Multiplicity Codes.

Simons Bootcamp

Prahladh Harsha
TIFR

Multiplicity Codes

Higher derivative variants of
Reed-Solomon Codes
&
Reed-Muller Codes

$$P \mapsto \begin{array}{|c|c|c|c|} \multicolumn{1}{c}{\alpha_1} & \multicolumn{1}{c}{\alpha_2} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{\alpha_n} \\ \hline P^{(<s)}(\alpha_1) & P^{(<s)}(\alpha_2) & \cdots\cdots & P^{(<s)}(\alpha_n) \\ \hline \end{array}$$

$$P^{(<s)}(\alpha) = \begin{pmatrix} P(\alpha) \\ P^{(1)}(\alpha) \\ P^{(2)}(\alpha) \\ \vdots \\ P^{(s-1)}(\alpha) \end{pmatrix}$$

Talk Outline

- Definitions (univariate & multivariate)
- Univariate Multiplicity Codes
  * List-decoding upto capacity.
- Multivariate Multiplicity Codes
  * Multiplicity Schwartz-Zippel Lemma
  * High-rate locally-decodable codes
- Open Questions

Polynomial Evaluation Codes.

Reed-Solomon Codes: Evaluations of univariate polynomials.

$\mathbb{F}$ - field ; k - degree

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

$p \in \mathbb{F}_{<k}[x]$

$$\mathbb{F}_{<k}[x] \longrightarrow \mathbb{F}^S$$

$$p \longmapsto \begin{array}{|c|c|c|c|} \hline p(\alpha_1) & p(\alpha_2) & \ldots & p(\alpha_n) \\ \hline \alpha_1 & \alpha_2 & & \alpha_n \end{array}$$

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

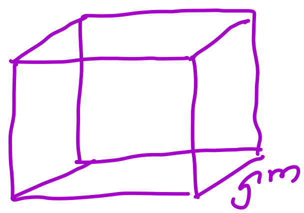
Reed-Muller Codes: Evaluations of multivariate polynomials

$\mathbb{F}$ - field ; d - degree

m - dimension

$S = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}$

$p(x_1, x_2, \ldots x_m) \in \mathbb{F}_{\leq d}[x_1 \ldots x_m]$



$$\mathbb{F}_{\leq d}[x_1 \ldots x_m] \longrightarrow \mathbb{F}^{S^m}$$

$$p \longmapsto \{p(\alpha_1 \ldots \alpha_m)\}_{\alpha_i \in S}$$

Polynomial Evaluation Codes - Distance

Reed-Solomon Codes: Evaluations of univariate polynomials

$\mathbb{F}_{<k}[x] \longrightarrow \mathbb{F}^{S}$

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

Degree Mantra:

$p \in \mathbb{F}_{<k}[x]$, $p \not\equiv 0$

$\Downarrow$

$\#\,\mathrm{zeros}(p) < k$

Reed-Muller Codes: Evaluations of multivariate polynomials

$\mathbb{F}_{\leq d}[x_1, \ldots x_m] \longrightarrow \mathbb{F}^{S^m}$

$p \longmapsto \{p(\alpha_1, \ldots \alpha_m)\}_{\alpha_i \in S}$

Schwartz-Zippel Lemma

$p \in \mathbb{F}_{\leq d}[x_1, \ldots x_m]$, $p \not\equiv 0$

$\Downarrow$

$$\Pr_{\bar{a} \in S^m}\left[p(\bar{a}) = 0\right] \leq \frac{d}{|S|}$$

Polynomial Evaluation Codes.

Reed-Solomon Codes: Evaluations of univariate polynomials

$$\mathbb{F}_{<k}[x] \longrightarrow \mathbb{F}^S$$

$\mathbb{F}$ - field ; k - degree

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

$p \in \mathbb{F}_{<k}[x]$

$$p \longmapsto \begin{array}{cccc} \hline p(\alpha_1) & p(\alpha_2) & \cdots & p(\alpha_n) \\ \hline \alpha_1 & \alpha_2 & & \alpha_n \end{array}$$

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

Folded Reed-Solomon Codes: $\mathbb{F}_{<k}[x] \to (\mathbb{F}^s)^S$

$\gamma \in \mathbb{F}^*$

(typically, generator)

$$p \longmapsto \begin{array}{|c|c|c|} \hline p(\alpha_1) & p(\alpha_2) & \\ p(\gamma\alpha_1) & p(\gamma\alpha_2) & \cdots \\ \vdots & \vdots & \\ p(\gamma^{s-1}\alpha_1) & p(\gamma^{s-1}\alpha_2) & \\ \hline \end{array}$$

$$p \longmapsto \left\{ \begin{pmatrix} p(\alpha) \\ p(\gamma\alpha) \\ \vdots \\ p(\gamma^{s-1}\alpha) \end{pmatrix} \right\}_{\alpha \in S}$$

Ideal Theoretic Viewpoint.

