] for RM codes when the finite grid is the full vector space $\mathbb{F}_q^m$ over the base field $\mathbb{F}_q$, designing a more general algorithm for arbitrary finite grids is still open!

As it turns out, the folding trick helps in the multivariate setting too. The multivariate multiplicity codes [45], which are the obviously defined multivariate analogues of univariate multiplicity codes, were shown to be list decodable *up to distance* (that is, up to radius $\delta - \epsilon$,

where $\delta$ is the minimum distance of the code) by [43] when the set of evaluation points is the full vector space $\mathbb{F}_q^m$. However, just as in the case of RM codes, an analogous result for arbitrary finite grids evaded us for quite some time. Very recently, [9] finally bolstered the algebraic algorithmic framework with some simple additional ingredients and managed to design an algorithm for list decoding multivariate multiplicity codes over arbitrary finite grids up to distance.

### Sensitivity of list decodability to the field characteristic

Finally, yet another crucial component that could influence the performance of the code (specifically a polynomial code) is the most fundamental underlying algebraic object – the base field over which the polynomials are considered, which is always a finite field in our discussion.

Unlike the unique decoding setting that we mentioned earlier, we do observe sensitivity to the field characteristic in the setting of the list decoding problem. Let us fix the notation that $\mathbb{F}_q$ denotes the base field, and $p$ denotes the characteristic of $\mathbb{F}_q$. On one hand, we know that when $q$ is a large power of $p$, there are RS codes that cannot achieve anywhere close to list decoding capacity [7] since we can show instances of received words having superpolynomial sized output lists. On the other hand, upon large constant folding, the univariate multiplicity codes achieve capacity when $p$ is larger than the degree parameter [29, 43], or smaller but linear in the degree [44], and the FRS codes achieve list decoding capacity [28, 29] insensitive to $p$. Thus, the list decodability of the FRS code is insensitive to the field characteristic, whereas the list decodability of the multiplicity code is sensitive to the field characteristic. Indeed, in the case when $q$ is a large power of $p$, the large output lists shown by [7] for RS codes can be used to construct large output lists for multiplicity codes, and so the list decodability is provably poor.

Things get even more interesting in the multivariate setting, since the multivariate multiplicity codes achieve distance when $p$ is larger than the degree parameter [55, 9], but we do not know of a field characteristic insensitive construction of a multivariate polynomial code that algorithmically achieves distance. Furthermore, we also do not know of an appropriate multivariate analogue of the field characteristic insensitive univariate FRS code. In this work, we answer both questions with a single code construction, along with a list decoding algorithm. In particular, our code subsumes the list decoding performance of the field characteristic sensitive multivariate multiplicity code [9], and also provides a natural *folded Reed-Muller code* construction. The motivation for our construction comes from an extremely simple yet foundational observation within the univariate world itself – the FRS code is also a multiplicity code!

## 1.2 FRS codes, univariate multiplicity codes, and divided differences

Fix a field $\mathbb{F}_q$. Consider distinct nonzero points $a_1, \ldots, a_n \in \mathbb{F}_q$. Let $\gamma \in \mathbb{F}_q^\times$ be a multiplicative generator, and suppose $s \geq 1$ such that the points $\gamma^j a_i$, $j \in [0, s-1]$, $i \in [n]$ are all distinct. For $k \in [sn]$, the degree-$k$ Folded Reed-Solomon (FRS) code is defined by

$$\mathrm{FRS}_s(a_1, \ldots, a_n; k) = \left\{ [f]_{\mathrm{FRS}} := \begin{bmatrix} f(a_1) \\ f(\gamma a_1) \\ \vdots \\ f(\gamma^{s-1} a_1) \end{bmatrix} \middle| \cdots \middle| \begin{bmatrix} f(a_n) \\ f(\gamma a_n) \\ \vdots \\ f(\gamma^{s-1} a_n) \end{bmatrix} : \begin{array}{l} f(X) \in \mathbb{F}_q[X], \\ \deg(f) < k \end{array} \right\} \subseteq \left(\mathbb{F}_q^s\right)^n.$$

Here, the distance function is the Hamming distance on alphabet $\mathbb{F}_q^s$, that is, the Hamming weight [2] of a codeword $[f]_{\mathrm{FRS}}$ is the number of $i \in [n]$ such that the block $\begin{bmatrix} f(a_i) & f(\gamma a_i) & \cdots & f(\gamma^{s-1} a_i) \end{bmatrix}^{\mathsf{t}}$ is a nonzero vector in $\mathbb{F}_q^s$.

On the other hand, simply assuming $a_1, \ldots, a_n \in \mathbb{F}_q$ are distinct and nothing more about these points, for $k \in [sn]$, the degree-$k$ (univariate) multiplicity code is defined by

$$\mathrm{Mult}_s(a_1, \ldots, a_n; k) = \left\{ [f]_{\mathrm{Mult}} := \begin{bmatrix} f^{(0)}(a_1) \\ f^{(1)}(a_1) \\ \vdots \\ f^{(s-1)}(a_1) \end{bmatrix} \middle| \cdots \middle| \begin{bmatrix} f^{(0)}(a_n) \\ f^{(1)}(a_n) \\ \vdots \\ f^{(s-1)}(a_n) \end{bmatrix} : \begin{array}{l} f(X) \in \mathbb{F}_q[X], \\ \deg(f) < k \end{array} \right\} \subseteq \left(\mathbb{F}_q^s\right)^n.$$

Here $f^{(j)}(X) := \frac{\mathrm{d}^j f(X)}{\mathrm{d}X^j}$ for all $j \in [0, s-1]$. [3] Once again, the Hamming weight of a codeword $[f]_{\mathrm{Mult}}$ is the number of $i \in [n]$ such that the block $\begin{bmatrix} f^{(0)}(a_i) & f^{(1)}(a_i) & \cdots & f^{(s-1)}(a_i) \end{bmatrix}^{\mathsf{t}}$ is a nonzero vector in $\mathbb{F}_q^s$.

Let us begin by looking at an algebraic feature that is intrinsic to multiplicity codes. Consider any $f(X) \in \mathbb{F}_q[X]$ with $\deg(f) < k$. For any $a \in \mathbb{F}_q$, we get the standard Taylor expansion

$$f(X) = f^{(0)}(a) + f^{(1)}(Y)(X-a) + f^{(2)}(a)\frac{(X-a)^2}{2!} + \cdots + f^{(k-1)}(a)\frac{(X-a)^{k-1}}{(k-1)!},$$

provided $p := \mathrm{char}(\mathbb{F}_q) \geq k$. Is there an analogous Taylor expansion in the context of the FRS code? As it turns out, there is such an expansion, and it is even simpler – it is the expansion in terms of the *Newton forward differences*. Precisely, we have

$$f(X) = f^{[0]}(a) + f^{[1]}(a)(X-a) + f^{[2]}(a)(X-a)(X-\gamma a) + \cdots + f^{[k-1]}(a)(X-a)\cdots(X-\gamma^{k-1}a),$$

where

$$f^{[0]}(a) = f(a), \;\; f^{[1]}(a) = \frac{f(\gamma a) - f(a)}{(\gamma-1)a}, \;\; \ldots, \;\; f^{[k-1]}(a) = \frac{f^{[k-2]}(\gamma a) - f^{[k-2]}(a)}{(\gamma^{k-1}-1)a}.$$

Notably, since $\gamma \in \mathbb{F}_q^\times$ is a multiplicative generator, we always have $\mathrm{ord}(\gamma) = q-1 \geq k$, and therefore, this expansion is valid *unconditional on* $p$.

In the first decade of the 20th century, Jackson [31, 32, 33] (also see [35, 34]) had defined the following specific *divided difference* operator on the polynomial ring,

$$\mathsf{D}_\gamma f(X) := \frac{f(\gamma X) - f(X)}{(\gamma-1)X}, \;\; \text{and} \;\; \mathsf{D}_\gamma^{t+1} := \mathsf{D}_\gamma \circ \mathsf{D}_\gamma^t \;\; \text{for all } t \geq 1.$$

In terms of this operator, the above expansion takes the form

$$f(X) = f(a) + \mathsf{D}_\gamma(a)(X-a) + \mathsf{D}_\gamma^2(a)\frac{(X-a)(X-\gamma a)}{[2]_\gamma!} + \cdots + \mathsf{D}_\gamma^{k-1}(a)\frac{(X-a)\cdots(X-\gamma^{k-1}a)}{[k-1]_\gamma!},$$

[2] We are only concerned with codes that are linear over the base field $\mathbb{F}_q$, and so the Hamming distance between two codewords $c_1, c_2$ is always equal to the Hamming weight of the codeword $c_1 - c_2$.

[3] Typically, since we are working over finite fields, there will also be a $j!$ scaling factor multiplied with the derivative, to prevent some pathologies arising in finite fields about higher multiplicity vanishing at a point. With this scaling factor, the derivative is usually called the Hasse derivative. We do not consider this, and implicitly assume that the characteristic is large enough so that these pathologies do not arise. Indeed, this is precisely the setting where the multiplicity codes have good list decodability.

where $[t]_\gamma := \frac{\gamma^t - 1}{\gamma - 1} = 1 + \gamma + \gamma^2 + \cdots + \gamma^{t-1}$, and $[t]_\gamma! := [t]_\gamma [t-1]_\gamma \cdots [1]_\gamma$. Returning to the code $\mathrm{FRS}_s(a_1, \ldots, a_n; k)$, it is then immediate by the definition of $D_\gamma$ that there are invertible lower triangular matrices $U(a_i) \in \mathbb{F}_q^{s \times s}$, $i \in [n]$ such that for any codeword $[f]_{\mathrm{FRS}}$, we have

$$\begin{bmatrix} f(a_i) \\ \mathsf{D}_\gamma f(a_i) \\ \vdots \\ \mathsf{D}_\gamma^{s-1} f(a_i) \end{bmatrix} = U(a_i) \cdot \begin{bmatrix} f(a_i) \\ f(\gamma a_i) \\ \vdots \\ f(\gamma^{s-1} a_i) \end{bmatrix} \qquad \text{for all } i \in [n].$$

In other words, after a specific change of basis (see, for instance, [42, 4] for a proof), the FRS code can be interpreted as a *multiplicity code* with respect to the *derivative-like operator* $\mathsf{D}_\gamma$.

Note that we have list decoding algorithms for FRS codes [28, 29], with the first one being algebraic and the second one being linear algebraic. If we are given the $\mathsf{D}_\gamma$*-multiplicity encoding*, we may just change the basis to the usual FRS encoding and run one of these two FRS decoders. However, what is really encouraging is that we can straightforwardly adapt the linear algebraic multiplicity decoder [29] to our $\mathsf{D}_\gamma$-multiplicity encoding, and the analysis will have a strong resemblance with that in the case of the classical derivatives. In this work, our main contribution is a construction that pushes this resemblance to the multivariate setting.

Our main algorithm will, in fact, work in the more general paradigm of list recovery, as was the case with the previous algorithms mentioned here.

### Assumption on the field

Since our intention is to present the basic ideas as clearly and quickly as possible, we will stick to a simpler setting henceforth, where we assume that the evaluation points are contained in a finite field $\mathbb{F}_q$, but the polynomials are over a degree-3 field extension $\mathbb{K} = \mathbb{F}_{q^3}$. (See Remark 4.) We can relax this setting to some extent by tinkering with the parameters involved, but we will not make this effort.

### The $\mathtt{Q}$-derivative

We will now forego the use of the symbol $\gamma$ for the multiplicative generator. Instead we will denote $\mathtt{Q} \in \mathbb{K}^\times$ to be a multiplicative generator, and henceforth refer to the operator $\mathsf{D}_\mathtt{Q}$ as the $\mathtt{Q}$-derivative. This is the more standard terminology in the literature where this operator has appeared before. The $\mathtt{Q}$-derivative [4] is also called the *Jackson derivative*, and is a special case of the *Hahn derivative* [30], as well as the *Newton forward difference* [36, Chapter 1, Section 9]. See [37, Chapter 26] for a discussion on a slightly more general *quantum differential*, as well as some symmetrized variants. These are all instances of a broader notion of *divided difference* in *finite calculus* [46, 10, 54, 64, 36, 59]. The $\mathtt{Q}$-derivative seems to have been used so far only over fields of characteristic zero, particularly in *q-combinatorics* [18, 3, 21, 60, 20] and *quantum calculus* [37, 17, 47]. Further, the $\mathtt{Q}$-derivative does not seem to have made any explicit appearance so far in the *polynomial method* literature. However, as we see in this work, this notion turns out to be useful over fields of positive characteristic, and indeed, as part of the polynomial method.

[4] We use the notation '$\mathtt{Q}$' in $\mathtt{Q}$-derivative in this work instead of the more popular '$q$', since we use $q$ to denote the field size.

## 1.3 Multivariate $\mathtt{Q}$-derivatives, multivariate $\mathtt{Q}$-multiplicity code, and *folded RM code*

Our extension of $\mathtt{Q}$-derivatives from the univariate to multivariate setting is natural, and mimicks the extension of the classical derivatives. Assume indeterminates $\mathbb{X} = (X_1, \ldots, X_m)$, and for any $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ and $\alpha \in \mathbb{N}^m$, we define the $\alpha$-th $\mathtt{Q}$-derivative as the iterated operator

$$\mathsf{D}^{\alpha}_{\mathtt{Q}} f(\mathbb{X}) := \mathsf{D}^{\alpha_1}_{\mathtt{Q},X_1} \cdots \mathsf{D}^{\alpha_m}_{\mathtt{Q},X_m} f(\mathbb{X}),$$

where $\mathsf{D}_{\mathtt{Q},X_i}$ denotes the univariate $\mathtt{Q}$-derivative in the variable $X_i$. It is easy to see that the operator $\mathsf{D}^{\alpha}_{\mathtt{Q}}$ is well-defined and invariant under the order of iterations, just as in the case of the classical partial derivatives.

