

Today

- Multiplicity Codes - I.

C33.318.1

Coding Theory

Lecture 23 (2022-11-21)

Instructor: Prabhakar
Harsha.

Recall polynomial-based codes

Reed-Solomon / Reed-Muller Codes.

Message as coefficients of a polynomial

RS/RM

Evaluation of poly over
a specific set of
points. $S = \{\alpha_1, \dots, \alpha_m\} \subseteq F_q^m$

$\{P(\alpha)\}_{\alpha \in S}$

III

$\{P(x) \pmod{(x-\alpha)}\}_{\alpha \in S}$

Multiplicity Codes

(univariate &
multivariate)

Evaluation of poly +
low-order derivatives
at a specific set of
evaluation points S

$\{P(\alpha), P'(\alpha), P''(\alpha), \dots\}$

III

$\{P(x) \pmod{(x-\alpha)^k}\}_{\alpha \in S}$

(low-order derivatives
all $\leq k$ derivatives)

History:

'97 $m=1$ Rosenblum & Teitelman

'01 $m=1$ Nielsen - extended WB + GS

algorithms b the constant multiplicity.

'11 general m Koppatty, Saraf, Yekhanin
(locally decodable codes)
w/ Rate $\rightarrow 1$

'12 $m=1$ Koppatty
Guruswami - Wang } first-decodable
all the way to distance.

Formal treatment:

Notion of derivatives: (of polynomials)

Reals / Complexes:

$$\begin{array}{ll}
 \text{eg:} & f(x) = x^2 \\
 & f'(x) = 2x \\
 & f''(x) = 2
 \end{array}
 \quad \left| \begin{array}{l}
 \text{Taylor Series:} \\
 f(x+\epsilon) = f(x) + f'(x) \cdot \epsilon + \frac{f''(x) \cdot \epsilon^2}{2} \\
 + \dots + \frac{f^{(n)}(x) \cdot \epsilon^n}{n!}
 \end{array} \right.$$

$$\begin{aligned}
 (x+\epsilon)^2 &= x^2 + 2x \cdot \epsilon + \frac{2 \cdot \epsilon^2}{2} \\
 &= x^2 + 2x \cdot \epsilon + \epsilon^2
 \end{aligned}$$

Let's look at $GF(2)$ -field.

above definition, does not extend
since division by $x!$ might not
be feasible).

Hasse Derivatives (of polynomials)

m - # variables

$$\bar{x} = (x_1, \dots, x_m)$$

Monomial $x_1^{e_1} x_2^{e_2} \dots x_m^{e_m} = \bar{x}^{\bar{e}}$ where

$$\bar{e} = (e_1, e_2, \dots, e_m)$$

\mathbb{F} - finite field (w/ characteristic p).

$$\bar{i} = (i_1, \dots, i_m).$$

i^{th} order derivative of $P(x)$ is $P^{(i)}(x)$

$$\text{where } P(x+z) = \sum P^{(i)}(x) z^i$$

$$P(x) = x^2 \quad (x+z)^2 = x^2 + z^2$$

$$P^{(0)}(x) = x^2$$

$$P^{(1)}(x) = 0$$

$$P^{(2)}(x) = 1$$

Properties of Hasse Derivatives:

$$(1) \quad P^{(c)}(x) + Q^{(c)}(x) = (P+Q)^{(c)}(x)$$

$$(2) \quad (P \cdot Q)^{(c)}(x) = \sum_{\bar{e}: \bar{e} \leq c} P^{(\bar{e})}(x) \cdot Q^{(c-\bar{e})}(x)$$

$$(3) \quad (P^{(c)})^{(d)}(x) = \binom{c+d}{c} P^{(c+d)}(x)$$

where $\binom{\bar{c}}{\bar{e}} = \prod_{i=1}^r \binom{c_i}{e_i}$

Multiplicity of P at point a .

$$\text{mult}(P, a) = \max \{ n \in \mathbb{Z}_{\geq 0} \mid P^{(n)}(a) = 0 \text{ for all } \bar{e} \text{ such that } |\bar{e}| < n \}$$

where $|\bar{e}| = \sum e_i$

$$P(x+z) = \sum P^{(\bar{e})}(x) z^{(\bar{e})}$$

Substitute $x \leftarrow a$

$$z \leftarrow x-a$$

$$P(x) = \sum P^{(\bar{e})}(a) (x-a)^{\bar{e}}$$

($m=1$) : Suppose $\text{mult}(P, a) \geq m$

$$P(x) = (x-a)^m Q(x)$$

re, Hasse derivative defn of multiplicity
coincides w/ GS' notion of multiplicity.