	RS	RM
message	$p \in \mathbb{F}_{<k}[x]$	$p(x_1, \dots x_m) \in \mathbb{F}_{\leq d}[x_1 \dots x_m]$
Codeword (Evaluation)	$\{p(\alpha)\}_{\alpha \in S}$.	$\{p(\bar{\alpha})\}_{\bar{\alpha} \in S^m}$
Alternate View	$\{p(x) \bmod \langle x-\alpha \rangle\}_{\alpha \in S}$	$\{p(x_1, .. x_m) \bmod \langle x_1-\alpha_1, \dots x_m-\alpha_m \rangle\}_{\bar{\alpha} \in S^m}$

Ideal Theoretic Viewpoint.

RS: $\quad p \longmapsto \{p(\alpha)\}_{\alpha \in S}$

$$\cong$$

$$\{p(x) \bmod \langle x-\alpha \rangle\}_{\alpha\in S}$$

FRS: $\quad p \longmapsto \left\{\begin{pmatrix} p(\alpha) \\ p(r\alpha) \\ \vdots \\ p(r^{s-1}\alpha)\end{pmatrix}\right\}_{\alpha \in S} \equiv \left\{\begin{pmatrix} p(x) \bmod \langle x-\alpha\rangle \\ p(x) \bmod \langle x-r\alpha\rangle \\ \\ p(x) \bmod \langle x-r^{s-1}\alpha\rangle \end{pmatrix}\right\}_{\alpha\in S}$

$\updownarrow$ CRT

$$\equiv \left\{p(x) \bmod \prod_{j=0}^{s-1}(x-r^j\alpha)\right\}_{\alpha\in S}$$

Ideal-Theoretic Codes.

$$p \in \mathbb{F}_{<k}[x] \quad , \quad E_1(x), E_2(x), \ldots E_n(x) \in \mathbb{F}_{=b}[x]$$

pairwise coprime

$$p \longmapsto \{p(x) \bmod E_i(x)\}_{i=1}^{n}$$

$$\mathbb{F}^k \cong \mathbb{F}_{<k}[x] \longrightarrow \left(\mathbb{F}_{<b}[x]\right)^n \cong \left(\mathbb{F}^b\right)^n$$

Ideal-Theoretic Codes.

$p \in \mathbb{F}_{<k}[x]$, $E_1(x), E_2(x), \ldots E_n(x) \in \mathbb{F}_q[x]$

$$p \longmapsto \{p(x) \bmod E_i(x)\}_{i=1}^{n}$$

Remarks:

1. All ideal-theoretic codes are MDS codes
2. Unique-decoding (to half-distance) - A la Berlekamp-Welch.
3. List-decoding (upto Johnson radius) - A la Guruswami-Sudan [Bhandari-Harsha-Kumar-Sudan '21]

Ideal-Theoretic Codes.

$p \in \mathbb{F}_{<k}[x]$, $E_1(x), E_2(x), \ldots E_n(x) \in \mathbb{F}_{=b}[x]$

$$p \longmapsto \{p(x) \bmod E_i(x)\}_{i=1}^{n}$$

$$\mathbb{F}^k \cong \mathbb{F}_{<k}[x] \longrightarrow (\mathbb{F}_{<b}[x])^n \cong (\mathbb{F}^b)^n$$

Decoding Beyond Johnson Radius?

Ideal-Theoretic Codes.

$p \in \mathbb{F}_{<k}[x]$, $E_1(x), E_2(x), \ldots E_n(x) \in \mathbb{F}_{=s}[x]$

$$p \longmapsto \{p(x) \bmod E_i(x)\}_{i=1}^{n}$$

$$\mathbb{F}^k \cong \mathbb{F}_{<k}[x] \longrightarrow (\mathbb{F}_{<s}[x])^n \cong (\mathbb{F}^s)^n$$

FRS codes: $E_i(x) = \prod_{j=0}^{s-1} (x - \gamma^j \alpha_i)$

Multiplicity Codes : $E_i(x) = (x - \alpha_i)^s$

Univariate Multiplicity Codes

[Rosenbloom-Tsfasman '97
Nielsen '01]

Univariate Multiplicity Codes.