Now consider indeterminates $\mathbb{Y} = (Y_1, \ldots, Y_m)$. For any $t \geq 0$, denote $(X_i - Y_i)^{(t)}_{\mathtt{Q}} := (X_i - Y_i)(X_i - \mathtt{Q}Y_i) \cdots (X_i - \mathtt{Q}^{t-1}Y_i)$, and further, for any $\alpha \in \mathbb{N}^m$, denote $(\mathbb{X} - \mathbb{Y})^{(\alpha)}_{\mathtt{Q}} := \prod_{i=1}^{m} (X_i - Y_i)^{(\alpha_i)}_{\mathtt{Q}}$. Also denote $[\alpha]_{\mathtt{Q}}! := [\alpha_1]_{\mathtt{Q}}! \cdots [\alpha_m]_{\mathtt{Q}}!$, and $\mathtt{Q}^{\alpha}\mathbb{X} = (\mathtt{Q}^{\alpha_1}X_1, \ldots, \mathtt{Q}^{\alpha_m}X_m)$. Then for any $s \geq 1$ and $a \in (\mathbb{F}_q^{\times})^m$, there exists (see Proposition 9) an invertible matrix $U(a) \in \mathbb{K}^{\binom{m+s-1}{s-1} \times \binom{m+s-1}{s-1}}$ such that

$$\left[\mathsf{D}^{\gamma}_{\mathtt{Q}} f(a)\right]_{|\gamma|<s} = U(a) \cdot \left[f(\mathtt{Q}^{\gamma} a)\right]_{|\gamma|<s} \qquad \text{for all } f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]. \tag{1}$$

Fix any $s \geq 1$, and consider any nonempty $A \subseteq \mathbb{F}_q^{\times}$. For any $k \in [s|A|]$, we define the $m$-variate multiplicity-$s$ degree-$k$ $\mathtt{Q}$-multiplicity code by

$$\begin{aligned}&\mathtt{Q}\text{-Mult}_{m,s}(A;k)\\ &\quad = \left\{[\mathsf{D}_{\mathtt{Q}} \mid f] := \left[\left[\mathsf{D}^{\gamma}_{\mathtt{Q}} f(a)\right]_{|\gamma|<s}\right]_{a \in A^m} : f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}],\, \deg(f) < k\right\} \subseteq \left(\mathbb{K}^{\binom{m+s-1}{s-1}}\right)^{|A|^m}.\end{aligned}$$

Note that the distance function is now the Hamming distance on the alphabet $\mathbb{K}^{\binom{m+s-1}{s-1}}$. Further, by the change of basis that we just saw above, we can define a natural multivariate analogue of the univariate FRS codes. For any $k \in [s|A|]$, we define the $s$-folded degree $k$ folded Reed-Muller (FRM) code by

$$\begin{aligned}&\mathrm{FRM}_{m,s}(A;k)\\ &\quad = \left\{[\mathtt{Q} \mid f] := \left[\left[f(\mathtt{Q}^{\gamma} a)\right]_{|\gamma|<s}\right]_{a \in A^m} : f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}],\, \deg(f) < k\right\} \subseteq \left(\mathbb{K}^{\binom{m+s-1}{s-1}}\right)^{|A|^m}.\end{aligned}$$

So by (1), we clearly have the change of basis

$$\mathtt{Q}\text{-Mult}_{m,s}(A;k) = \mathrm{diag}(U(a) : a \in A^m) \cdot \mathrm{FRM}_{m,s}(A;k).$$

The rate and distance of our code constructions can be given as follows, which will be immediate from Corollary 11 and Theorem 13.

▶ **Proposition 1.** *For any $k \in [s|A|]$, the codes $\mathtt{Q}$-Mult$_{m,s}(A;k)$ and $\mathrm{FRM}_{m,s}(A;k)$ have*

*rate equal to* $\dfrac{\binom{m+k-1}{k-1}}{\binom{m+s-1}{s-1}|A|^m}$, *and distance at least* $1 - \dfrac{k-1}{s|A|}$.

## 1.4 Our result

Our main result is that over *any* field $\mathbb{F}_q$ with sufficiently large $q$, and for sufficiently large constant multiplicity $s$, any constant rate multivariate $\mathtt{Q}$-multiplicity code $\mathtt{Q}$-Mult$_{m,s}(A;k)$, can be efficiently list decoded up to distance.

▶ **Theorem 2.** *Consider any $\delta \in (0,1)$, $\epsilon \in (0, 1-\delta)$. For any $A \subseteq \mathbb{F}_q^\times$ and for the choices $s = O(1/\epsilon^{2m+1})$ and $k = \lceil (1-\delta)s|A| \rceil$, the code $\mathtt{Q}$-$\mathrm{Mult}_s^m(A;k)$ is efficiently list decodable up to radius $\delta - \epsilon$ with output list contained in a $\mathbb{K}$-affine space of dimension atmost $O(1/\epsilon^{2m})$.*

Our list decoding algorithm is conceptually simpler than that by [9] for the classical multivariate multiplicity codes. Their algorithm in the classical setting entailed recovering the close enough polynomial messages one homogeneous component at a time, while using the classical *Euler's formula for homogeneous polynomials* (that relates a homogeneous polynomial to its first order derivatives) [5] to fully recover a homogeneous component (or a partial derivative of it) from its further first order partial derivatives. This formula, as well as the Taylor expansion for classical derivatives employed within the recovery step, both require the field characteristic to be large. In our $\mathtt{Q}$-setting, firstly there is no Euler's formula involving $\mathtt{Q}$-derivatives, and interestingly we don't need one! Secondly, the Taylor expansion for $\mathtt{Q}$-derivatives is clearly field characteristic insensitive. These are the only two places in the analysis where conceptually, the field characteristic was relevant in the classical setting, and is now irrelevant in the $\mathtt{Q}$-setting. Further, the short and clean analysis that we obtain encourages us to believe that this construction is the correct way to obtain a folded version of the RM code.

Let us give a quick outline of our algorithm. We make use of a clean *gluing* trick from [9] [6] and then proceed to perform a simpler analysis that is extremely close to the univariate analysis of [29]. The informal takeaway of what we show is that

$$\text{gluing trick} \;+\; \text{univariate list decoding analysis} \;=\; \text{multivariate list decoding analysis}.$$

Suppose we are given the code $\mathtt{Q}$-$\mathrm{Mult}_{m,s}(A;k)$ as in the statement of Theorem 2. Consider any received word

$$w = \Big(w_a := \Big[w_a^{(\gamma)}\Big]_{|\gamma|<s} : a \in A^m\Big) \in \big(\mathbb{K}^{\binom{m+s-1}{s-1}}\big)^{|A|^m}.$$

Consider two fresh sets of indeterminates $\mathbb{Y} = (Y_\gamma)_{|\gamma|<s}$ and $\mathbf{Z} = (Z_1, \ldots, Z_m)$. For a suitably chosen parameter $r \leq s$, we will find a nonzero interpolating polynomial with coefficients in $\mathbb{K}[\mathbf{Z}]$, having the form

$$P(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) = \widetilde{P}(\mathbb{X}) + \sum_{j=0}^{r-1} P_j(\mathbb{X}) \Big( \sum_{|\gamma|=j} Y_\gamma \mathbf{Z}^\gamma \Big),$$

such that the following hold.

**(Z1)** The polynomials $\widetilde{P}(\mathbb{X}), P_0(\mathbb{X}), \ldots, P_{r-1}(\mathbb{X})$ must have suitably chosen $\mathbb{X}$-degree bounds. We will also simultaneously ensure a good $\mathbf{Z}$-degree bound on the coefficients of these polynomials by performing Gaussian elimination over $\mathbb{K}[\mathbf{Z}]$, as given in [38] or [9, Lemma 3].

**(Z2)** For any $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$, define a projection

$$P^{[f]}(\mathbb{X}) := \widetilde{P}(\mathbb{X}) + \sum_{j=0}^{r-1} \Big( \sum_{|\gamma|=j} \mathsf{D}_{\mathtt{Q}}^\gamma f(\mathbb{X}) \mathbf{Z}^\gamma \Big).$$

[5] Euler's formula states that for a homogeneous degree-$d$ polynomial $f(\mathbb{X})$ over a field of characteristic greater than $d$, we have $\sum_{i=1}^m X_i \cdot \frac{\partial f(\mathbb{X})}{\partial X_i} = d \cdot f(\mathbb{X})$.

[6] As mentioned in [9], this gluing trick seems to have first appeared in the construction of a *hitting set generator* in [25].

Further, for every $\alpha \in \mathbb{N}^m$, $|\alpha| < s - r$, define a $\mathbb{K}(\mathbf{Z})$-linear operator $\Delta^{(\alpha)}$ (on an appropriate subspace of $\mathbb{K}(\mathbf{Z})[\mathbb{X}, \mathbb{Y}]$) that satisfies the condition $(\Delta^{(\alpha)}(P))^{[f]}(\mathbb{X}) = \mathsf{D}^{\alpha}_{\mathtt{Q}} P^{[f]}(\mathbb{X})$. The polynomial $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z})$ must now satisfy the vanishing conditions

$$\Delta^{(\alpha)}(P)(a, w_a, \mathbf{Z}) = 0 \qquad \text{for all } \alpha \in \mathbb{N}^m \text{ with } |\alpha| < s - r, \text{ and } a \in A^m.$$

Note that the vanishing conditions in (Z2) define a linear system on the coefficients of $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z})$, and we obtain the interpolating polynomial as a nontrivial solution of this linear system, by having large enough degree bounds as in (Z1). So for any close enough polynomial $f(\mathbb{X})$ (that is, having a large number of agreements with $w$), the conditions in (Z2) will imply that $P^{[f]}(\mathbb{X})$ vanishes at the agreement points with multiplicity at least $s - r$ (in the sense of multivariate $\mathtt{Q}$-derivatives, which we will define later), and this will imply that $P^{[f]}(\mathbb{X}) = 0$ by a suitable version of Polynomial Identity Lemma for multivariate $\mathtt{Q}$-derivatives. We can then solve this equation to recover $f(\mathbb{X})$. Importantly, the list decoding radius is dependent on the choice of $r$. We can achieve list decoding up to distance, that is, the claim of Theorem 2 by choosing $s = O(1/\epsilon^{2m})$ and $r = O(1/\epsilon^m)$. In fact, as in the analyses of [29, 9], we will show that the collection of all close enough polynomials is contained in a $\mathbb{K}$-affine subspace having dimension at most $\binom{m+r-2}{r-2}$.

This is a fairly simple strategy, very much within the algebraic algorithmic framework started employed in previous list decoding algorithms [65, 27, 28, 29, 43, 9]. Further, employing the gluing trick with the additional $\mathbf{Z}$-variables as in [9] allows us to formulate what we believe is the correct way to extend the linear algebraic decoding framework from the univariate to the multivariate setting, and our extension turns out to be simpler than the analysis in [9].

There is a subtlety in the recovery step in our multivariate setting vis-à-vis the univariate setting. When we solve the equation $P^{[f]}(\mathbb{X}) = 0$ to recover a close enough polynomial $f(\mathbb{X})$, we will see that the coefficients of $f(\mathbb{X})$ will be captured within the coefficients of some linear relations between monomials in the $\mathbf{Z}$-variables. Using a large enough efficient hitting set (an interpolating set of affine points that is large enough to certify all polynomials with a degree bound) in the $\mathbf{Z}$-variables, we can then recover each of these coefficients. This is similar to what was done in [9] in an analogous situation, but our overall analysis is a bit different and simpler. We will outline this difference now.

Formally, for a vector space $V_d \subseteq \mathbb{K}[\mathbf{Z}]$ of all polynomials having degree at most $d$, a hitting set is a finite set $H \subseteq \mathbb{K}^m$ such that for any $g(\mathbf{Z}) \in V_d$, if $g(\mathbf{Z}) \neq 0$ then there exists $u \in H$ such that $g(u) \neq 0$. For instance, by the Combinatorial Nullstellensatz [1, Theorem 1.1], every finite grid $S^m$ with $S \subseteq \mathbb{K}$, $|S| > d$ is a hitting set for $V_d$. (We will precisely use this obvious hitting set in our analysis.) Our departure from the analysis of [9] is that they need to recover the coefficients of $f(\mathbb{X})$ one homogeneous component at a time, by employing the Euler's formula. In our analysis, we will directly recover one coefficient at a time (with respect to a suitable choice of basis), and this is extremely similar to the corresponding step in the linear algebraic list decoding algorithm [29] for classical univariate multiplicity codes. Recall that we intend to obtain an affine subspace of small dimension that contains all close enough polynomials. Assume the form $f(\mathbb{X}) = \sum_{|\alpha|<k} f_\alpha \mathbb{X}^\alpha$ for all *target polynomials* in the affine subspace. We will recover the target polynomials inductively from *lower coefficients to higher coefficients*. In order to kick-start the recovery procedure, as a base case of the induction, we set the coefficients $\big(f_\gamma : |\gamma| \leq r - 2\big)$ arbitrarily. Then for any $\alpha \in \mathbb{N}^m$, $|\alpha| \leq k - r$, the equation $P^{[f]}(\mathbb{X}) = 0$ would imply an equation that has the form

$$\begin{aligned}\mathbb{K}[\mathbf{Z}]\text{-linear combination}\Big(f_{\alpha+\gamma} : |\gamma| = r - 1\Big)& \\ = \ \mathbb{K}[\mathbf{Z}]\text{-linear combination}\Big(f_{\theta+\eta} : (|\eta|, \theta) \leq (r-1, \alpha),\ (|\eta|, \theta) \neq (r-1, \alpha)\Big),&\end{aligned}$$

where the polynomials comprising the above $\mathbb{K}[\mathbf{Z}]$-linear combinations all have a good $\mathbf{Z}$-degree bound due to the $\mathbf{Z}$-degree bound on $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z})$. Note that each of the coefficients $f_{\theta+\eta}$ in the R.H.S. above is *strictly below* (in the usual componentwise partial order) some coefficient $f_{\alpha+\gamma}$ in the L.H.S. above. Since by induction hypothesis, we have already recovered all the coefficients in the R.H.S, we have the $\mathbb{K}[\mathbf{Z}]$-linear combination comprising the L.H.S. above also determined. We then instantiate a hitting set in the $\mathbf{Z}$-variables to recover the individual coefficients in the L.H.S. above, in much the same way as [9] instantiate for their linear combinations.

