Polynomials, Divided Differences, and Codes

S. Venkitesh
Tel Aviv University
venkitesh.mail@gmail.com

Error-Correcting Codes: Theory and Practice Reunion
Simons Institute for the Theory of Computing
April 2025

Codes

$$\underbrace{(m_1, \ldots, m_k)}_{\text{message}} \longmapsto \underbrace{(c_1, \ldots, c_N)}_{\text{codeword}}, \quad \text{injective}$$

Code: $C \subseteq \Sigma^N$ (N is the length of C)

Linear code: $\Sigma = \mathbb{F}_q^s$, and C is an $\mathbb{F}_q$-vector space

In this case, message space $\mathbb{F}_q^k$

Rate: $R := \dfrac{\log_{|\Sigma|} |C|}{N} = \dfrac{k}{sN}$

Hamming distance: $d(x, y) := \mathop{\mathbb{P}}_{i \sim [n]} [x_i \neq y_i]$, for $x, y \in \mathbb{F}_q^N$

Minimum distance: $\delta := \min\{d(x, 0) : x \in C \setminus \{0\}\}$

Rate v/s distance tradeoff

$\delta \leq 1 - R$ (Singleton bound)

$\delta = 1 - R$ (Maximum Distance Separable (MDS) code)

List Decodable codes

C is (ρ, L)-list decodable:

$$\left|\{c \in C : d(w, c) \leq \rho\}\right| \leq L \quad \text{for all } w \in \mathbb{F}_q^N.$$

"At most L codewords have agreement at least $(1-\rho)N$ with w."

$$\rho \leq \frac{L}{L+1}(1-R) \qquad \text{(List decoding Singleton bound [ST20])}$$

$$\rho = 1 - R - \varepsilon, \;\; L \sim 1/\varepsilon \qquad \text{(List decoding capacity)}$$

(Explicit codes ?)

List Decodable codes

C is (ρ, L)-list decodable:

$$\left|\{c \in C : d(w,c) \le \rho\}\right| \le L \quad \text{for all } w \in \mathbb{F}_q^N.$$

"At most L codewords have agreement at least $(1-\rho)N$ with w."

$$\rho \le \frac{L}{L+1}(1-R) \qquad \text{(List decoding Singleton bound [ST20])}$$

$$\rho = 1 - R - \varepsilon,\ \ L \sim 1/\varepsilon \qquad \text{(List decoding capacity)}$$

(Explicit codes ✓)

Univariate polynomial codes

Reed-Solomon (RS) code :

$$f(X) \quad \longmapsto \quad \begin{bmatrix} f(a_1) & \cdots & f(a_n) \end{bmatrix}, \qquad \deg(f) < k$$

Folded Reed-Solomon (FRS) code ($\gamma \in \mathbb{F}_q^\times$ generator) :

$$f(X) \quad \longmapsto \quad \left[\begin{bmatrix} f(a_1) \\ f(\gamma a_1) \\ \vdots \\ f(\gamma^{s-1} a_1) \end{bmatrix} \quad \cdots \quad \begin{bmatrix} f(a_n) \\ f(\gamma a_n) \\ \vdots \\ f(\gamma^{s-1} a_n) \end{bmatrix} \right], \qquad \deg(f) < k$$

Multiplicity code :

$$f(X) \quad \longmapsto \quad \left[\begin{bmatrix} f(a_1) \\ \frac{df}{dX}(a_1) \\ \vdots \\ \frac{d^{s-1}f}{dX^{s-1}}(a_1) \end{bmatrix} \quad \cdots \quad \begin{bmatrix} f(a_n) \\ \frac{df}{dX}(a_n) \\ \vdots \\ \frac{d^{s-1}f}{dX^{s-1}}(a_n) \end{bmatrix} \right], \qquad \deg(f) < k$$

List decoding univariate polynomial codes

For FRS and Multiplicity codes, $s = \Theta(1/\varepsilon^2)$.