$\mathbb{F}$ - field

k - degree

s - multiplicity bound

$S = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}$ (set of evaluation points)

Message Space $= \mathbb{F}^k \cong \mathbb{F}_{<k}[X]$

Codeword Space $= (\mathbb{F}^s)^n \cong (\mathbb{F}_{<s}[X])^n$

$$P \longmapsto \{ P(X) \bmod \langle X-\alpha \rangle^s \}_{\alpha \in S}$$

Univariate Multiplicity Codes.

$$p \mapsto \{ p(x) \bmod \langle x-\alpha \rangle^s \}_{\alpha \in S}$$

For each $\alpha \in S$, write $p(x)$ in the basis $1, (x-\alpha), (x-\alpha)^2, \ldots$

$$p(x) = \underbrace{\sum_{i=0}^{s-1} p^{(i)}(\alpha) \cdot (x-\alpha)^i}_{} + R(x)(x-\alpha)^s$$

$$p^{(<s)}(\alpha) \triangleq p(x) \bmod (x-\alpha)^s$$

$p^{(i)}(\alpha)$ - Hasse derivatives.

Multivariate Multiplicity Codes

[Kopparty Saraf Yekhanin '11]

Multivariate Multiplicity Codes.

$\mathbb{F}$ - field

k - degree

s - multiplicity bound

m - dimension

$S = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}$ (set of evaluation points)

Message Space $= \mathbb{F}_{<d}[X_1, X_2, \ldots, X_m]$

Codeword Space $= \left(\mathbb{F}_{<s}[X_1, \ldots X_m]\right)^n$

$$P(X_1, \ldots, X_m) \longmapsto \left\{ P \bmod \langle X_1 - \alpha_1, X_2 - \alpha_2, \ldots, X_m - \alpha_m \rangle^s \right\}_{\bar{\alpha} \in S^m}$$

Multivariate Multiplicity Codes.

$$p(x_1, \dots, x_m) \longmapsto \left\{ p \bmod \langle x-\alpha_1, x-\alpha_2, \dots, x-\alpha_m \rangle^s \right\}_{\bar{\alpha} \in S^m}$$

For each $\bar{\alpha} = (\alpha_1, \dots, \alpha_m) \in S^m$

writing $p(\bar{x})$ in appropriate basis.

$$p(\bar{x}) = \sum_{\substack{\bar{e} = (e_1, \dots, e_m) \\ 0 \le \sum e_i < s}} p^{(\bar{e})}(\bar{\alpha}) \cdot \prod_{i=1}^{m} (x_i - \alpha_i)^{e_i} + R(\bar{x}) \cdot \prod_{i=1}^{m} (x_i - \alpha_i)^s$$

$$\underbrace{p(\bar{x}) \bmod \langle x_1 - \alpha_1, \dots, x_m - \alpha_m \rangle^s}_{} \triangleq p^{(<s)}(\bar{\alpha})$$

Rate $\approx$ Distance of Multiplicity Codes

Univariate:

$$P \longmapsto \{ P(X) \bmod \langle X-\alpha \rangle^{s} \}_{\alpha \in S}$$

$$\text{Rate} = \frac{k}{s|S|}$$

Degree Mantra: $P \in \mathbb{F}_{<k}[X]$; $P \neq 0$

zeros of P < k.

Rate : Distance of Multiplicity Codes

Univariate:

$$P \longmapsto \{ P(x) \bmod \langle x-\alpha\rangle^s \}_{\alpha\in S}$$

$$\text{Rate} = \frac{k}{s|S|}$$

Degree Mantra: $p \in \mathbb{F}_{<k}[X]$; $p \neq 0$

zeros of P (counting w/ multiplicity) $< k$.

Rate & Distance of Multiplicity Codes

Univariate:

$$P \longmapsto \{ P(x) \bmod \langle x-\alpha \rangle^s \}_{\alpha \in S}$$

$$\text{Rate} = \frac{k}{s|S|}$$

Degree Mantra: $P \in \mathbb{F}_{<k}[X]$, $P \neq 0$

zeros of P (counting w/ multiplicity) $< k$.

$$\text{Distance} > 1 - \frac{k}{s|S|}$$

MDS code!