Thus, the coefficients $\left(f_\gamma : |\gamma| \leq r-2\right)$ are the only possible *free coefficients* in the above procedure, and therefore, the output list is contained in an affine $\mathbb{K}$-subspace having dimension at most $\binom{m+r-2}{r-2}$. We can further adapt the off-the-shelf *pruning* algorithm by [44] and its improved analysis by [66] to the multivariate setting, nearly identically as in [9], to finally end up with a randomized algorithm that guarantees constant output list size. Very recently, two concurrent works [63, 12] improved the output list size guarantee for list decoding FRS codes and univariate multiplicity codes from exponential in $1/\epsilon$ to $O(1/\epsilon^2)$ and the optimal $O(1/\epsilon)$ respectively. It is possible to extend their argument in the obvious way in the multivariate setting to give an even smaller output list size guarantee in the case of list decoding multivariate $\mathtt{Q}$-multiplicity codes. We do not mention the details in this presentation.

We will, in fact, prove a more general list recovery result as in Theorem 19, but stick to only showing polynomial output list size guarantee, for simplicity.

## 1.5 Further questions

Multivariate multiplicity codes evaluated on the vector space $\mathbb{F}_q^m$ are known to have good locality properties [45], especially when the field characteristic is larger than the degree [43, 44]. It will be interesting to see if similar locality properties hold for the multivariate $\mathtt{Q}$-multiplicity code in a field characteristic insensitive sense.

# 2 Preliminaries

### List decoding and list recovery

Let $\Sigma$ be a finite alphabet. An input list is any tuple $S = (S_1, \ldots, S_n)$ of subsets $S_i \subseteq \Sigma$. Further, for any $a \in \Sigma^n$, the (relative) Hamming distance between $a$ and $S$ is defined by

$$\mathsf{d}(a, S) = \frac{1}{n}|\{i \in [n] : a_i \notin S_i\}|.$$

We say an input list $S = (S_1, \ldots, S_n)$ is $\ell$-sized if $|S_i| \leq \ell$ for all $i \in [n]$.

Let $\mathbb{F}$ be a field, and consider an $\mathbb{F}$-linear code $C$, that is, $\Sigma$ is an $\mathbb{F}$-linear space.[7] For $\rho \in [0, 1]$ and $\ell, L \in \mathbb{Z}^+$, we say $C$ is $(\rho, \ell, L)$-list recoverable (LR) if there does not exist any $\ell$-sized sequence of input lists $S$ that admits $L+1$ distinct codewords $c^{(1)}, \ldots, c^{(L+1)} \in C$ such that

$$\mathsf{d}(c^{(j)}, S) \leq \rho, \qquad \text{for all } j \in [L+1].$$

The case $\ell = 1$ corresponds to list decoding with identical definitions.

[7] The more conventional definition defines $C$ to be a linear code if $C$ is linear over $\Sigma = \mathbb{F}$, but our definition is more relaxed where we allow $\Sigma$ to be an $\mathbb{F}$-linear space. Our relaxed definition holds for our codes of interest, whereas the conventional definition does not hold. Indeed, we heavily use the relaxed linearity properties of our code constructions, often implicitly.

### Field extensions

Fix a finite field $\mathbb{F}_q$, and a finite degree extension $\mathbb{K}/\mathbb{F}_q$ having extension degree $\kappa$, that is, $\mathbb{K} = \mathbb{F}_{q^\kappa}$. Also denote $[\kappa]_q = 1 + q + \cdots + q^{\kappa-1}$. Fix a multiplicative generator $\mathtt{Q} \in \mathbb{K}^\times$. We immediately note the following basic observations (see, for instance, [48, Chapter 2]), and also add quick proofs for completeness.

▶ **Proposition 3.**
**(a)** [48, Theorem 2.10] $\mathbb{K} = \mathbb{F}_q(\mathtt{Q})$.
**(b)** [48, Lemma 2.3] $\mathtt{Q}^t \notin \mathbb{F}_q$, *for all* $t \in [[\kappa]_q - 1]$.

**Proof.**
**(a)** Since $\mathbb{F}_q \subseteq \mathbb{K}$ and $\mathtt{Q} \in \mathbb{K}$, we have $\mathbb{F}_q(\mathtt{Q}) \subseteq \mathbb{K}$. Since $\mathbb{K}^\times = \{\mathtt{Q}^t : t \geq 0\}$, we have $\mathbb{K} \subseteq \mathbb{F}_q(\mathtt{Q})$.
**(b)** Since $\mathtt{Q}$ is the multiplicative generator of $\mathbb{K}^\times$, and $\mathbb{K} = \mathbb{F}_{q^\kappa}$, the multiplicative order of $\mathtt{Q}$ is $q^\kappa - 1$. Obviously, $\mathtt{Q}^t \neq 0$ for all $t \geq 1$. Now suppose $\mathtt{Q}^t \in \mathbb{F}_q^\times$ for some $t \geq 1$. Then $\mathtt{Q}^{t(q-1)} = 1$, which means $q^\kappa - 1 \leq t(q-1)$, that is, $t \geq (q^\kappa - 1)/(q-1) = 1 + q + \cdots + q^{\kappa-1} = [\kappa]_q$. ◀

▶ Remark 4. Note that in this work, we will assume that the field size $q \to \infty$. We will also consider an additional parameter $s \geq 1$, and always work in the case where $\mathtt{Q}, \ldots, \mathtt{Q}^{s-1} \notin \mathbb{F}_q$. By Proposition 3(b), this is true if $s - 1 < [\kappa]_q = 1 + q + q^2 + \cdots + q^{\kappa-1}$. Further, we will have the degree $d$ of all polynomials that we consider to satisfy $d \leq sq - 1$. Therefore, we will also need $sq - 1 < [\kappa]_q = 1 + q + q^2 + \cdots + q^{\kappa-1}$. Both these requirements are satisfied if we take $\kappa = 3$ and $s \leq q$, and we assume these throughout the rest of this work. In fact, we will only take $s$ to be a constant relative to $q$. So henceforth, we have $\mathbb{K} = \mathbb{F}_{q^3}$, and $\mathtt{Q}$ is a multiplicative generator of $(\mathbb{F}_{q^3})^\times$.

For any $n \geq k \geq 0$, denote

$$[n]_\mathtt{Q} = \sum_{t=0}^{n-1} \mathtt{Q}^t = \frac{\mathtt{Q}^n - 1}{\mathtt{Q} - 1}, \quad [n]_\mathtt{Q}! = \prod_{t=1}^{n} [t]_\mathtt{Q}, \quad \text{and} \quad \begin{bmatrix} n \\ k \end{bmatrix}_\mathtt{Q} = \frac{[n]_\mathtt{Q}!}{[k]_\mathtt{Q}![n-k]_\mathtt{Q}!}.$$

Note that $[n]_\mathtt{Q} \neq 0$ for all $n \in [q^\kappa - 2]$, and $[0]_\mathtt{Q}! = 1$. The quantity $\begin{bmatrix} n \\ k \end{bmatrix}_\mathtt{Q}$ is called the Gaussian binomial coefficient [22]. We will also have the convention that $[n]_\mathtt{Q}! = 0$ if $n < 0$, and $\begin{bmatrix} n \\ k \end{bmatrix}_\mathtt{Q} = 0$ if $k > n$.

## 2.1 Univariate $\mathtt{Q}$-derivatives

For any $f(X) \in \mathbb{K}[X]$, the $\mathtt{Q}$-derivative [31, 32, 33, 34, 35] is defined by

$$\mathsf{D}_\mathtt{Q} f(X) = \frac{f(\mathtt{Q}X) - f(X)}{(\mathtt{Q} - 1)X}.$$

Further, we are interested in iterated applications of the operator $\mathsf{D}_\mathtt{Q}$, and so we denote $\mathsf{D}_\mathtt{Q}^0 f(X) = f(X)$, and $\mathsf{D}_\mathtt{Q}^{t+1} f(X) = \mathsf{D}_\mathtt{Q}(\mathsf{D}_\mathtt{Q}^t f)(X)$ for all $t \geq 0$.

▶ Remark 5. We have $\mathsf{D}_\mathtt{Q}^t(X^k) = [k]_\mathtt{Q}[k-1]_\mathtt{Q} \cdots [k-t+1]_\mathtt{Q} X^{k-t+1}$ for all $k, t \geq 0$. Consider any nonconstant $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ and $t \in [0, \deg(f)]$. Then we immediately get $\deg(\mathsf{D}_\mathtt{Q}^t f) \leq \deg(f) - t$ by linearity of $\mathsf{D}_\mathtt{Q}^t$ (see Proposition 6(a) below). More importantly, as a departure from classical derivatives, we get $\deg(\mathsf{D}_\mathtt{Q}^t f) = \deg(f) - t$ if $\deg(f) \leq [\kappa]_q - 1$.

Let us quickly collect a few basic properties of $\mathtt{Q}$-derivatives. For an indeterminate $Y$ and $k \geq 0$, denote $(X - Y)_\mathtt{Q}^{(k)} = \prod_{t=0}^{k-1} (X - \mathtt{Q}^t Y)$. For any $f(X) \in \mathbb{K}[X]$ and $a \in \mathbb{K}^\times$, denote $(f \circ a)(X) = f(aX)$.

▶ **Proposition 6** ([37, 17]).

**(a)** Linearity. $\mathsf{D}_{\mathtt{Q}}^k$ *is an* $\mathbb{K}$*-linear map on* $\mathbb{K}[X]$*, for all* $k \geq 0$.

**(b)** Scaling. *For any* $f(X) \in \mathbb{K}[X]$ *and* $a \in \mathbb{K}^\times$,

$$\mathsf{D}_{\mathtt{Q}}^k(f \circ a)(X) = a^k \mathsf{D}_{\mathtt{Q}}^k f(aX) \qquad \text{for all } k \geq 0.$$

**(c)** Taylor expansion. *For any* $f(X) \in \mathbb{K}[X]$,

$$f(X) = \sum_{k \geq 0} \frac{\mathsf{D}_{\mathtt{Q}}^k f(Y)}{[k]_{\mathtt{Q}}!} (X - Y)_{\mathtt{Q}}^{(k)}.$$

*In particular,*

- *For any* $a \in \mathbb{K}$*, we have* $f(X) = \sum_{k \geq 0} \frac{\mathsf{D}_{\mathtt{Q}}^k f(a)}{[k]_{\mathtt{Q}}!} (X - a)_{\mathtt{Q}}^{(k)}$.
- *For any* $k \geq 0$*, we have* $\mathsf{D}_{\mathtt{Q}}^k f(0) = [k]_{\mathtt{Q}}! \cdot \mathsf{H}^{(k)} f(0)$*, where* $\mathsf{H}^{(k)} f(0)$ *is the* $k$-th Hasse derivative[8] *of* $f(X)$ *at* $0$.

**(d)** Product rule. *For any* $f(X), g(X) \in \mathbb{K}[X]$ *and* $k \geq 0$,

$$\mathsf{D}_{\mathtt{Q}}^k(fg)(X) = \sum_{t=0}^{k} \begin{bmatrix} k \\ t \end{bmatrix}_{\mathtt{Q}} \mathsf{D}_{\mathtt{Q}}^{k-t} f(\mathtt{Q}^t X) \mathsf{D}_{\mathtt{Q}}^t g(X) = \sum_{t=0}^{k} \begin{bmatrix} k \\ t \end{bmatrix}_{\mathtt{Q}} \mathsf{D}_{\mathtt{Q}}^{k-t} f(X) \mathsf{D}_{\mathtt{Q}}^t g(\mathtt{Q}^{k-t} X).$$

### Change of basis

A simple change of basis shows that $\mathtt{Q}$-derivatives are built out of simple evaluations at correlated points. Define an infinite matrix $\nu(X) \in (\mathbb{K}(X))^{\mathbb{N} \times \mathbb{N}}$ by

$$\nu_{k,t}(X) = \frac{(-1)^t \mathtt{Q}^{\binom{t}{2} - (k-1)t}}{(\mathtt{Q} - 1)^k X^k} \binom{k}{t}, \qquad \text{for all } k, t \geq 0.$$

Clearly, $\nu_{k,t}(X) = 0$ whenever $k < t$, that is, $\nu$ lower triangular. Further, we have the diagonal entries $\nu_{k,k}(X) = (-1)^k / (\mathtt{Q}^{\binom{k}{2}} (\mathtt{Q} - 1)^k X^k) \neq 0$ for all $k \geq 0$. So $\nu$ is invertible, and $\xi(X) := \nu(X)^{-1}$ is lower triangular, given by

$$\xi_{k,t}(X) = \begin{cases} (-1)^k \mathtt{Q}^{\binom{k}{2}} (\mathtt{Q} - 1)^k X^k & \text{if } k = t \geq 0, \\ \dfrac{(-1)^t (\mathtt{Q} - 1)^t X^t}{\mathtt{Q}^{\binom{k}{2} + (k-1)t}} \binom{k}{t} \left(1 - \left(1 - \dfrac{1}{\mathtt{Q}^{k-t-1}}\right)^{k-t}\right) & \text{if } k > t \geq 0. \end{cases}$$

This can be proven by instantiating, for instance, [62, Theorem 1.2.3].

▶ **Proposition 7** (Change of basis for $\mathtt{Q}$-derivatives). *For any* $f(X) \in \mathbb{K}[X]$ *and* $k \geq 0$*, we have*

$$\mathsf{D}_{\mathtt{Q}}^k f(X) = \sum_{t=0}^{k} \nu_{k,t}(X) f(\mathtt{Q}^t X) \quad [42, 4], \quad \text{and} \quad f(\mathtt{Q}^k X) = \sum_{t=0}^{k} \xi_{k,t}(X) \mathsf{D}_{\mathtt{Q}}^t f(X).$$

**Proof.** For any $f(X) \in \mathbb{K}[X]$, denote

$$(f \bullet \mathtt{Q}) = \left[f(\mathtt{Q}^k X)\right]_k \in (\mathbb{K}[X])^{\mathbb{N} \times 1} \quad \text{and} \quad (\mathsf{D}_{\mathtt{Q}} \bullet f) = \left[\mathsf{D}_{\mathtt{Q}}^k f(X)\right]_k \in (\mathbb{K}[X])^{\mathbb{N} \times 1}.$$

We have $(\mathsf{D}_{\mathtt{Q}} \bullet f) = \nu \cdot (f \bullet \mathtt{Q})$ by [42, 4]. Further, since $\xi = \nu^{-1}$, this implies $(f \bullet \mathtt{Q}) = \xi \cdot (\mathsf{D}_{\mathtt{Q}} \bullet f)$. ◀

[8] For $f(X) \in \mathbb{K}[X]$, the Hasse derivatives $\mathsf{H}^{(k)} f(Y)$, $k \geq 0$ satisfy: $f(X) = \sum_{k \geq 0} \mathsf{H}^{(k)} f(Y) (X - Y)^k$.