Multiplicity Codes:

\mathbb{F} - field (w/ characteristic p)

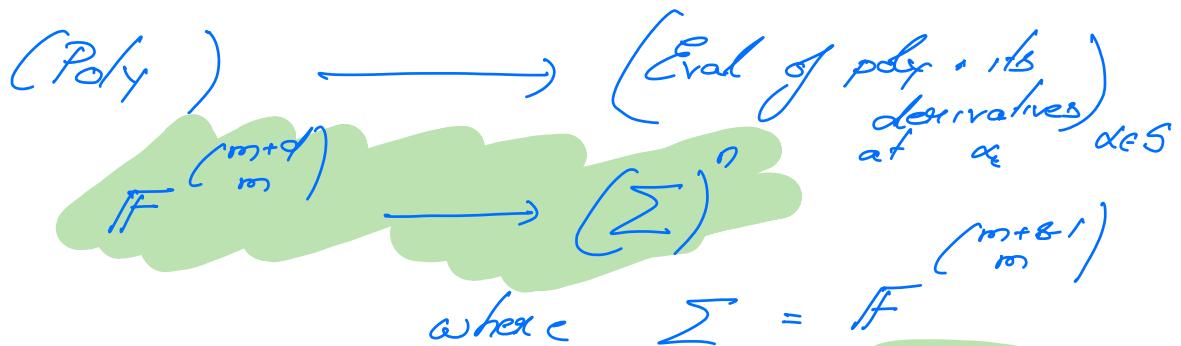
m - # variables ($\in \mathbb{Z}_{\geq 0}$)

d - degree parameter ($\in \mathbb{Z}_{\geq 0}$)

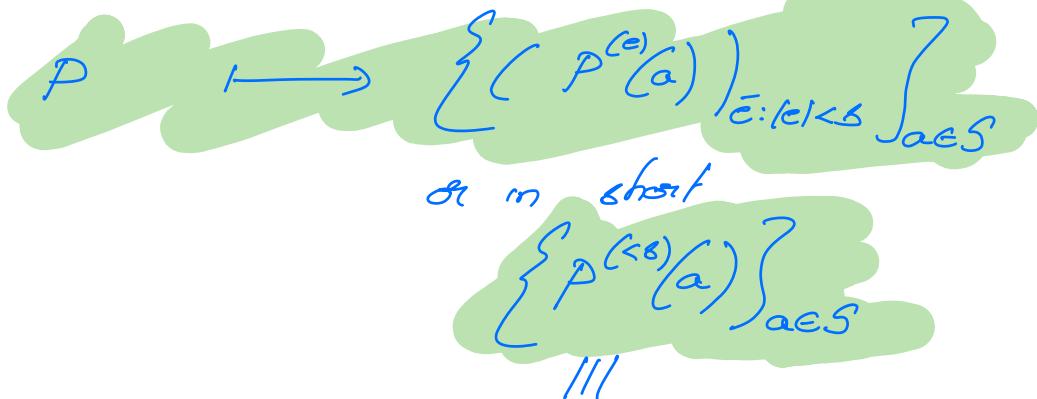
s - multiplicity parameter ($\in \mathbb{Z}_{\geq 0}$)

n - # point of evaluation

$S = \{\alpha_1, \alpha_2, \dots, \alpha_n\} \subseteq \mathbb{F}_q^m$



where $\sum = \mathbb{F}_{q^m}^{(m+1)}$



(in the univariate setting.)

$$\left\{ P(x) \pmod{(x-\alpha)^s} \right\}_{\alpha \in S}$$

for general m , $P(x) \pmod{\langle x_0-a, x_1-a, \dots, x_m-a \rangle^s}$

For rest of lecture, focus on univariate
(i.e. $m=1$) setting

Distance of the univariate multiplicity code

Suppose $P \neq 0$ $\deg(P) \leq d$, $S = \{a_1, \dots, a_n\}$

$$\Pr_{\alpha \in S} [P^{(<0)}(\alpha) = 0] = \Pr_{\alpha \in S} [\text{mult}(P, \alpha) \geq 1] \leq \frac{d}{n}$$

Distance of univariate multiplicity $\geq 1 - \frac{d}{n}$

Rate of univariate multiplicity = $\frac{d+1}{n}$

Univariate Multiplicity Codes achieve the Singleton Bound
are MDS codes

$$a_1, \dots, a_n \rightarrow P(x) \pmod{(x-a_i)^k} = R_i(x)$$

$$P(x) = \sum_{a \in S} R_a(x) \prod_{b \in S \setminus a} \frac{(x-b)^{k_b}}{(a-b)^{k_a}}$$

Decoding Algorithms for Univariate Multiplicity Code

1. Unique Decoding upto half the min
distance $\sum \left(1 - \frac{d}{2n}\right)$

2. List-decoding upto the Johnson Radius.

CWB = GS generalize Nielsen '01

3. List-decoding beyond the Johnson Radius

Kopparty, Cucamonga-Hang

F_E , $\exists \delta = \delta_0(E)$ s.t. $Mult(F, m=1, \delta \geq \delta_0, d; n)$

is list-decodable till $1 - \frac{d}{2n} - \epsilon$.

In lecture, Kopparty's list-decoding algorithm.