Distance of Multivariate Multiplicity Codes

$$P(X_1, \ldots, X_m) \longmapsto \left\{ P \bmod \langle X-\alpha_1, X-\alpha_2, \ldots, X-\alpha_m \rangle^s \right\}_{\bar{\alpha} \in S^m}$$

$s = 1$: Reed Muller Codes.

Schwartz-Zippel Lemma

$P \in \mathbb{F}_{\leq d}[X_1, \ldots X_m]$, $P \not\equiv 0$

$$\Downarrow$$

$$\Pr_{\bar{a} \in S^m} \left[P(\bar{a}) = 0 \right] \leq \frac{d}{|S|}$$

Multiplicity Variant (for larger s)

Multiplicity Schwartz-Zippel Lemma

[Dvir-Kopparty-Saraf-Sudan '09]

Multiplicity Schwartz-Zippel Lemma

Extend the notion of multiplicities to large dimensions

$P \in \mathbb{F}[x_1, x_2 \dots x_m]$; $\bar{a} \in \mathbb{F}^m$

$$\mathrm{mult}(P, \bar{a}) = \begin{cases} \text{largest } M \text{ s.t. } \forall \text{ exponent } \bar{e} \\ \mathrm{wt}(\bar{e}) < M, \quad P^{(\bar{e})}(\bar{a}) = 0 \end{cases}$$

Classical SZ Lemma: $\mathbb{E}_{\bar{a} \leftarrow S^m}\left[\mathbb{1}[P(\bar{a}) = 0]\right] \leq \frac{d}{|S|}$

Mult. SZ Lemma:

$$\mathbb{E}_{\bar{a} \leftarrow S^m}\left[\mathrm{mult}(P, \bar{a})\right] \leq \frac{d}{|S|}$$

Distance of multivariate multiplicity Code

Mult. SZ Lemma:

$$\mathop{\mathbb{E}}_{\bar{a} \leftarrow S^m}\left[\mathrm{mult}(P, \bar{a})\right] \leq \frac{d}{|S|}$$

Corollary: $P \neq Q \in \mathbb{F}_{\leq d}[X_1, X_2 \dots X_m]$

$$\Pr_{\bar{a} \leftarrow S^m}\left[P^{(<s)}(\bar{a}) = Q^{(<s)}(\bar{a})\right] = \Pr\left[\mathrm{mult}(P-Q, \bar{a}) \geq s\right]$$

$$\leq \frac{d}{s|S|}$$

$$\text{Distance} \geq 1 - \frac{d}{s|S|}$$

List-decoding Univariate Multiplicity Codes

List-decoding Univariate Multiplicity Codes

[Kopparty '12 + Guruswami-Wang '11]

Problem: Given a received $r = \{\beta_i^{(<s)} \in \mathbb{F}^s\}_{i=1}^{n}$ find all deg d polynomials P such that

$$\#\{i \mid P^{(<s)}(\alpha_i) = \beta_i^{(<s)}\} \geq t.$$

Goal: Make t as small as possible.

List-decoding Univariate Multiplicity Codes

[Kopparty '12 & Guruswami-Wang '11]

Theorem: $\forall\ R, \varepsilon \in (0,1)$, there is a multiplicity parameter s such that the univariate multiplicity code with degree d, blocklength n, multiplicity s and rate $R = \frac{d}{sn}$ over fields of characteristic $\geq \max\{d, n\}$ is list-decodable from $(1-R-\varepsilon)$ fraction of errors.

Univariate Mult codes of large enough mult are list-decodable upto capacity.

Guruswami-Wang Linear Algebraic Framework

Input: $\mathfrak{r} = \{ \beta_i^{(<s)} \in \mathbb{F}^s \}_{i=1}^n$

Step 1: Find an "algebraic explanation" for $\mathfrak{r}$

Find $Q(X, Y_0, Y_1, \ldots Y_{m-1}) = A(X) + \sum_{i=0}^{m-1} Y_i \cdot B_i(X)$

satisfying $(\star\star\star)$

Guruswami-Wang Linear Algebraic Framework

Conditions (***) are such that

if polynomial $P \in \mathbb{F}_{<k}[X]$ satisfies

$$P^{(<s)}(\alpha_i) = \beta_i^{(<s)}$$

then $R(X) \triangleq Q(X, P(X), P^{(1)}(X), \ldots, P^{(m-1)}(X))$

has a root at α_i with multiplicity $s-m$

Guruswami-Wang Linear Algebraic Framework

Conditions $(\star\star\star)$ are such that

if polynomial $P \in \mathbb{F}_{<k}[X]$ satisfies

$$P^{(<s)}(\alpha_i) = \beta_i^{(<s)}$$

then $R(X) \equiv Q(X, P(X), P^{(1)}(X), \ldots, P^{(m-1)}(X))$

has a root at α_i with multiplicity $s-m$.