## 2.2 Multivariate $\mathtt{Q}$-derivatives

Now assume indeterminates $\mathbb{X} = (X_1, \ldots, X_m)$, and for any subset $I \subseteq [m]$, denote $\mathbb{X}_I = (X_i : i \in I)$. For every $i \in [m]$, denote the $\mathbb{K}$-linear $\mathtt{Q}$-derivative map on $\mathbb{K}[X_i]$ by $\mathsf{D}_{\mathtt{Q},X_i}$, and note that it extends in an obvious (and unique) way to a $\mathbb{K}(\mathbb{X}_{[m]\setminus\{i\}})$-linear map on $\mathbb{K}[\mathbb{X}]$. It is also immediate that $\mathsf{D}_{\mathtt{Q},X_1}, \ldots, \mathsf{D}_{\mathtt{Q},X_m}$ commute as $\mathbb{K}$-linear maps on $\mathbb{K}[\mathbb{X}]$. Then for any $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ and $\alpha \in \mathbb{N}^m$, we define the $\alpha$-th $\mathtt{Q}$-derivative by

$$\mathsf{D}^{\alpha}_{\mathtt{Q}} f(\mathbb{X}) = \mathsf{D}^{\alpha_1}_{\mathtt{Q},X_1} \cdots \mathsf{D}^{\alpha_m}_{\mathtt{Q},X_m} f(\mathbb{X}).$$

For $\alpha, \beta \in \mathbb{N}^m$, $\beta \le \alpha$, denote

$$[\alpha]_{\mathtt{Q}} = \prod_{i=1}^{m} [\alpha_i]_{\mathtt{Q}}, \quad [\alpha]_{\mathtt{Q}}! = \prod_{i=1}^{m} [\alpha_i]_{\mathtt{Q}}!, \quad \text{and} \quad \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_{\mathtt{Q}} = \frac{[\alpha]_{\mathtt{Q}}!}{[\beta]_{\mathtt{Q}}![\alpha-\beta]_{\mathtt{Q}}!} = \prod_{i=1}^{m} \begin{bmatrix} \alpha_i \\ \beta_i \end{bmatrix}_{\mathtt{Q}}.$$

Also, note the usual binomial coefficient $\binom{\alpha}{\beta} := \prod_{i=1}^{m} \binom{\alpha_i}{\beta_i}$. For indeterminates $\mathbb{Y} = (Y_1, \ldots, Y_m)$ and $\alpha \in \mathbb{N}^m$, denote $(\mathbb{X} - \mathbb{Y})^{(\alpha)}_{\mathtt{Q}} = \prod_{i=1}^{m} (X_i - Y_i)^{(\alpha_i)}_{\mathtt{Q}}$. For any $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ and $a \in \mathbb{K}^{\times}$, denote $a\mathbb{X} = (a_1 X_1, \ldots, a_m X_m)$, and $(f \circ a)(\mathbb{X}) = f(a\mathbb{X})$. Also denote $a^{\gamma} = a_1^{\gamma_1} \cdots a_m^{\gamma_m}$. For any $\gamma \in \mathbb{N}^m$, denote $\mathtt{Q}^{\gamma}\mathbb{Y} = (\mathtt{Q}^{\gamma_1} Y_1, \ldots, \mathtt{Q}^{\gamma_m} Y_m)$.

We easily get the following basic properties of multivariate $\mathtt{Q}$-derivatives.

▶ **Proposition 8.**

**(a)** Linearity. $\mathsf{D}^{\alpha}_{\mathtt{Q}}$ *is a* $\mathbb{K}$*-linear map on* $\mathbb{K}[\mathbb{X}]$*, for all* $\alpha \in \mathbb{N}^m$*.*

**(b)** Scaling. *For any* $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ *and* $a \in \mathbb{K}^{\times}$*, we have*

$$\mathsf{D}^{\beta}_{\mathtt{Q}}(f \circ a)(\mathbb{X}) = a^{\beta} \mathsf{D}^{\beta}_{\mathtt{Q}} f(a\mathbb{X}) \qquad \text{for all } \beta \in \mathbb{N}^m.$$

**(c)** Taylor expansion. *For any* $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$*,*

$$f(\mathbb{X}) = \sum_{\alpha \in \mathbb{N}^m} \frac{\mathsf{D}^{\alpha}_{\mathtt{Q}} f(\mathbb{Y})}{[\alpha]_{\mathtt{Q}}!} (\mathbb{X} - \mathbb{Y})^{(\alpha)}_{\mathtt{Q}}.$$

*In particular,*

- *For any* $a \in \mathbb{K}^m$*, we have* $f(X) = \sum_{\alpha \in \mathbb{N}^m} \frac{\mathsf{D}^{\alpha}_{\mathtt{Q}} f(a)}{[k]_{\mathtt{Q}}!} (\mathbb{X} - a)^{(\alpha)}_{\mathtt{Q}}$*.*
- *For any* $\alpha \in \mathbb{N}^m$*, we have* $\mathsf{D}^{\alpha}_{\mathtt{Q}} f(0^m) = [\alpha]_{\mathtt{Q}}! \cdot \mathsf{H}^{(\alpha)} f(0^m)$*, where* $\mathsf{H}^{(\alpha)} f(0^m)$ *is the* $\alpha$-th Hasse derivative[9] *of* $f(\mathbb{X})$ *at* $0^m$*.*

**(d)** Product rule. *For any* $f(\mathbb{X}), g(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ *and* $\alpha \in \mathbb{N}^m$*,*

$$\mathsf{D}^{\alpha}_{\mathtt{Q}}(fg)(\mathbb{X}) = \sum_{\beta \le \alpha} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_{\mathtt{Q}} \mathsf{D}^{\alpha-\beta}_{\mathtt{Q}} f(\mathtt{Q}^{\beta}\mathbb{X}) \mathsf{D}^{\beta}_{\mathtt{Q}} g(\mathbb{X}) = \sum_{\beta \le \alpha} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_{\mathtt{Q}} \mathsf{D}^{\alpha-\beta}_{\mathtt{Q}} f(\mathbb{X}) \mathsf{D}^{\beta}_{\mathtt{Q}} g(\mathtt{Q}^{\alpha-\beta}\mathbb{X}).$$

**Proof.** Each item follows easily by induction on $m$, with the base cases for Item (a), (b), (c), and (d) being Proposition 6(a), (b), (c), and (d) respectively. ◀

### Change of basis

Using the infinite matrices defined in Section 2.1, define two infinite matrices $\nu^{(m)}(\mathbb{X}), \xi^{(m)}(\mathbb{X}) : (\mathbb{K}(\mathbb{X}))^{\mathbb{N}^m \times \mathbb{N}^m}$ by

$$\nu^{(m)}_{\alpha,\beta}(\mathbb{X}) = \prod_{i=1}^{m} \nu_{\alpha_i,\beta_i}(X_i), \quad \xi^{(m)}_{\alpha,\beta}(\mathbb{X}) = \prod_{i=1}^{m} \xi_{\alpha_i,\beta_i}(X_i), \qquad \text{for all } \alpha, \beta \in \mathbb{N}^m.$$

[9] For $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$, the Hasse derivatives $\mathsf{H}^{(\alpha)} f(\mathbb{Y})$, $\alpha \in \mathbb{N}^m$ satisfy: $f(\mathbb{X}) = \sum_{\alpha \in \mathbb{N}^m} \mathsf{H}^{(\alpha)} f(\mathbb{Y})(\mathbb{X} - \mathbb{Y})^{\alpha}$.

It is then easy to see (for instance, by induction on $m$) that $\nu^{(m)}(\mathbb{X})$ is invertible and $\xi^{(m)}(\mathbb{X}) = (\nu^{(m)}(\mathbb{X}))^{-1}$. Also, $\nu^{(m)}_{\alpha,\beta}(\mathbb{X}) = \xi^{(m)}_{\alpha,\beta}(\mathbb{X}) = 0$ for all $\alpha, \beta \in \mathbb{N}^m$, $\alpha \not\geq \beta$, and $\nu^{(m)}_{\alpha,\alpha}(\mathbb{X}) \neq 0 \neq \xi^{(m)}_{\alpha,\alpha}(\mathbb{X})$ as well as $\nu^{(m)}_{\alpha,\alpha}(\mathbb{X}) = 1/\xi^{(m)}_{\alpha,\alpha}(\mathbb{X})$ for all $\alpha \in \mathbb{N}^m$. Further, we obtain the following change of basis, again by induction on $m$.

▶ **Proposition 9** (Change of basis for multivariate $\mathtt{Q}$-derivatives). *For any $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ and $\alpha \in \mathbb{N}^m$, we have*

$$\mathsf{D}^{\alpha}_{\mathtt{Q}} f(\mathbb{X}) = \sum_{\beta \leq \alpha} \nu^{(m)}_{\alpha,\beta}(\mathbb{X}) f(\mathtt{Q}^{\beta}\mathbb{X}), \quad \textit{and} \quad f(\mathtt{Q}^{\alpha}\mathbb{X}) = \sum_{\beta \leq \alpha} \xi^{(m)}_{\alpha,\beta}(\mathbb{X}) \mathsf{D}^{\beta}_{\mathtt{Q}} f(\mathbb{X}).$$

## A monomial basis for function spaces

We assume familiarity with Gröbner basis theory. For definitions and more details, see [13, Chapters 2–5]. For any $A \subseteq \mathbb{F}_q^{\times}$, consider the ideal defined (by appealing to the change of basis in Proposition 9) as

$$\begin{aligned}\mathcal{D}^m_s(A) &= \{f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}] : f(\mathtt{Q}^{\gamma}a) = 0 \text{ for all } a \in A \text{ and } \gamma \in \mathbb{N}^m, |\gamma| < s\} \\ &= \{f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}] : \mathsf{D}^{\gamma}_{\mathtt{Q}} f(a) = 0 \text{ for all } a \in A \text{ and } \gamma \in \mathbb{N}^m, |\gamma| < s\}.\end{aligned}$$

The following is a characterization of a Gröbner basis of $\mathcal{D}^m_s(A)$ that is *universal* (invariant under choice of monomial order) and *reduced* (minimal with respect to divisibility of leading terms).[10] This is an extension of [1, Theorem 1.1] and [6, Theorem 4.1], while being a special case of [23, Theorem 4.7].[11] A similar characterization in the case of classical multivariate derivatives was given in [43, Section 6], and can also be obtained by [23, Theorem 4.7].

▶ **Theorem 10** ([23]). *For any $A \subseteq \mathbb{F}_q^{\times}$, the set of polynomials*

$$\mathcal{G}^m_s(A) := \left\{ \prod_{i=1}^{m} \prod_{t=0}^{\gamma_i - 1} \left( \prod_{a_i \in A} (X_i - \mathtt{Q}^t a_i) \right) : \gamma \in \mathbb{N}^m, |\gamma| = s \right\}$$

*is a universal reduced Gröbner basis for $\mathcal{D}^m_s(A)$.*

Further, for any $A \subseteq \mathbb{F}_q^{\times}$, define the function spaces

$$V_{m,s}(A) = \left\{ [f] := \left[ [f]_a := \left[ f(\mathtt{Q}^{\gamma}a) \right]_{|\gamma|<s} \right]_{a \in A^m} : f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}] \right\},$$

$$\text{and} \quad \mathsf{D}_{\mathtt{Q}} V_{m,s}(A) = \left\{ [\mathsf{D}_{\mathtt{Q}} \mid f] := \left[ [\mathsf{D}_{\mathtt{Q}} \mid f]_a := \left[ \mathsf{D}^{\gamma}_{\mathtt{Q}} f(a) \right]_{|\gamma|<s} \right]_{a \in A^m} : f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}] \right\}.$$

As an immediate corollary of Theorem 10 and the simple properties of Euclidean division for polynomials, we can describe a *monomial basis* (a basis where each vector is the appropriate evaluation of a monomial) for the above vector spaces.

[10] Given any monomial order, a universal Gröbner basis and a reduced Gröbner basis for an ideal both always exist; however, a Gröbner basis that is both universal and reduced may not always exist. A universal reduced Gröbner basis, whenever it exists, is the closest to being *the* Gröbner basis for an ideal, and allows performing Euclidean division *carelessly*.

[11] A related characterization of *standard monomials*, which is a strictly weaker notion than Gröbner basis, was obtained much earlier by [19, 50] via determination of winning strategies of a *lex game*, and a further reinterpretation of these winning strategies using the notion of *compression* for set systems. This reinterpretation was also rediscovered independently by [51].

▶ **Corollary 11.** *The collections of evaluation vectors*

$$\left\{[\mathbb{X}^\alpha] : \alpha \in \triangle^m_{s-1}(|A|)\right\} \quad \text{and} \quad \left\{[\mathsf{D}_\mathtt{Q} \mid \mathbb{X}^\alpha] : \alpha \in \triangle^m_{s-1}(|A|)\right\}$$

*are $\mathbb{K}$-linear bases of $V_{m,s}(A)$ and $\mathsf{D}_\mathtt{Q}V_{m,s}(A)$ respectively, where*

$$\triangle^m_{s-1}(|A|) = \left\{\alpha \in \mathbb{N}^m : \left\lfloor \frac{\alpha_1}{|A|} \right\rfloor + \cdots + \left\lfloor \frac{\alpha_m}{|A|} \right\rfloor \leq s-1 \right\}.$$

## 2.3 Counting Q-roots of polynomials with multiplicities

The discussion so far naturally leads us to the question of bounding the number of Q-*roots* of a polynomial with multiplicities.

For any nonzero univariate $f(X) \in \mathbb{K}[X]$ and $a \in \mathbb{K}$, define the Q-multiplicity of $f(X)$ at $a$ by $\mu_\mathtt{Q}(f,a) = \min\left\{k \geq 0 : \mathsf{D}^k_\mathtt{Q} f(a) \neq 0\right\}$. The following claim is easy, by appealing to univariate factorization.

