Today
- Multiplicity Codes - I.

CSS.318.1
Coding Theory
Lecture 23 (2022-11-21)
Instructor: Prahladh Harsha.

Recall polynomial-based codes

Reed Solomon / Reed-Muller Codes.

Message as coefficients of a polynomial

$\xrightarrow{\text{RS/RM}}$

Evaluation of poly over a specific set of points. $S = \{\alpha_1, \ldots \alpha_n\} \subseteq \mathbb{F}_q^m$

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

$$|||$$

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

$\longrightarrow$ Multiplicity Codes (univariate & multivariate)

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

$$\{(p(\alpha), p'(\alpha), p''(\alpha), \ldots)\}$$

$$|||$$

$$\{p(x) \pmod{(x-\alpha)^s}\}_{\alpha \in S}$$

(low-order derivatives all $< s$ derivatives)

History:

'97 $m=1$ Rosenblum & Tsfasman

'01 $m=1$ Nielsen - extended WB & GS algorithms to the univariate multiplicity

'11 general m Kopparty, Saraf, Yekhanin (locally decodables codes w/ Rate $\to 1$)

'12 $m=1$ Kopparty, Guruswami - Wang } list-decodable all the way to distance.

Formal treatment:

Notion of derivatives: (of polynomials)

Reals / Complexes:

eg:

$$f(x) = x^2$$
$$f'(x) = 2x$$
$$f''(x) = 2$$

Taylor Series:

$$f(\alpha+\varepsilon) = f(\alpha) + f'(\alpha)\cdot\varepsilon + f''(\alpha)\cdot\frac{\varepsilon^2}{2} + \dots + \frac{f^{''\cdots r}(\alpha)\,\varepsilon^r}{r!}$$

$$(\alpha+\varepsilon)^2 = \alpha^2 + 2\alpha\cdot\varepsilon + \frac{2}{2}\cdot\varepsilon^2$$
$$= \alpha^2 + 2\alpha\cdot\varepsilon + \varepsilon^2$$

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).

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

$\bar{i}^{th}$ order derivative: of $P(x)$ is $P^{(\bar{i})}(x)$ where $P(x+Z) = \sum P^{(\bar{e})}(x) \bar{Z}^{\bar{e}}$

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

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

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

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

Properties of Hasse Derivatives:

(1) $P^{(\bar{i})}(X) + Q^{(\bar{i})}(X) = (P+Q)^{(\bar{i})}(X)$

(2) $(P\cdot Q)^{(\bar{i})}(X) = \sum_{\bar{e} : \bar{e} \leq \bar{i}} P^{(\bar{e})}(X) \cdot Q^{(\bar{i}-\bar{e})}(X)$

(3) $\left(P^{(\bar{i})}\right)^{(\bar{j})}(X) = \binom{\bar{i}+\bar{j}}{\bar{i}} P^{(\bar{i}+\bar{j})}(X)$

where $\binom{\bar{e}}{\bar{f}} = \prod \binom{e_i}{f_i}$

—

Multiplicity of P at point α.

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

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 $\text{mult}(P, a) \geq r$

$P(X) = (X-a)^r\, Q(X)$

ie, Hasse derivative defn of multiplicity coincides w/ GS-notion of multiplicity.

Multiplicity Codes:

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

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

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

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

n - # point of evaluation

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

(Poly) $\longrightarrow$ (Eval of poly + its derivatives at α_i) $_{\alpha \in S}$

$$\mathbb{F}^{\binom{m+d}{m}} \longrightarrow (\Sigma)^n$$

where $\Sigma = \mathbb{F}^{\binom{m+s-1}{m}}$

$$P \longmapsto \left\{ \left(P^{(e)}(a) \right)_{\bar{e}: |e| < s} \right\}_{a \in S}$$

or in short

$$\left\{ P^{(<s)}(a) \right\}_{a \in S}$$

$$|||$$

(in the univariate setting. $\left\{ P(x) \ (\mathrm{mod}\ (x-a)^s \right\}_{a \in S}$

for general m, $P(x) \bmod \langle x_1 - a_1, x_2 - a_2 \ldots x_m - a_m \rangle^s$

For rest of lecture, focus on univariate (ie $m=1$) setting

Distance of the univariate multiplicity code

Suppose $P \not\equiv 0$ $\quad \deg(P) \le d$. ; $S = \{\alpha_1, \ldots, \alpha_n\}$

$$\Pr_{a \leftarrow S}\left[P^{(<s)}(a) = 0\right] = \Pr_{a \leftarrow S}\left[\mathrm{mult}(P, a) \ge s\right]$$

$$\le \frac{d}{sn}.$$

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

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

Univariate Multiplicity Codes achieve the Singleton Bound :

are MDS codes.

$a_1 \ldots a_n \quad \sim \quad P(x) \pmod{(x-a_i)^s} = R_i(x)$

$$P(x) = \sum_{a \in S} R_i(x) \prod_{b \in S \setminus a} \frac{(x-b)^s}{(a-b)^s}$$

Decoding Algorithms for Univariate Multiplicity Code

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

2. List-decoding upto the Johnson Radius.

CWB : GS generalize [Nielsen '01]

3. List-decoding beyond the Johnson Radius

Kopparty, Saraswami-Wang
$\forall \varepsilon$, $\exists$ $s_0 = s_0(\varepsilon)$ s.t. $\mathrm{Mult}(\mathbb{F}, m=1, s \geq s_0, d, n)$ is list-decodable till $1-\frac{d}{sn}-\varepsilon$.

In lecture, Kopparty's list-decoding algorithm.