Corollary: If P & $\bar{r}$ agree on t points

then $R(X)$ has $(s-m)t$ roots (w/ multiplicities).

Cor: $\deg(R) < (s-m)t \Rightarrow R \equiv 0$.

Guruswami-Wang Linear Algebraic Framework

Input: $r = \{\beta_i^{(<s)} \in \mathbb{F}^s\}_{i=1}^n$

Step 1: Find an "algebraic explanation" for r

Find $Q(X, Y_0, Y_1, \ldots Y_{m-1}) = A(X) + \sum_{i=0}^{m-1} Y_i \cdot B_i(X)$

satisfying $(\star\star\star)$

Step 2: Solve the differential equation to find all polynomials P s.t

$Q(X, P(X), P^{(1)}(X), \ldots, P^{(m-1)}(X)) \equiv 0.$

Guruswami-Wang Linear Algebraic Framework

Remarks:

1. Deterministic Algorithm that list-decodes to capacity and outputs lists of size $\leq q^m$
2. Pruning [Kopparty-Ron Zewi-Saraf-Wootters '18] Randomized procedure to reduce list size to constant $O_\varepsilon(1)$
3. $O(n \cdot \text{polylog}\, n)$-time algorithm [Goyal-Harsha-Kumar-Shankar '24]

Local-Decoding of Multivariate Multiplicity Codes.

Local-Decoding of Multivariate Multiplicity Codes.

[Kopparty - Saraf - Yekhanin '11]

Theorem: For every $\varepsilon, \alpha \in (0,1)$ and $k \in \mathbb{Z}_{>0}$ there are multiplicity codes of dimension k, rate $1-\alpha$ and locally-decodable from constant fraction of errors in $O_{\varepsilon,\alpha}(k^{\varepsilon})$ time

[Alternate Constructions: Guo-Kopparty-Sudan '13
Guo '13
Hemenway-Ostrovsky-Wootters '13

Local Decoding

Problem: Given $f : \mathbb{F}^m \to \mathbb{F}_{<\delta}[x_1, \dots x_m]$

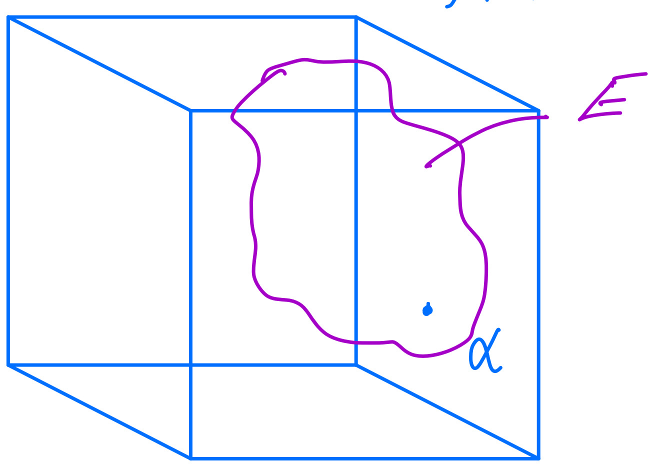
s.t there exist $P \in \mathbb{F}_{\le d}[x_1, \dots x_m]$

$$\Pr_{a \leftarrow \mathbb{F}^m}\left[P^{(<\delta)}(a) \neq f(a) \right] \le \delta_0 = \frac{\delta}{8}.$$

& $\alpha \in \mathbb{F}^m$

find $P^{(<\delta)}(\alpha)$.