▶ **Proposition 12** (Easy). *For any nonempty set $A \subseteq \mathbb{F}_q^\times$, and nonzero $f(X) \in \mathbb{K}[X]$ with $\deg(f) \leq d < [3]_q$, we have $\sum_{a\in A} \mu_\mathtt{Q}(f,a) \leq d$. In particular, for any $s \geq 1$, we have $|\{a \in A : \mu_\mathtt{Q}(f,a) \geq s\}| \leq \lfloor d/s \rfloor$.*

In the multivariate setting, for any nonzero $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ and $a \in \mathbb{K}^m$, define the Q-multiplicity of $f(\mathbb{X})$ at $a$ by

$$\mu_\mathtt{Q}(f,a) = \min\left\{k \geq 0 : \text{there exists } \gamma \in \mathbb{N}^m,\ |\gamma| = k \text{ such that } \mathsf{D}^\gamma_\mathtt{Q} f(a) \neq 0\right\}.$$

In this section, we will prove the following multivariate extension of Proposition 12, which is analogous to [15, Lemma 2.7] in the setting of classical derivatives.

▶ **Theorem 13.** *For any nonempty set $A \subseteq \mathbb{F}_q^\times$, and any nonzero $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ with $\deg(f) \leq d < [3]_q$, we have*

$$\sum_{a\in A^m} \mu_\mathtt{Q}(f,a) \leq d|A|^{m-1}.$$

*In particular, for any $s \geq 1$, we have $|\{a \in A^m : \mu_\mathtt{Q}(f,a) \geq s\}| \leq \lfloor d\,|A|^{m-1}/s \rfloor$.*

Towards a proof of Theorem 13, we first consider some simple consequences of the definition of multivariate Q-multiplicity.

▶ **Lemma 14.** *Consider any nonzero $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$.*

**(a)** *For any $a \in \mathbb{K}^m$, if $\mu_\mathtt{Q}(f,a) \geq k$, then*

$$\mu_\mathtt{Q}(\mathsf{D}^\gamma_\mathtt{Q} f, a) \geq k - |\gamma| \qquad \text{for all } \gamma \in \mathbb{N}^m,\ |\gamma| \leq k.$$

**(b)** *For any $(a_1,\ldots,a_m) \in \mathbb{K}^m$ and $\gamma \in \mathbb{N}^m$, if $\mathsf{D}^\gamma_\mathtt{Q} f(a_1,\ldots,a_{m-1},X_m) \neq 0$, then*

$$\mu_\mathtt{Q}(\mathsf{D}^\gamma_\mathtt{Q} f, (a_1,\ldots,a_{m-1},a_m)) \leq \mu_\mathtt{Q}(\mathsf{D}^\gamma_\mathtt{Q} f(a_1,\ldots,a_{m-1},X_m), a_m).$$

**Proof.**

**(a)** Since $\mu_\mathtt{Q}(f,a) \geq k$, we have

$$\mathsf{D}^\gamma_\mathtt{Q} f(a) = 0 \qquad \text{for all } \gamma \in \mathbb{N}^m,\ |\gamma| \leq k-1.$$

Consider any $\gamma, \beta \in \mathbb{N}^m$, $|\gamma| \leq k$, $|\beta| \leq k - |\gamma| - 1$. So $|\beta+\gamma| \leq k-1$, and therefore $\mathsf{D}^\beta_\mathtt{Q}(\mathsf{D}^\gamma_\mathtt{Q} f)(a) = \mathsf{D}^{\beta+\gamma}_\mathtt{Q} f(a) = 0$. This means $\mu_\mathtt{Q}(\mathsf{D}^\gamma_\mathtt{Q} f, a) \geq k - |\gamma|$.

**(b)** Suppose $\mu_{\mathtt{Q}}(\mathsf{D}^{\gamma}_{\mathtt{Q}} f, (a_1, \ldots, a_{m-1}, a_m)) = k$. This means

$$\mathsf{D}^{\beta+\gamma}_{\mathtt{Q}} f(a_1, \ldots, a_{m-1}, a_m) = 0 \qquad \text{for all } \beta \in \mathbb{N}^m,\ |\beta| \leq k-1.$$

In particular, restricting our attention to $\beta \in \mathbb{N}^m$ of the form $\beta = (0^{m-1}, t)$, we get

$$\mathsf{D}^{t}_{\mathtt{Q},X_m}(\mathsf{D}^{\gamma}_{\mathtt{Q}} f)(a_1, \ldots, a_{m-1}, a_m) = 0 \qquad \text{for all } t \leq k-1.$$

This means $\mu_{\mathtt{Q}}(\mathsf{D}^{\gamma}_{\mathtt{Q}} f(a_1, \ldots, a_{m-1}, X_m), a_m) \geq k$. ◀

We can now prove Theorem 13.

**Proof of Theorem 13.** We will prove by induction on $m$. The base case $m = 1$ is true by Proposition 12. Now suppose the assertion is true for some $m \geq 1$, and now consider indeterminates $\mathbb{X} = (X_1, \ldots, X_m, X_{m+1})$. Without loss of generality, assume $\deg(f) = d$, and write

$$f(X_1, \ldots, X_m, X_{m+1}) = \sum_{t=0}^{\ell} f_t(X_1, \ldots, X_m) \cdot X_{m+1}^t, \quad \text{where } f_\ell(X_1, \ldots, X_m) \neq 0,\ \deg(f_\ell) = d - \ell.$$

For any $a_1, \ldots, a_m \in A$, denote $s_{a_1,\ldots,a_m} = \mu_{\mathtt{Q}}(f_\ell, (a_1, \ldots, a_m))$. So by induction hypothesis, we have

$$\sum_{(a_1,\ldots,a_m)\in A^m} s_{a_1,\ldots,a_m} \leq (d-\ell)|A|^{m-1}. \tag{2}$$

Now fix $a_1, \ldots, a_m \in A$, and let $\gamma = (\gamma_1, \ldots, \gamma_m) \in \mathbb{N}^m$ such that $|\gamma| = s_{a_1,\ldots,a_m}$ and $\mathsf{D}^{\gamma}_{\mathtt{Q}} f_\ell(a_1, \ldots, a_m) \neq 0$. This means

- $\mathsf{D}^{\gamma}_{\mathtt{Q}} f_\ell(X_1, \ldots, X_m) \neq 0$, and so

$$\mathsf{D}^{(\gamma,0)}_{\mathtt{Q}} f(X_1, \ldots, X_m, X_{m+1}) = \sum_{t=0}^{\ell} \mathsf{D}^{\gamma}_{\mathtt{Q}} f_t(X_1, \ldots, X_m) \cdot X_{m+1}^t \neq 0.$$

- $g^{(\gamma)}(X_{m+1}) := \mathsf{D}^{(\gamma,0)}_{\mathtt{Q}} f(a_1, \ldots, a_m, X_{m+1}) \neq 0$, and $\deg(g^{(\gamma)}) = \ell$.

Then, for any $a_{m+1} \in A$, we get

$$\begin{aligned} \mu_{\mathtt{Q}}(f, (a_1, \ldots, a_m, a_{m+1})) &\leq |(\gamma, 0)| + \mu_{\mathtt{Q}}(\mathsf{D}^{(\gamma,0)}_{\mathtt{Q}} f, (a_1, \ldots, a_m, a_{m+1})) && \text{by Lemma 14(a)} \\ &\leq s_{a_1,\ldots,a_m} + \mu_{\mathtt{Q}}(g^{(\gamma)}, a_{m+1}) && \text{by Lemma 14(b)} \end{aligned}$$

So by Proposition 12,

$$\sum_{a_{m+1}\in A} \mu_{\mathtt{Q}}(f, (a_1, \ldots, a_m, a_{m+1})) \leq s_{a_1,\ldots,a_m}|A| + \ell.$$

Then (2) implies

$$\sum_{(a_1,\ldots,a_m,a_{m+1})\in A^{m+1}} \mu_{\mathtt{Q}}(f, (a_1, \ldots, a_m, a_{m+1})) \leq (d-\ell)|A|^m + \ell|A|^m = d|A|^m,$$

which completes the induction. ◀

## 3 List decoding/recovery of $\mathtt{Q}$-multiplicity codes

We will now move to our main result on list decoding multivariate $\mathtt{Q}$-multiplicity codes. In fact, we will present the algorithm for the more general list recovery paradigm.

## 3.1 List decoding/recovery of univariate $\mathtt{Q}$-multiplicity codes

Let us see that the classical univariate multiplicity code list decoder [29] can be suitably adapted to list decode $\mathtt{Q}$-Mult$_s(A;k)$, which therefore provides an alternative algorithm to list decode FRS codes. We will, in fact, consider list recovery.

▶ **Theorem 15.** *Consider any $R \in (0,1)$, $\epsilon \in (0, 1-R)$. For any $A \subseteq \mathbb{F}_q^\times$, $|A| = n$ and $\ell \geq 1$, and for the choices $s = \lceil \ell/\epsilon^2 \rceil$ and $k = \lceil Rsn \rceil$, the code $\mathtt{Q}$-Mult$_s(A;k)$ is efficiently list recoverable up to radius $1 - R - \epsilon$ with output list size at most $(\ell/\epsilon)^{O((1+\log \ell)/\epsilon)}$.*

Consider additional indeterminates $\mathbb{Y} = (Y_0, \ldots, Y_{s-1})$, and the $\mathbb{K}$-linear subspace of the polynomial ring $\mathbb{K}[X, \mathbb{Y}]$ defined by

$$\mathsf{L}_s(X, \mathbb{Y}) = \big\{ \widetilde{P}(X) + P_0(X)Y_0 + \cdots + P_{s-1}(X)Y_{s-1} : \widetilde{P}(X), P_0(X), \ldots, P_{s-1}(X) \in \mathbb{K}[X] \big\}.$$

Also, denote $Y_s = 0$. Define a $\mathbb{K}$-linear operator $\Delta : \mathsf{L}_s(X, \mathbb{Y}) \to \mathsf{L}_s(X, \mathbb{Y})$ by

$$\Delta\bigg( \widetilde{P}(X) + \sum_{j=0}^{s-1} P_j(X) Y_j \bigg) = \mathsf{D}_\mathtt{Q} \widetilde{P}(X) + \sum_{j=0}^{s-1} \big( \mathsf{D}_\mathtt{Q} P_j(X) Y_j + P_j(\mathtt{Q}X) Y_{j+1} \big).$$

We will be interested in iterated applications of $\Delta$, and therefore, denote $\Delta^0 = \mathrm{Id}$ and $\Delta^{r+1} = \Delta \circ \Delta^r$ for all $r \geq 0$. For any $P(X, \mathbb{Y}) \in \mathsf{L}_s(X, \mathbb{Y})$ and $f(X) \in \mathbb{K}[X]$, denote $P^{[f]}(X) = P(X, f(X), \mathsf{D}_\mathtt{Q} f(X), \ldots, \mathsf{D}_\mathtt{Q}^{s-1} f(X))$. The following is immediate by the definition of $\Delta$.

▶ **Lemma 16.** *Let $P(X, \mathbb{Y}) \in \mathsf{L}_s(X, \mathbb{Y})$.*

**(a)** *If $j \in [0, s-1]$ such that $\deg_{Y_{j'}}(P) = 0$ for all $j' \geq j$, then $\deg_{Y_{j'}}(\Delta P) = 0$ for all $j' \geq j+1$.*

**(b)** *$(\Delta P)^{[f]}(X) = \mathsf{D}_\mathtt{Q}(P^{[f]})(X)$, for all $f(X) \in \mathbb{K}[X]$.*

**Proof.** Let $P(X, \mathbb{Y}) = \widetilde{P}(X) + P_0(X)Y_0 + \cdots + P_{s-1}(X)Y_{s-1} \in \mathsf{L}_s(X, \mathbb{Y})$.

**(a)** If $j \in [0, s-1]$ such that $\deg_{Y_j}(P) = 0$ for all $j' \geq j$, this means $P_j(X) = \cdots = P_{s-1}(X) = 0$. Now we have

$$\begin{aligned}(\Delta P)(X, \mathbb{Y}) &= \mathsf{D}_\mathtt{Q} \widetilde{P}(X) + \sum_{j'=0}^{s-1} \big( \mathsf{D}_\mathtt{Q} P_{j'}(X) Y_j + P_{j'}(\mathtt{Q}X) Y_{j'+1} \big) \\ &= \mathsf{D}_\mathtt{Q} \widetilde{P}(X) + \sum_{j'=0}^{s-1} \big( P_{j'-1}(\mathtt{Q}X) + \mathsf{D}_\mathtt{Q} P_{j'}(X) \big) Y_{j'}.\end{aligned}$$

So, $P_{j'-1}(\mathtt{Q}X) + \mathsf{D}_\mathtt{Q} P_{j'}(X) = 0$ for all $j' \geq j+1$. This means $\deg_{Y_{j'}}(\Delta P) = 0$ for all $j' \geq j+1$.

**(b)** We have

$$\begin{aligned}(\Delta P)^{[f]}(X) &= \mathsf{D}_\mathtt{Q} \widetilde{P}(X) + \sum_{j=0}^{s-1} \big( \mathsf{D}_\mathtt{Q} P_j(X) \mathsf{D}_\mathtt{Q}^j f(X) + P_j(\mathtt{Q}X) \mathsf{D}_\mathtt{Q}^{j+1} f(X) \big) \\ &= \mathsf{D}_\mathtt{Q} \widetilde{P}(X) + \sum_{j=0}^{s-1} \mathsf{D}_\mathtt{Q} \big( P_j \cdot \mathsf{D}_\mathtt{Q}^j f \big)(X) \qquad \text{by Proposition 6(c)} \\ &= \mathsf{D}_\mathtt{Q} P^{[f]}(X).\end{aligned}$$

◀

It is worth noting that a close variant of the operator $\Delta$ appears in [24, Definition 8.1] in the context of nearly linear-time list decoding of FRS codes, without the interpretation in terms of $\mathtt{Q}$-derivatives. So it is reasonable to surmise that a nearly linear-time implementation of the list decoding algorithm à la [24] is possible for the univariate $\mathtt{Q}$-multiplicity codes. In order to keep our main presentation short, we limit ourselves here to adapting the more conventional polynomial-time algorithm of [29].