Code (constant rate R)	Johnson bound $(1-\sqrt{R})$	Capacity $(1-R-\varepsilon)$	List size $O_\varepsilon(1)$
RS code [Guruswami, Sudan, 1999]	✓	NO [Ben-Sasson et al., 2006]	✓ $O(\sqrt{1/R})$
FRS code [Guruswami, Rudra, 2008]	✓	✓	$q^{O_\varepsilon(1)}$
Multiplicity code [Kopparty, 2013]	✓	✓	$q^{O_\varepsilon(1)}$
FRS and Multiplicity code [Guruswami, Wang, 2013]	✓	✓	$q^{O_\varepsilon(1)}$
FRS and Multiplicity code [Kopparty et al., 2018] [Tamo, 2023]	✓	✓	✓ $(1/\varepsilon)^{O(1/\varepsilon)}$
FRS and Multiplicity code [Srivastava, 2024] [Chen, Zhang, 2024]	✓	✓	✓ $O(1/\varepsilon)$

Our interest.

For $s = \Theta(1/\varepsilon^2)$, FRS codes and Multiplicity codes can be list decoded up to radius $1 - R - \varepsilon$, where k is the degree, and $k = Rsn$.

Important.

For Multiplicity codes, $\mathrm{char}(\mathbb{F}_q) > k$ (necessary),

but *no such restriction* for FRS codes.

List decodability of FRS codes is *insensitive* to field characteristic.

Multivariate polynomial codes

$A^m \subseteq \mathbb{F}_q^m$ is a finite grid.

Reed-Muller (RM) code :

$$f(X) \quad \longmapsto \quad \left[f(a)\right]_{a \in A^m}, \qquad \deg(f) < k$$

Multivariate multiplicity code :

$$f(X) \quad \longmapsto \quad \left[\left[\frac{\partial^\alpha f}{\partial X_1^{\alpha_1} \cdots \partial X_m^{\alpha_m}}(a)\right]_{|\alpha|<s}\right]_{a \in A^m}, \quad \deg(f) < k$$

[Guruswami, Sudan, 1999] RM codes are list decodable up to radius $1 - \sqrt[m]{R}$ with list size $O_{R,m}(1)$.

[Bhandari, Harsha, Kumar, and Sudan, 2023]

For $s = \Theta(1/\varepsilon^{2m})$, m-variate multiplicity codes over a finite grid A^m can be list decoded up to radius $\delta - \varepsilon$, where k is the degree, and $k = (1-\delta)s|A|$,

as long as $\mathrm{char}(\mathbb{F}_q) > k$ **(necessary)**.

Questions. Is there a *characteristic insensitive* variant with similar list decodability?

Can we extend the univariate FRS codes to the multivariate setting?

Questions. Is there a *characteristic insensitive* variant with similar list decodability (algorithmic)?

Can we extend the univariate FRS codes to the multivariate setting?

Answer. [V., 2025] YES.

The univariate FRS code is also a multiplicity code!

Simple multivariate extension gives a *divided difference/folded RM* code.

Divided Difference (The Q-derivative)

We choose $\mathtt{Q} := \gamma \in \mathbb{F}_q^\times$ multiplicative generator

For any $f(X) \in \mathbb{F}_q[X]$, define the γ-*derivative*

$$D_\gamma f(X) = \frac{f(\gamma X) - f(X)}{(\gamma - 1)X}$$

Important.

For any monomial X^t, $D_\gamma(X^t) = [t] \cdot X^{t-1}$, where $[t] := \dfrac{\gamma^t - 1}{\gamma - 1}$.

So if $1 \leq \deg(f) < q - 1$, then $\deg(D_\gamma f) = \deg(f) - 1$,

i.e. $D_\gamma\big(\text{large degree monomial}\big) \neq 0$.

Divided Difference (The Q-derivative)

Until now*. . .

– Q-combinatorics [Exton, 1983; Roman, 2005], quantum calculus [Ernst, 2012], over fields of characteristic zero

– *multiplicative rate of change*; no previous explicit appearance in the *polynomial method* literature

Now*. . .