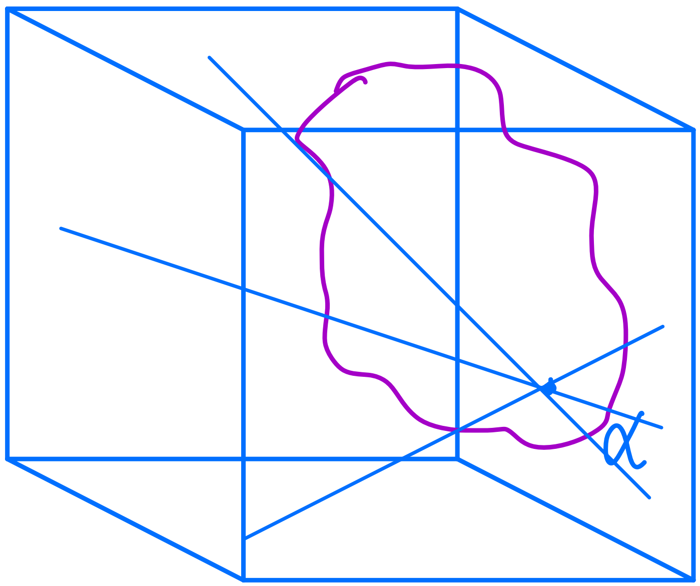
$\mathbb{F}^m$



$f : \mathbb{F}^m \to \mathbb{F}_{<\delta}[x_1, \dots x_m]$

E - error $= \{a \mid f(a) \neq P^{(<\delta)}(a)\}$

Local Decoding [Kopparty-Saraf-Yekhanin '11
+ Kopparty '14]



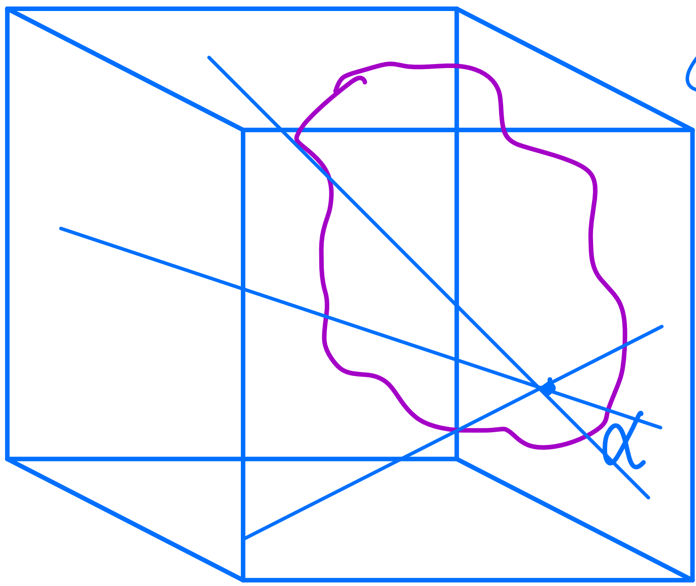
1. Let $S \subseteq \mathbb{F}$ be a set of size $10s^2$.
Pick $a, b_1, \ldots b_m \in_R \mathbb{F}^m$

$$B = \{ a + \sum x_i b_i \mid x_i \in S \}$$

2. For each $\beta \in B$ run univariate decoder along $l_\beta(t) = \alpha + t\beta$ to obtain $P^{(e)}(\alpha + t\beta)$.

(more precisely get the univariate polynomial $Q_{\beta,e}(T)$)

Local Decoding [Kopparty-Saraf-Yekhanin '11, Kopparty '14]



(*) For most $a, b_1, \ldots b_m$ at least $2/3$ of lines ℓ_β satisfy

$$Q_{\beta,e}(T) = P^{(e)}(\alpha + \beta T)$$

(*) Look at coefficient of T^i in above polynomial

degree $\le s$, m-variate multiplicity encoding on set B.

Do global decoding to recover $P^{(e)}(\alpha)$. $\forall\ e,\ wt(e) < s$.

Open Questions

I. Decoding

Univariate: What is list-decoding radius (current algorithms work only for large s ≥ characteristic)

Multivariate:

Unique-decoding [Bhandari-Harsha-Kumar-Shankar '23]

List-decoding on grids [Bhandari-Harsha-Kumar-Sudan '21]

Open Questions

II Testing:

Are multiplicity codes testable?

[Karliner-Salama-Ta-Shma '22
Karliner-Ta-Shma '22]

III Applications:

Unbalanced Expanders

[Kalev-Ta-Shma '22]

Multiplicity Codes

Kopparty, "Some Remarks on Multiplicity Codes", 2014

Thank You..

Speed Talks! Thursday/Friday!

- Tell us what you are excited about!
    - Open Problems!
    - Cool Results!
    - Fun Techniques!
    - “Hi my name is _____ and here’s a quick summary of what I work on!”

- Submit a talk title here!
    - Link also on Zulip and in your inbox.

Please submit by Tuesday evening!