The interpolation step of the list recovery algorithm, which will be used multiple times in this discussion, can be captured as follows.

▶ **Proposition 17.** *Consider any $A = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_q^\times$, parameters $s \geq r \geq 1$, and $k \in [s|A|]$. Let $\ell \geq 1$, and define*

$$d = \left\lceil \frac{n\ell(s-r+1) - (r+k) + 1}{r+1} \right\rceil.$$

*Then for any $S_1, \ldots, S_n \subseteq \mathbb{K}^s$ with $|S_i| \leq \ell$, $i \in [n]$, there exists a nonzero polynomial $P(X, \mathbb{Y}) = \widetilde{P}(X) + \sum_{j=0}^{r-1} P_j(X) Y_j \in \mathsf{L}_s(X, \mathbb{Y})$ with*

$$\deg(\widetilde{P}) \leq d + k - 1, \quad \textit{and} \quad \deg(P_j) \leq d \qquad \textit{for all } j \in [0, r-1],$$

*such that for any $f(X) \in \mathbb{K}[X]$, $\deg(f) < k$,*

$$\textit{if} \quad \mathsf{d}_A^{(s)}(f, S) \geq \frac{\ell}{r+1} + \frac{k}{(s-r+1)n} \qquad \textit{then} \quad P(X, f(X), \mathsf{D}_{\mathtt{Q}} f(X), \ldots, \mathsf{D}_{\mathtt{Q}}^{s-1} f(X)) = 0.$$

**Proof.** Assume the notation $u = (u^{(0)}, \ldots, u^{(s-1)}) \in \mathbb{K}^s$. We can, in fact, add additional arbitrary elements and assume $|S_i| = \ell$, for all $i \in [n]$. Also enumerate $S_i = \{w_{i,1}, \ldots, w_{i,\ell}\}$, $i \in [n]$. We will construct a nonzero polynomial $P(X, \mathbb{Y}) = \widetilde{P}(X) + \sum_{j=0}^{s-1} P_j(X) Y_j \in \mathsf{L}_s(X, \mathbb{Y})$ such that

**(a)** $P(X, \mathbb{Y}) = \widetilde{P}(X) + \sum_{j=0}^{r-1} P_j(X) Y_j \in \mathsf{L}_s(X, \mathbb{Y})$, that is, $P_r(X) = \cdots = P_{s-1}(X) = 0$.

**(b)** $\deg(\widetilde{P}) \leq d + k - 1$, and $\deg(P_j) \leq d$ for all $j \in [0, r-1]$.

**(c)** $(\Delta^j P)\big(\alpha_i, w_{i,t}^{(0)}, \ldots, w_{i,t}^{(s-1)}\big) = 0$ for all $j \in [0, s-r]$, $t \in [\ell]$, $i \in [n]$.

The number of linear constraints is $n\ell(s-r+1)$, and the number of coefficients is $d + k + r(d+1) = d(r+1) + (r+k)$. So for the choice

$$d = \left\lceil \frac{n\ell(s-r+1) - (r+k) + 1}{r+1} \right\rceil,$$

we indeed have $d(r+1) + (r+k) > n\ell(s-r+1)$, and this ensures a nontrivial solution, that is, $P(X, \mathbb{Y}) \neq 0$.

Now consider any $f(X) \in \mathbb{K}[X]$, and suppose $\mathsf{d}_A^{(s)}(f, S) = 1 - (\nu/n)$. By Lemma 16, this implies $\sum_{a \in A} \mu_{\mathtt{Q}}(P^{[f]}, a) \geq \nu s - r + 1$. But we also have $\deg(P^{[f]}) \leq d + k - 1$. Therefore, by Proposition 12, we can conclude that $P^{[f]}(X) = 0$ if $\nu > \lceil (d+k-1)/(s-r+1) \rceil$. This is equivalent to

$$\nu > \left\lceil \frac{\left\lceil \frac{n\ell(s-r+1)-(r+k)+1}{r+1} \right\rceil + k - 1}{s-r+1} \right\rceil = \left\lceil \frac{n\ell(s-r+1) - (r+k) + (r+1)(k-1) + 1}{(r+1)(s-r+1)} \right\rceil.$$

The above is true if

$$\nu \geq \frac{n\ell}{r+1} + \frac{k}{s-r+1}, \quad \text{that is,} \quad \frac{\nu}{n} \geq \frac{\ell}{r+1} + \frac{k}{(s-r+1)n}.$$ ◀

Once we have an interpolating polynomial that captures the correct codewords, we can extract the output list as follows.

▶ **Proposition 18.** *Consider parameters $s \geq r \geq 1$, and $k, d \geq 1$ such that $d + k - 1 < [3]_q$. If $P(X, \mathbb{Y}) = \widetilde{P}(X) + \sum_{j=0}^{r-1} P_j(X) Y_j \in \mathsf{L}_s(X, \mathbb{Y})$ is a nonzero polynomial with*

$$\deg(\widetilde{P}) \leq d + k - 1, \quad \textit{and} \quad \deg(P_j) \leq d \qquad \textit{for all } j \in [0, r-1],$$

*then the solution space*

$$\{f(X) \in \mathbb{K}[X] : P^{[f]}(X) = 0\}$$

*is an affine $\mathbb{K}$-linear space with dimension at most $r - 1$.*

**Proof.** Consider any $f(X) \in \mathbb{K}[X]$ satisfying $P^{[f]}(X) = 0$. Note that we have $P(X, \mathbb{Y}) \neq 0$. If $P_j(X) = 0$ for all $j \in [0, r-1]$, then $P^{[f]}(X) = \widetilde{P}(X) = 0$, which means $P(X, \mathbb{Y}) = 0$, a contradiction. So there exists $j \in [0, r-1]$ such that $P_j(X) \neq 0$. Without loss of generality, we assume $P_{r-1}(X) \neq 0$. (Otherwise, we work with the largest $r'$ such that $P_{r'-1}(X) \neq 0$.)

Let us also quickly consider another notation. For any $\mathtt{Q}^b \in \mathbb{K}^\times$, $h \geq 0$, and $g(X) \in \mathbb{K}[X]$, denote

$$g_{h,b} := \mathrm{coeff}\left( \frac{(X - \mathtt{Q}^b)_{\mathtt{Q}}^{(h)}}{[h]_{\mathtt{Q}}!}, g \right) = \mathsf{D}_{\mathtt{Q}}^h g(\mathtt{Q}^b) \qquad \text{by Proposition 6(b)}$$

Recall that $\mathbb{K} = \mathbb{F}_{q^3}$. Since $\deg(P_{r-1}) \leq d < [3]_q$, there exists $\mathtt{Q}^b \in \mathbb{K}^\times$ such that $P_{r-1}(\mathtt{Q}^{h+b}) \neq 0$ for all $h \in [0, d+k-1]$. Further, since $\deg(P) \leq d + k - 1 < [3]_q$, we will work with the basis of monomials $\{(X - \mathtt{Q}^b)_{\mathtt{Q}}^{(h)} : h \in [0, d+k-1]\}$. Now we have

$$P^{[f]}(X) \equiv \widetilde{P}(X) + P_0(X) f(X) + P_1(X) \mathsf{D}_{\mathtt{Q}} f(X) + \cdots + P_{r-1}(X) \mathsf{D}_{\mathtt{Q}}^{r-1} f(X) = 0$$

So by Proposition 6(c), for every $h \in [0, d+k-1]$, we have

$$\begin{aligned} 0 = P_{h,b}^{[f]} &= (\widetilde{P})_{h,b} + \sum_{j=0}^{r-1} \sum_{c=0}^{h} \begin{bmatrix} h \\ c \end{bmatrix}_{\mathtt{Q}} (P_j)_{h-c,c+b} (\mathsf{D}_{\mathtt{Q}}^j f)_{c,b} \\ &= (\widetilde{P})_{h,b} + \sum_{j=0}^{r-1} \sum_{c=0}^{h} \begin{bmatrix} h \\ c \end{bmatrix}_{\mathtt{Q}} (P_j)_{h-c,c+b} f_{c+j,b}. \end{aligned}$$

Now for every $h \in [0, d+k-1]$, since $(P_{r-1})_{0,h+b} = P_{r-1}(\mathtt{Q}^{h+b}) \neq 0$, we can rewrite the above

$$f_{h+r-1,b} = -\frac{1}{(P_{r-1})_{0,h+b}} \left( (\widetilde{P})_{h,b} + \sum_{\substack{(j,c) \leq (r-1,h) \\ (j,c) \neq (r-1,h)}} \begin{bmatrix} h \\ c \end{bmatrix}_{\mathtt{Q}} (P_j)_{h-c,c+b} f_{c+j,b} \right).$$

So we can set the undetermined coefficients among $f_{0,b}, \ldots, f_{r-2,b} \in \mathbb{K}$ freely, and the remaining coefficients of $f(X)$ are uniquely determined the above equation. This means the solution space is an affine $\mathbb{K}$-linear space having dimension at most $r - 1$. ◀

The final list recovery result can now be proven.

**Proof of Theorem 15.** Choosing $r = \lceil \ell/\epsilon \rceil$, and plugging in all the parameters into Proposition 17 and Proposition 18 immediately implies that the output list is contained in an affine $\mathbb{K}$-linear space with dimension at most $\lceil \ell/\epsilon \rceil - 1$. The pruning algorithm with the improved analysis [44, 66] then asserts that the output list size is at most $(\ell/\epsilon)^{O((1+\log \ell)/\epsilon)}$. ◀

## 3.2 List decoding/recovery of multivariate $\mathtt{Q}$-multiplicity codes

We will now see an algorithm to list decode $\mathtt{Q}\text{-Mult}_{m,s}(A;k)$. Even though it is inspired by the classical multivariate multiplicity code list decoder [9], it turns out that we can give a simpler algorithm and analysis that is perhaps the correct multivariate extension of our list decoder in the univariate case. We will, in fact, perform list recovery, and the main theorem statement is the following.

▶ **Theorem 19.** *Consider any $\delta \in (0,1)$, $\epsilon \in (0, 1-\delta)$. For any $A \subseteq \mathbb{F}_q^\times$ and $\ell \geq 1$, and for the choices $s = O(\ell/\epsilon^{2m+1})$ and $k = \lceil (1-\delta)s|A| \rceil$, the code $\mathtt{Q}\text{-Mult}_s^m(A;k)$ is efficiently list recoverable up to radius $\delta - \epsilon$ with output list contained in a $\mathbb{K}$-affine space of dimension atmost $O(\ell^m/\epsilon^{2m})$.*

Note that setting $\ell = 1$ in Theorem 19 gives Theorem 2.

Consider additional indeterminates $\mathbb{Y} = (Y_\gamma)_{|\gamma|<s}$, $\mathbf{Z} = (Z_1, \ldots, Z_m)$, and the $\mathbb{K}$-linear subspace of the polynomial ring $\mathbb{K}[\mathbb{X}, \mathbb{Y}]$ defined by

$$\mathsf{L}_s(\mathbb{X}, \mathbb{Y}) = \left\{ \widetilde{P}(\mathbb{X}) + \sum_{j=0}^{s-1} P_j(\mathbb{X}) \left( \sum_{|\gamma|=j} Y_\gamma \mathbf{Z}^\gamma \right) \in \mathbb{K}(\mathbf{Z})[\mathbb{X}, \mathbb{Y}] \right\}.$$

Also, denote $Y_\gamma = 0$ for all $\gamma \in \mathbb{N}^m$, $|\gamma| \geq s$. For any $\alpha \in \mathbb{N}^m$, define a $\mathbb{K}$-linear operator $\Delta^{(\alpha)} : \mathsf{L}_s(\mathbb{X}, \mathbb{Y}) \to \mathsf{L}_s(\mathbb{X}, \mathbb{Y})$ by

$$\Delta^{(\alpha)} \left( \widetilde{P}(\mathbb{X}) + \sum_{j=0}^{s-1} P_j(\mathbb{X}) \left( \sum_{|\gamma|=j} Y_\gamma \mathbf{Z}^\gamma \right) \right) = \mathsf{D}_\mathtt{Q}^\alpha \widetilde{P}(\mathbb{X}) + \sum_{j=0}^{s-1} \sum_{|\gamma|=j} \left( \sum_{\beta \leq \alpha} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_\mathtt{Q} \mathsf{D}_\mathtt{Q}^{\alpha-\beta} P_j(\mathtt{Q}^\beta \mathbb{X}) Y_{\beta+\gamma} \right) \mathbf{Z}^\gamma.$$

For any $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) \in \mathsf{L}_s(\mathbb{X}, \mathbb{Y})$ and $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$, denote

$$P^{[f]}(\mathbb{X}) = P\left( \mathbb{X}, \left( \mathsf{D}_\mathtt{Q}^\gamma f(\mathbb{X}) \right)_{|\gamma|<s}, \mathbf{Z} \right) \in \mathbb{K}(\mathbf{Z})[\mathbb{X}].$$

The following is then immediate.

▶ **Lemma 20.** *Let $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) \in \mathsf{L}_s(\mathbb{X}, \mathbb{Y})$.*

**(a)** *If $j \in [0, s-1]$ such that $\deg_{Y_\gamma}(P) = 0$ for all $\gamma \in \mathbb{N}^m$, $|\gamma| \geq j$, then $\deg_{Y_\gamma}(\Delta^{(\alpha)} P) = 0$ for all $\gamma \in \mathbb{N}^m$, $|\gamma| \geq j + |\alpha|$.*

**(b)** *$(\Delta^{(\alpha)} P)^{[f]}(\mathbb{X}) = \mathsf{D}_\mathtt{Q}^\alpha (P^{[f]})(\mathbb{X})$, for all $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$.*

▶ Remark 21. A consequence of Lemma 20 is that $\Delta^{(\alpha+\beta)} = \Delta^{(\alpha)} \circ \Delta^{(\beta)}$ for all $\alpha, \beta \in \mathbb{N}^m$. We do not explicitly use this elsewhere.

**Proof of Lemma 20.** Let $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) = \widetilde{P}(\mathbb{X}) + \sum_{j=0}^{s-1} P_j(\mathbb{X}) \left( \sum_{|\gamma|=j} Y_\gamma \mathbf{Z}^\gamma \right) \in \mathsf{L}_s(\mathbb{X}, \mathbb{Y})$.