- over fields of small characteristic
- within the polynomial method

*to my knowledge

Basic properties of γ-derivative

Classical Taylor expansion. For any $f(X) \in \mathbb{F}_q[X]$ and $a \in \mathbb{F}_q$,

$$f(X) = \sum_{t=0}^{d} \frac{\frac{d^t f}{dX^t}(a)}{t!}(X-a)^t,$$

if $\deg(f) = d < \mathrm{char}(\mathbb{F}_q)$.

γ-Taylor expansion. For any $f(X) \in \mathbb{F}_q[X]$ and $a \in \mathbb{F}_q$,

$$f(X) = \sum_{t=0}^{d} \frac{D_\gamma^t f(a)}{[t]!}(X-a)\cdots(X-\gamma^{t-1}a),$$

if $\deg(f) = d < q-1$ (*insensitive to field characteristic*).

Basic properties of γ-derivative

Classical product rule. For any $f(X), g(X) \in \mathbb{F}_q[X]$,

$$\frac{d^r(fg)}{dX^r}(X) = \sum_{t=0}^{r} \frac{r!}{t!(r-t)!} \cdot \frac{d^t f}{dX^t}(X) \cdot \frac{d^{r-t} g}{dX^{r-t}}(X).$$

γ-product rule. For any $f(X), g(X) \in \mathbb{F}_q[X]$,

$$\begin{aligned} D^r(fg)(X) &= \sum_{t=0}^{r} \frac{[r]!}{[t]![r-t]!} \cdot D^t f(\gamma^{r-t} X) \cdot D^{r-t} g(X) \\ &= \sum_{t=0}^{r} \frac{[r]!}{[t]![r-t]!} \cdot D^t f(X) \cdot D^{r-t} g(\gamma^t X). \end{aligned}$$

Multivariate γ-derivative and γ-multiplicity code

Encoding. Denote $\mathbb{X} = (X_1, \ldots, X_m)$, $D_\gamma^\alpha = D_{\gamma,X_1}^{\alpha_1} \cdots D_{\gamma,X_m}^{\alpha_m}$.

$$f(\mathbb{X}) \quad \longmapsto \quad \Big[\big[D_\gamma^\alpha f(a) \big]_{|\alpha|<s} \Big]_{a \in A^m}, \qquad \deg(f) < k$$

Algorithmic list decoding

[Bhandari, Harsha, Kumar, and Sudan, 2023]

For $s = \Theta(1/\varepsilon^{2m})$, m-variate multiplicity codes over a finite grid A^m can be list decoded *efficiently* up to radius $\delta - \varepsilon$, where k is the degree, and $k = (1-\delta)s|A|$,

as long as $k < \mathrm{char}(\mathbb{F}_q)$ **(necessary)**.

[V., 2025]

For $s = \Theta(1/\varepsilon^{2m})$, m-variate γ-multiplicity codes over a finite grid A^m can be list decoded *efficiently* up to radius $\delta - \varepsilon$, where k is the degree, and $k = (1-\delta)s|A|$,

(unconditional on $\mathrm{char}(\mathbb{F}_q)$**)**

"List decodability of multivariate γ-multiplicity codes is insensitive to field characteristic."

Another interpretation

[Easy] In the univariate case, there exists an invertible $U_a \in \mathbb{F}_q^{s \times s}$ such that

$$\begin{bmatrix} f(a) \\ f(\gamma a) \\ \vdots \\ f(\gamma^{s-1} a) \end{bmatrix} = U_a \cdot \begin{bmatrix} f(a) \\ D_\gamma f(a) \\ \vdots \\ D_\gamma^{s-1} f(a) \end{bmatrix}.$$

"Distance preserving map between FRS and γ-multiplicity codes."

Analogous extension $\longrightarrow$ *Folded RM* code

List decoding algorithm: Polynomial method

"γ-extension of [BHKS23], with simpler technical details."

"Natural multivariate analogue of [GW13] algorithm."

Main takeaway.

multivariate analysis =

folding trick [BHKS23] + univariate [GW13] analysis

List decoding algorithm: Polynomial method

Consider m-variate γ-multiplicity code over finite grid $A^m \subseteq \mathbb{F}_q^m$, with multiplicity s.

Received word $w = \left[\left[w_{a,\alpha}\right]_{|\alpha|<s}\right]_{a\in A^m}$.