**(a)** If $j \in [0, s-1]$ such that $\deg_{Y_\gamma}(P) = 0$ for all $\gamma \in \mathbb{N}^m$, $|\gamma| \geq j$, this means $P_{j'}(\mathbb{X}) = 0$ for all $j' \geq j$. Now we have

$$\begin{aligned}
(\Delta^{(\alpha)} P)(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) &= \mathsf{D}_\mathtt{Q}^\alpha \widetilde{P}(\mathbb{X}) + \sum_{j'=0}^{s-1} \sum_{|\gamma|=j'} \left( \sum_{\beta \leq \alpha} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_\mathtt{Q} \mathsf{D}_\mathtt{Q}^{\alpha-\beta} P_{j'}(\mathtt{Q}^\beta \mathbb{X}) Y_{\beta+\gamma} \right) \mathbf{Z}^\gamma \\
&= \mathsf{D}_\mathtt{Q}^\alpha \widetilde{P}(\mathbb{X}) + \sum_{j'=0}^{s-1} \sum_{|\gamma|=j'} \left( \sum_{\beta \leq \alpha} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_\mathtt{Q} \mathsf{D}_\mathtt{Q}^{\alpha-\beta} P_{j'-|\beta|}(\mathtt{Q}^\beta \mathbb{X}) \mathbf{Z}^{\gamma-\beta} \right) Y_\gamma
\end{aligned}$$

So, $\sum_{\beta \leq \alpha} \mathsf{D}_\mathtt{Q}^{\alpha-\beta} P_{j'-|\beta|}(\mathtt{Q}^\beta \mathbb{X}) \mathbf{Z}^{\gamma-\beta} = 0$ for all $j' \geq j + |\alpha|$. This means $\deg_{Y_{j'}}(\Delta^{(\alpha)} P) = 0$ for all $j' \geq j + |\alpha|$.

**(b)** We have

$$\begin{aligned}(\Delta^{(\alpha)}P)^{[f]}(\mathbb{X}) &= \mathsf{D}_{\mathtt{Q}}^{\alpha}\widetilde{P}(\mathbb{X}) + \sum_{j=0}^{s-1}\sum_{|\gamma|=j}\Big(\sum_{\beta\le\alpha}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}_{\mathtt{Q}}\mathsf{D}_{\mathtt{Q}}^{\alpha-\beta}P_j(\mathtt{Q}^{\beta}\mathbb{X})\mathsf{D}_{\mathtt{Q}}^{\beta+\gamma}f(\mathbb{X})\Big)\mathbf{Z}^{\gamma}\\ &= \mathsf{D}_{\mathtt{Q}}^{\alpha}\widetilde{P}(\mathbb{X}) + \sum_{j=0}^{s-1}\sum_{|\gamma|=j}\mathsf{D}_{\mathtt{Q}}^{\alpha}\big(P_j\cdot\mathsf{D}_{\mathtt{Q}}^{\gamma}f\big)(\mathbb{X})\mathbf{Z}^{\gamma} \qquad \text{by Proposition 8(d)}\\ &= \mathsf{D}_{\mathtt{Q}}^{\alpha}(P^{[f]})(\mathbb{X}).\end{aligned}$$

◀

The interpolation step of the list recovery algorithm, which will be used multiple times in this discussion, can be captured as follows.

▶ **Proposition 22.** *Consider any $A\subseteq\mathbb{F}_q^{\times}$, parameters $s\ge r\ge 1$, and $k\in[s|A|]$. Let $\ell\ge 1$, and define*

$$d=\left\lceil 5\Big(\frac{\ell}{r+1}\Big)^{1/m}(s-r+1)|A|\right\rceil.$$

*Then for any $S_a\subseteq\mathbb{K}^{\binom{m+s-1}{s-1}}$ with $|S_a|\le\ell$, $a\in A^m$, there exists a nonzero polynomial $P(\mathbb{X},\mathbb{Y},\mathbf{Z})=\widetilde{P}(\mathbb{X})+\sum_{j=0}^{r-1}P_j(\mathbb{X})\sum_{|\gamma|=j}Y_{\gamma}\mathbf{Z}^{\gamma}\in\mathsf{L}_s(\mathbb{X},\mathbb{Y})$ with*

$$\deg(\widetilde{P})\le d+k-1,\quad \textit{and}\quad \deg(P_j)\le d\qquad \textit{for all } j\in[0,r-1].$$

*such that for any $f(\mathbb{X})\in\mathbb{K}[\mathbb{X}]$, $\deg(f)<k$,*

$$\textit{if}\quad \mathsf{d}_A^{(m,s)}(f,S)\ge 5\Big(\frac{\ell}{r+1}\Big)^{1/m}+\frac{k}{(s-r+1)|A|^{m-1}}.\qquad \textit{then}\quad P^{[f]}(\mathbb{X})=0.$$

*Moreover, we can ensure that $P(\mathbb{X},\mathbb{Y},\mathbf{Z})$ is a polynomial in $\mathbf{Z}$ with $\deg_{\mathbf{Z}}(P)<ms$.*

**Proof.** Assume the notation $u=(u^{(\gamma)}:|\gamma|<s)\in\mathbb{K}^{\binom{m+s-1}{s-1}}$. We can, in fact, add additional arbitrary elements and assume $|S_a|=\ell$, for all $a\in A^m$. Also enumerate $S_a=\{w_{a,1},\dots,w_{a,\ell}\}$, $a\in A^m$. We will construct a nonzero polynomial $P(\mathbb{X},\mathbb{Y},\mathbf{Z})=\widetilde{P}(\mathbb{X})+\sum_{j=0}^{s-1}P_j(\mathbb{X})\big(\sum_{|\gamma|=j}Y_{\gamma}\mathbf{Z}^{\gamma}\big)\in\mathsf{L}_s(\mathbb{X},\mathbb{Y})$ such that

**(a)** $P(\mathbb{X},\mathbb{Y},\mathbf{Z})=\widetilde{P}(\mathbb{X})+\sum_{j=0}^{r-1}P_j(\mathbb{X})\big(\sum_{|\gamma|=j}Y_{\gamma}\mathbf{Z}^{\gamma}\big)$, that is, $P_r(\mathbb{X})=\cdots=P_{s-1}(\mathbb{X})=0$.

**(b)** $\deg(\widetilde{P})\le d+k-1$, and $\deg(P_j)\le d$ for all $j\in[0,r-1]$.

**(c)** $(\Delta^{(\alpha)}P)\Big(a,\big(w_{a,t}^{(\gamma)}\big)_{|\gamma|<s}\Big)=0$ for all $\alpha\in\mathbb{N}^m$ with $|\alpha|\in[0,s-r]$, $t\in[\ell]$, $a\in A^m$.

The number of linear constraints is

$$|A|^m\ell\binom{m+s-r}{s-r}\le\ell\Big(\frac{5(s-r+1)|A|}{m}\Big)^m,$$

and the number of coefficients is

$$\binom{m+d+k-1}{d+k-1}+r\binom{m+d}{d}\ge(r+1)\binom{m+d}{d}\ge(r+1)\Big(\frac{d}{m}\Big)^m.$$

So for the choice

$$d=\left\lceil 5\Big(\frac{\ell}{r+1}\Big)^{1/m}(s-r+1)|A|\right\rceil,$$

we indeed get a nontrivial solution, that is, $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) \neq 0$. Further, since each linear constraint is a polynomial in $\mathbf{Z} = (Z_1, \ldots, Z_m)$ having degree at most $s-1$, we can ensure that $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z})$ is a polynomial in $\mathbf{Z}$ having $\deg_{\mathbf{Z}}(P) < ms$ (see [38] or [9, Lemma 3].)

Now consider any $f(X) \in \mathbb{K}[X]$, and suppose $\mathsf{d}_A^{(m,s)}(f, S) = 1-(\nu/|A|^{m-1})$. By Lemma 20, this implies $\sum_{a \in A^m} \mu_{\mathtt{Q}}(P^{[f]}, a) \geq \nu(s-r+1)$. But we also have $\deg(P^{[f]}) \leq (d+k-1)|A|^{m-1}$. Therefore, by Theorem 13, we can conclude that $P^{[f]}(\mathbb{X}) = 0$ if $\nu > (d+k-1)|A|^{m-1}/(s-r+1)$, which holds if

$$\nu > \left\lceil \frac{5(\ell/(r+1))^{1/m}(s-r+1)|A|^{m-1} + k - 1}{s-r+1} \right\rceil.$$

The above is true if

$$\nu \geq 5\left(\frac{\ell}{r+1}\right)^{1/m} |A|^{m-1} + \frac{k}{s-r+1},$$

$$\text{that is,} \quad \frac{\nu}{|A|^{m-1}} \geq 5\left(\frac{\ell}{r+1}\right)^{1/m} + \frac{k}{(s-r+1)|A|^{m-1}}. \qquad \blacktriangleleft$$

Once we have an interpolating polynomial that captures the correct codewords, we can extract the output list as follows.

▶ **Proposition 23.** *Consider parameters $s \geq r \geq 1$, and $k, d \geq 1$ such that $d + k - 1 < [3]_q$. If $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) = \widetilde{P}(\mathbb{X}) + \sum_{j=0}^{r-1} P_j(\mathbb{X}) \sum_{|\gamma|=j} Y_\gamma \mathbf{Z}^\gamma \in \mathsf{L}_s(\mathbb{X}, \mathbb{Y}, \mathbf{Z})$ is a nonzero polynomial with*

$$\deg(\widetilde{P}) \leq d + k - 1, \quad \textit{and} \quad \deg(P_j) \leq d \qquad \textit{for all } j \in [0, r-1],$$

*then the solution space*

$$\{f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}] : P^{[f]}(\mathbb{X}) = 0\}$$

*is an affine $\mathbb{K}$-linear space with dimension at most $\binom{m+r-2}{r-2}$.*

**Proof.** Consider any $f(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$ satisfying $P^{[f]}(\mathbb{X}) = 0$. Note that we have $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) \neq 0$. If $P_j(\mathbb{X}) = 0$ for all $j \in [0, r-1]$, then $P^{[f]}(\mathbb{X}) = \widetilde{P}(\mathbb{X}) = 0$, which means $P(\mathbb{X}, \mathbb{Y}, \mathbf{Z}) = 0$, a contradiction. So there exists $j \in [0, r-1]$ such that $P_j(\mathbb{X}) \neq 0$. Without loss of generality, we assume $P_{r-1}(\mathbb{X}) \neq 0$. (Otherwise, we work with the largest $r'$ such that $P_{r'-1}(\mathbb{X}) \neq 0$.)

Let us also quickly consider another notation. For any $\mathtt{Q}^\beta \in (\mathbb{K}^\times)^m$, $\alpha \in \mathbb{N}^m$, and $g(\mathbb{X}) \in \mathbb{K}[\mathbb{X}]$, denote

$$g_{\alpha,\beta} := \operatorname{coeff}\left(\frac{(\mathbb{X} - \mathtt{Q}^\beta)_{\mathtt{Q}}^{(\alpha)}}{[\alpha]_{\mathtt{Q}}!}, g\right) = \mathsf{D}_{\mathtt{Q}}^\alpha g(\mathtt{Q}^\beta) \qquad \text{by Proposition 8(b)}$$

Recall that $\mathbb{K} = \mathbb{F}_{q^3}$. Since $\deg(P_{r-1}) \leq d < [3]_q$, there exists $\mathtt{Q}^\beta \in (\mathbb{K}^\times)^m$ such that $P_{r-1}(\mathtt{Q}^{\alpha+\beta}) \neq 0$ for all $\alpha \in \mathbb{N}^m$, $|\alpha| \leq d+k-1$. Further, since $\deg(P) \leq d+k-1 < [3]_q$, we will work with the basis of monomials $\{(\mathbb{X} - \mathtt{Q}^\beta)_{\mathtt{Q}}^{(\alpha)} : \alpha \in \mathbb{N}^m, |\alpha| \leq d+k-1\}$. Now we have

$$P^{[f]}(\mathbb{X}) \equiv \widetilde{P}(\mathbb{X}) + \sum_{j=0}^{r-1} P_j(\mathbb{X}) \sum_{|\gamma|=j} \mathsf{D}_{\mathtt{Q}}^\gamma f(\mathbb{X}) \mathbf{Z}^\gamma = 0.$$

So for every $\alpha \in \mathbb{N}^m$, $|\alpha| \leq d+k-1$, we have

$$\begin{aligned} 0 = P_{\alpha,\beta}^{[f]} &= \widetilde{P}_{\alpha,\beta} + \sum_{j=0}^{r-1} \sum_{|\gamma|=j} \left( \sum_{\theta \leq \alpha} \begin{bmatrix} \alpha \\ \theta \end{bmatrix}_{\mathtt{Q}} (P_j)_{\alpha-\theta,\theta+\beta} \left(\mathsf{D}_{\mathtt{Q}}^\gamma f\right)_{\theta,\beta} \mathbf{Z}^\gamma \right) \\ &= \widetilde{P}_{\alpha,\beta} + \sum_{j=0}^{r-1} \sum_{\theta \leq \alpha} \begin{bmatrix} \alpha \\ \theta \end{bmatrix}_{\mathtt{Q}} (P_j)_{\alpha-\theta,\theta+\beta} \left( \sum_{|\gamma|=j} f_{\theta+\gamma,\beta} \mathbf{Z}^\gamma \right). \end{aligned}$$

Now for every $\alpha \in \mathbb{N}^m$, $|\alpha| \leq d+k-1$, since $P_{r-1}(\mathtt{Q}^{\alpha+\beta}) = (P_{r-1})_{0^m,\alpha+\beta} \neq 0$, we can rewrite the above as

$$\sum_{|\gamma|=r-1} f_{\alpha+\gamma,\beta}\mathbf{Z}^\gamma$$
$$= -\frac{1}{(P_{r-1})_{0^m,\alpha+\beta}}\left((\widetilde{P})_{\alpha,\beta} + \sum_{\substack{(j,\theta)\leq(r-1,\alpha)\\(j,\theta)\neq(r-1,\alpha)}} \begin{bmatrix}\alpha\\ \theta\end{bmatrix}_{\mathtt{Q}} (P_j)_{\alpha-\theta,\theta+\beta}\left(\sum_{|\gamma|=j} f_{\theta+\gamma,\beta}\mathbf{Z}^\gamma\right)\right) \tag{3}$$

So we can set the undetermined coefficients among $f_{\gamma,\beta} \in \mathbb{K}$, $|\gamma| \leq r-2$ freely, and the remaining coefficients of $f(\mathbb{X})$ are uniquely determined the above equation. This means the solution space is an affine $\mathbb{K}$-linear space having dimension at most $\binom{m+r-2}{r-2}$. Further, at any instance of (3), if we know the R.H.S. and determine the L.H.S., then each coefficient $f_{\alpha+\gamma,\beta}$ can be recovered by instantiating an arbitrary finite grid $S^m$ with $S \subseteq \mathbb{K}$, $|S| \geq ms$ as a hitting set for the $\mathbf{Z}$-variables, since we have $\deg_{\mathbf{Z}}(P) < ms$. ◀

We are now ready to complete the proof of our main theorem.

**Proof of Theorem 19.** Choosing $r = O(\ell/\epsilon^m)$, and plugging in all the parameters into Proposition 17 and Proposition 18 immediately proves the claim. ◀

## References


1 Noga Alon. Combinatorial Nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999. doi:10.1017/S0963548398003411.

2 Omar Alrabiah, Venkatesan Guruswami, and Ray Li. Randomly Punctured Reed–Solomon Codes Achieve List-Decoding Capacity over Linear-Sized Fields. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, pages 1458–1469, New York, NY, USA, 2024. Association for Computing Machinery. doi:10.1145/3618260.3649634.

3 G.E. Andrews. *q-Series: Their Development and Application in Analysis, Number Theory, Combinatorics, Physics and Computer Algebra*, volume 66 of *CBMS Regional Conference Lecture Series in Mathematics*. AMS, 1986.

4 M.H. Annaby and Z.S. Mansour. $q$-Taylor and interpolation series for Jackson $q$-difference operators. *Journal of Mathematical Analysis and Applications*, 344(1):472–483, 2008. doi:10.1016/j.jmaa.2008.02.033.

5 László Babai, Lance Fortnow, Leonid A. Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*, STOC '91, pages 21–32, New York, NY, USA, 1991. Association for Computing Machinery. doi:10.1145/103418.103428.

6 Simeon Ball and Oriol Serra. Punctured combinatorial nullstellensätze. *Combinatorica*, 29(5):511–522, 2009. doi:10.1007/s00493-009-2509-z.

7 Eli Ben-Sasson, Swastik Kopparty, and Jaikumar Radhakrishnan. Subspace Polynomials and Limits to List Decoding of Reed–Solomon Codes. *IEEE Transactions on Information Theory*, 56(1):113–120, 2010. doi:10.1109/TIT.2009.2034780.

8 Siddharth Bhandari, Prahladh Harsha, Mrinal Kumar, and Ashutosh Shankar. Algorithmizing the Multiplicity Schwartz-Zippel Lemma. In Nikhil Bansal and Viswanath Nagarajan, editors, *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22-25, 2023*, pages 2816–2835. SIAM, 2023. doi:10.1137/1.9781611977554.ch106.

9 Siddharth Bhandari, Prahladh Harsha, Mrinal Kumar, and Madhu Sudan. Decoding Multivariate Multiplicity Codes on Product Sets. *IEEE Transactions on Information Theory*, 70(1):154–169, 2024. doi:10.1109/TIT.2023.3306849.

10 George Boole. *A Treatise on the Calculus of Finite Differences*. MacMillan and Co., 1860. Reprint: Cambridge University Press, 2009. doi:10.1017/CBO9780511693014.

11 Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Generic Reed-Solomon Codes Achieve List-Decoding Capacity. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, pages 1488–1501, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3564246.3585128.

12 Yeyuan Chen and Zihan Zhang. Explicit Folded Reed-Solomon and Multiplicity Codes Achieve Relaxed Generalized Singleton Bound. *arXiv Preprint*, 2024. doi:10.48550/arXiv.2408.15925.

13 David Cox, John Little, and Donald O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

14 P. Delsarte, J.M. Goethals, and F.J. Mac Williams. On generalized Reed Muller codes and their relatives. *Information and Control*, 16(5):403–442, 1970. doi:10.1016/S0019-9958(70)90214-7.

15 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. doi:10.1137/100783704.

16 Peter Elias. *List Decoding for Noisy Channels*. Ph.d. thesis, Massachusetts Institute of Technology, 1957. RLE Technical Report No. 335. http://hdl.handle.net/1721.1/4484.

17 Thomas Ernst. *A Comprehensive Treatment of q-Calculus*. Birkhäuser Basel, 2012. doi:10.1007/978-3-0348-0431-8.

18 H. Exton. *q-Hypergeometric Functions and Applications*. Halsted Press, Chichister, 1983.

19 Bálint Felszeghy, Balázs Ráth, and Lajos Rónyai. The lex game and some applications. *Journal of Symbolic Computation*, 41(6):663–681, 2006. doi:10.1016/j.jsc.2005.11.003.

20 Dominique Foata and Guo-Niu Han. The $q$-Series in Combinatorics: Permutation Statistics (Lecture addendums, revised version). *Unpublished*, 2021. Available at https://irma.math.unistra.fr/~foata/paper/pub91.pdf.

21 George Gasper and Mizan Rahman. *Basic Hypergeometric Series*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 2004. doi:10.1017/CBO9780511526251.

22 Carl Friedrich Gauß. *Summatio quarumdam serierum singularium*. Dieterich, 1808. Digitized version available at http://eudml.org/doc/203313.

23 O. Geil and U. Martínez-Peñas. Bounding the Number of Common Zeros of Multivariate Polynomials and their Consecutive Derivatives. *Combinatorics, Probability and Computing*, 28(2):253–279, 2019. doi:10.1017/S0963548318000342.

24 Rohan Goyal, Prahladh Harsha, Mrinal Kumar, and Ashutosh Shankar. Fast list-decoding of univariate multiplicity and folded Reed-Solomon codes. *arXiv Preprint*, 2023. doi:10.48550/arXiv.2311.17841.

25 Zeyu Guo, Mrinal Kumar, Ramprasad Saptharishi, and Noam Solomon. Derandomization from algebraic hardness. *SIAM Journal on Computing*, 51(2):315–335, 2022. doi:10.1137/20M1347395.

26 Zeyu Guo and Zihan Zhang. Randomly Punctured Reed-Solomon Codes Achieve the List Decoding Capacity over Polynomial-Size Alphabets. *arXiv Preprint*, 2023. doi:10.48550/arXiv.2304.01403.

27 V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 28–37, 1998. doi:10.1109/SFCS.1998.743426.

28 Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008. doi:10.1109/TIT.2007.911222.

29 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. doi:10.1109/TIT.2013.2246813.

30 Wolfgang Hahn. Über Orthogonalpolynome, die $q$-Differenzengleichungen genügen. *Mathematische Nachrichten*, 2(1-2):4–34, 1949. doi:10.1002/mana.19490020103.

31 F. H. Jackson. A $q$-form of Taylor's theorem. *Messenger of Mathematics*, 38:62–64, 1909.

32 F. H. Jackson. A $q$-series corresponding to Taylor's series. *Messenger of Mathematics*, 39:26–28, 1909.

33 F. H. Jackson. On $q$-Functions and a certain Difference Operator. *Transactions of the Royal Society of Edinburgh*, 46(2):253–281, 1909. doi:10.1017/S0080456800002751.

34 F. H. Jackson. On $q$-Definite Integrals. *The Quarterly Journal of Pure and Applied Mathematics*, 41:193–203, 1910.

35 F. H. Jackson. $q$-Difference Equations. *American Journal of Mathematics*, 32(4):305–314, 1910. doi:10.2307/2370183.

36 Charles Jordan. *Calculus of Finite Differences*. Chelsea Publishing Company, New York, 2nd edition, 1950.

37 Victor Kac and Pokman Cheung. *Quantum Calculus*. Springer New York, NY, 2002. doi:10.1007/978-1-4613-0071-7.

38 R. Kannan. Solving systems of linear equations over polynomials. *Theoretical Computer Science*, 39:69–88, 1985. Third Conference on Foundations of Software Technology and Theoretical Computer Science. doi:10.1016/0304-3975(85)90131-8.

39 T. Kasami, Shu Lin, and W. Peterson. New generalizations of the Reed-Muller codes–I: Primitive codes. *IEEE Transactions on Information Theory*, 14(2):189–199, 1968. doi:10.1109/TIT.1968.1054127.

40 T. Kasami, Shu Lin, and W. Peterson. Polynomial codes. *IEEE Transactions on Information Theory*, 14(6):807–814, 1968. doi:10.1109/TIT.1968.1054226.

41 John Y. Kim and Swastik Kopparty. Decoding Reed-Muller Codes over Product Sets. *Theory of Computing*, 13(21):1–38, 2017. doi:10.4086/toc.2017.v013a021.

42 Wolfram Koepf, Predrag M. Rajković, and Sladjana D. Marinković. Properties of $q$-holonomic functions. *Journal of Difference Equations and Applications*, 13(7):621–638, 2007. doi:10.1080/10236190701264925.

43 Swastik Kopparty. List-Decoding Multiplicity Codes. *Theory of Computing*, 11(5):149–182, 2015. URL: 10.4086/toc.2015.v011a005, doi:10.4086/TOC.2015.V011A005.

44 Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters. Improved List Decoding of Folded Reed-Solomon and Multiplicity Codes. *SIAM Journal on Computing*, 52(3):794–840, 2023. doi:10.1137/20M1370215.

45 Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-Rate Codes with Sublinear-Time Decoding. *J. ACM*, 61(5), 2014. doi:10.1145/2629416.

46 S.F. Lacroix. *Traité des Différences et des Séries*. Vol. 3 of *Traité du Calcul Differentiel et du Calcul Intégral*. Courcier, Paris, 1819.

47 D. Larsson and S.D. Silvestrov. Burchnall-Chaundy Theory for $q$-Difference Operators and $q$-Deformed Heisenberg Algebras. *Journal of Nonlinear Mathematical Physics*, 10(sup2):95–106, 2003. doi:10.2991/jnmp.2003.10.s2.7.

48 Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge University Press, 2nd edition, 1997.

49 J. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15(1):122–127, 1969. doi:10.1109/TIT.1969.1054260.

50 Tamás Mészáros. *S-extremal set systems and Gröbner bases* (Diploma Thesis). PhD thesis, Budapest University of Technology and Economics, 2005. Available at https://sites.google.com/view/tamas-meszaros/.

**51** Shay Moran and Cyrus Rashtchian. Shattered Sets and the Hilbert Function. In Piotr Faliszewski, Anca Muscholl, and Rolf Niedermeier, editors, *41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016)*, volume 58 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 70:1–70:14, Dagstuhl, Germany, 2016. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2016.70.

**52** D.E. Muller. Application of Boolean algebra to switching circuit design and to error detection. *Transactions of the I.R.E. Professional Group on Electronic Computers*, EC-3(3):6–12, 1954. doi:10.1109/IREPGELC.1954.6499441.

**53** Rasmus Refslund Nielsen. *List decoding of linear block codes*. Ph.d. thesis, Technical University of Denmark, 2001. Available at https://orbit.dtu.dk/files/3028444/List%20decoding%20of%20linear%20block%20codes.pdf.

**54** Niels Erik Nörlund. *Vorlesungen über Differenzenrechnung*. Springer Berlin, 1924.

**55** R. Pellikaan and Xin-Wen Wu. List decoding of $q$-ary Reed-Muller codes. *IEEE Transactions on Information Theory*, 50(4):679–682, 2004. doi:10.1109/TIT.2004.825043.

**56** W. Peterson. Encoding and error-correction procedures for the Bose-Chaudhuri codes. *IRE Transactions on Information Theory*, 6(4):459–470, 1960. doi:10.1109/TIT.1960.1057586.

**57** I. Reed. A class of multiple-error-correcting codes and the decoding scheme. *Transactions of the IRE Professional Group on Information Theory*, 4(4):38–49, 1954. doi:10.1109/TIT.1954.1057465.

**58** I. S. Reed and G. Solomon. Polynomial Codes Over Certain Finite Fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960. doi:10.1137/0108018.

**59** C.H. Richardson. *An Introduction to the Calculus of Finite Differences*. D. Van Nostrand Company, Inc., New York, 1954.

**60** Steven Roman. *The Umbral Calculus*. Dover Publications, 2005.

**61** Noga Ron-Zewi, S. Venkitesh, and Mary Wootters. Efficient List Decoding of Polynomial Ideal Codes with Optimal List Size. *arXiv Preprint*, 2024. doi:10.48550/arXiv.2401.14517.

**62** Eugene Spiegel and Christopher O'Donnell. *Incidence Algebras*. CRC Press, 1997.

**63** Shashank Srivastava. Improved List Size for Folded Reed-Solomon Codes. *arXiv Preprint*, 2024. doi:10.48550/arXiv.2410.09031.

**64** J.F. Steffensen. *Interpolation*. The Williams & Wilkins Company, Baltimore, 1927.

**65** Madhu Sudan. Decoding of Reed Solomon Codes beyond the Error-Correction Bound. *Journal of Complexity*, 13(1):180–193, 1997. doi:10.1006/jcom.1997.0439.

**66** Itzhak Tamo. Tighter list-size bounds for list-decoding and recovery of folded Reed-Solomon and multiplicity codes. *IEEE Transactions on Information Theory (Early Access)*, pages 1–1, 2024. doi:10.1109/TIT.2024.3402171.

**67** L. Welch. Error Correction for Algebraic Block Codes. *IEEE Int. Symp. Inform. Theory*, 1983. URL: https://cir.nii.ac.jp/crid/1573668924281711104.

**68** E. Weldon. New generalizations of the Reed-Muller codes–II: Nonprimitive codes. *IEEE Transactions on Information Theory*, 14(2):199–205, 1968. doi:10.1109/TIT.1968.1054128.

**69** J.M. Wozencraft. List Decoding. *Quarterly Progress Report, Research Lab of Electronics, MIT*, 48:90–95, 1958.