Folding trick. Auxiliary variables $\mathbf{Z} = (Z_1, \dots, Z_m)$.

Capture the received word. Interpolate

$$Q\left(\mathbb{X}, \left(Y_\alpha\right)_{|\alpha|<r}, \mathbf{Z}\right) = \widetilde{Q}(\mathbb{X}) + \sum_{j=0}^{r-1} Q_j(\mathbb{X})\left(\sum_{|\alpha|=j} Y_\alpha \mathbf{Z}^\alpha\right)$$

such that Q vanishes with **high γ-multiplicity** at all points $\left(a, \left[w_{a,\alpha}\right]_{|\alpha|<s}, \mathbf{Z}\right)$. $\quad (r \ll s, \quad r \sim 1/\varepsilon^m)$

List decoding algorithm: Polynomial method

Vanishing conditions imply:

If $f(\mathbb{X})$ is "close" to w, then

$$Q_f(\mathbb{X}) := Q\big(\mathbb{X}, \big[D_\gamma^\alpha f(\mathbb{X})\big]_{|\alpha|<s}, \mathbf{Z}\big)$$

$$\widetilde{Q}(\mathbb{X}) + \sum_{j=0}^{r-1} Q_j(\mathbb{X}) \Bigg(\sum_{|\alpha|=j} D_\gamma^\alpha f(\mathbb{X}) \mathbf{Z}^\alpha \Bigg)$$

must be the **zero** polynomial.

Due to the affine-linear structure of $Q\big(\mathbb{X}, \big(Y_\alpha\big)_{|\alpha|<r}, \mathbf{Z}\big)$,

solution space of "$Q_f(\mathbb{X}) = 0$" is an r-dim affine linear subspace.

$$3 \times \text{trick} = \text{technique}$$

So far... 1. ✓

Hardness of decoding

Bounded distance decoding (BDD).

Given a code C, a word w, and radius $\rho > 0$,

return YES/NO if there exists/not exists $c \in C$ with disagreement at most ρ.

[Guruswami, Vardy, 2005]

NP-hard for RS codes at radius $1 - R - \frac{1}{n}$.

[Gandikota, Ghazi, Grigorescu, 2018]

NP-hard for RS codes at radius $1 - R - \varepsilon$, for some $\varepsilon \gg \frac{1}{n}$, $\varepsilon \to 0$.

Hardness of decoding

FRS codes and univariate multiplicity codes with folding $s \geq 1$:

Assume some $\varepsilon \gg \frac{1}{n}$, $\varepsilon \to 0$.

[GGG, 2018] For $s = 1$, NP-hard at radius $1 - R - \varepsilon$.

We have efficient algorithms for $s \sim 1/\varepsilon^2$.

(Runtime not yet 'poly' in $1/\varepsilon$, but still EASY.)

Question. Is there a threshold s_0 such that

HARD for $s < s_0$, and EASY for $s > s_0$?

Hardness of decoding

Assume some $\varepsilon \gg \frac{1}{n}$, $\varepsilon \to 0$.

[GGG18] BDD is NP-hard for $s = 1$.

We know: List decoding is EASY for $s \sim 1/\varepsilon^2$.

[Gandikota, Grigorescu, V., 2025]

BDD is NP-hard for $s \sim (\log(1/\varepsilon))^{\frac{1}{2}-o(1)}$.

For multiplicity codes,

[GGG18] $+$ polynomial method *extended to multiplicities*.

For FRS codes,

with γ-derivatives ✓, without γ-derivatives ?

Hardness of decoding

Assume some $\varepsilon \gg \frac{1}{n}$, $\varepsilon \to 0$.

[GGG18] BDD is NP-hard for $s = 1$.

We know: List decoding is EASY for $s \sim 1/\varepsilon^2$.

[Gandikota, Grigorescu, V., 2025]

BDD is NP-hard for $s \sim (\log(1/\varepsilon))^{\frac{1}{2}-o(1)}$.

Question. What happens at $s \sim 1/\varepsilon$?

$$3 \times \text{trick} = \text{technique}$$

So far... 1. ✓
2. ✓
3. ?

Thank You