Today
- Multiplicity Codes - III.

Univariate Setting
* List-decoding
* Unbalanced Expanders

CS5.318.1
Coding Theory
Lecture 25 (2022-11-28)
Instructor: Prahladh Harsha.

Last time: List-decoding Univariate Multiplicity Codes

Step 2: Extracting $P(X) \in \mathbb{F}_{\leq d}[X]$ from $Q(X, Y_0, \dots, Y_m)$ given $Q(X, P^{(\leq m)}(X)) \equiv 0$.

Idea: (i) Guess the first few coefficients of P

$$P(X) = \sum_{i=0}^{d} P_i X^i$$

Guess $P_0, P_1 \dots P_m$.

(ii) Use Hensel lifting like procedure to obtain the remaining coefficients (if certain quantities are non-zero).

Let see: P_{m+1} from $P_0, \dots P_m$.

$$Q(X, P^{(\leq r)}(X)) \equiv 0$$

$$Q(X, P(X), P^{(1)}(X), \ldots P^{(r)}(X)) \equiv 0 \pmod{X^2}$$

$$Q(X, P_0 + P_1 X, P_1 + 2P_2 X, \ldots P_r + \binom{r+1}{r} P_{r+1} X) \equiv 0$$

(since $P(X) = \sum_{i=0}^{d} P_i X^i$

$$P^{(j)}(X) = \sum_{i=0}^{d} \binom{i}{j} P_i X^{i-j} = \sum_{i=j}^{d} \binom{i}{j} P_i X^{i-j}$$
$$= \sum_{i=0}^{d-j} \binom{j+i}{j} P_{i+j} X^i \quad)$$

Apply Taylor around the point

$$M = (0, P_0, P_1 \ldots P_r) = (0, P^{(\leq r)}(0))$$

$$Q(r) + \sum_{i=0}^{r} \left(\frac{\partial Q}{\partial Y_i}\right)(M) \cdot (i+1) P_{i+1} \cdot X + \left(\frac{\partial Q}{\partial X}\right)(M) \cdot X$$
$$+ X^2 (\qquad) \equiv 0 \pmod{X^2}$$

$\ldots (*)$

Can infer P_{r+1} from $(*)$ provided $\left(\frac{\partial Q}{\partial Y_r}\right)(M) \cdot (r+1) \neq 0$.

If $\frac{\partial Q}{\partial Y_r}(X, P^{(\leq r)}(X)) \neq 0$, then $\exists\, \alpha \in \mathbb{F}_{q^t}$ (assuming $D < q^t$)

s.t $\frac{\partial Q}{\partial Y_r}(\alpha, P^{(\leq r)}(\alpha)) \neq 0$

And expand around $(\alpha, P^{(\leq r)}(\alpha))$ instead of $M = (0, P^{(\leq r)}(0))$.

What about p_{k+r} from $p_0, \ldots p_{k+r-1}$.

- go mod x^{k+1}

$$p^{(r)}(x) \pmod{x^{k+1}}$$

$$= \sum_{i=0}^{d-r} \binom{r+i}{i} p_{r+i} x^i \pmod{x^{k+1}}$$

$$= \sum_{i=0}^{k} \binom{r+i}{i} p_{r+i} x^i \pmod{x^{k+1}}$$

$$= p^{(r)}(x) \pmod{x^k} + \binom{r+k}{r} p_{r+k} x^k$$

Coefficient of p_{r+k} in $Q(x, p^{(\leq r)}(x)) \pmod{x^{k+1}}$

$$= \left\{ \left(\frac{\partial Q}{\partial Y_r}\right)\left(x,\ p(x) \pmod{x^k},\ p^{(1)}(x) \pmod{x^k},\ \ldots\ p^{(r)}(x) \pmod{x^k}\right)\right\} \cdot \binom{r+k}{r} p_{r+k} x^k \pmod{x^{k+1}}$$

$$= \left\{ \left(\frac{\partial Q}{\partial Y_r}\right)\left(0,\ p^{(\leq r)}(0)\right)\right\} \cdot \binom{r+k}{r} p_{r+k} x^k \pmod{x^{k+1}}$$

Can infer p_{r+k} if $\left(\frac{\partial Q}{\partial Y_r}\right)(\ldots) \neq 0$ & $\binom{r+k}{r} \neq 0$

Works as long as $\mathrm{char}(\mathbb{F}) > \deg(P) = d$.

Parameter Setting:

① . $\#\text{cons} < \#\text{vars}$

② $D < TM$

—

Recall from last lecture

$(\omega_1 \ldots \omega_k) \in \mathbb{Z}_{\geq 0}^k$

$$M(\omega, t) = \#\{(a_1 \ldots a_k) \,/\, \sum \omega_i a_i \leq t\}$$

Lemma: $$\frac{\binom{t+k}{k}}{\prod \omega_i} \leq M(\omega, t) \leq \frac{\binom{t+\sum\omega_i + k}{k}}{\prod \omega_i}$$

—

① $$\#\text{vars} = \#\{(e, e_0 \ldots, e_x) \,/\, e + \sum_{j=0}^{x} (d-j) \leq D\}$$

$$\geq \frac{\binom{D+x+2}{x+2}}{\prod_{j=0}^{x}(d-j)} \geq \frac{D^{x+2}}{(x+2)!\, d^{x+1}}$$

② $$\#\text{cons} = n \cdot \#\{(e, e_0 \ldots, e_x) \,/\, e + \sum_{j=0}^{x} (b-j) e_j < M\}$$

$$< n \cdot \frac{\binom{M + x + 2 + \sum_{j=0}^{x}(b-j) + 1}{x+2}}{\prod_{j=0}^{x} (b-j)}$$

$$\leq \frac{n \cdot (M+B)^{x+2}}{(x+2)!\, (b-x)^{x+1}}$$

$B = f(b, x)$

$$\#\text{cons} < \#\text{vars} \iff \frac{D^{r+2}}{(r+2)!\, d^{r+1}} > n \cdot \frac{(M+B)^{r+2}}{(r+2)!\, (s-r)^{r+1}}$$

Satisfied if $\displaystyle \frac{D}{M+B} > \left(\frac{d}{s-r}\right)^{\frac{r+1}{r+2}} \cdot n^{1/r+2} =: A$

For every $\varepsilon \in (0,1)$

$$M = \left\lceil \frac{2B}{\varepsilon} \right\rceil \;;\quad T = (1+\varepsilon)A$$

$$D = TM - 1$$

for this setting of parameters, we have

$$D < TM \quad \checkmark$$

$$\frac{D}{M+B} > A \quad \checkmark$$

(1) & (2) are met.

List-decoding Radius:

$$1 - \frac{T}{n} = 1 - \frac{(1+\varepsilon)A}{n}$$

$$= 1 - \left(\frac{d}{s-r}\right)^{\frac{r+1}{r+2}} \left(\frac{1}{n}\right)^{\frac{r+1}{r+2}} (1+\varepsilon)$$

$$= 1 - \left(\frac{d}{sn} \cdot \frac{s}{s-r}\right)^{\frac{r+1}{r+2}} (1+\varepsilon)$$

$$= 1 - \left(\frac{s}{s-r} \cdot R\right)^{\frac{r+1}{r+2}} (1+\varepsilon)$$

$\approx 1 - R - \delta$ for appropriate choice of α & β (in terms of R & δ).

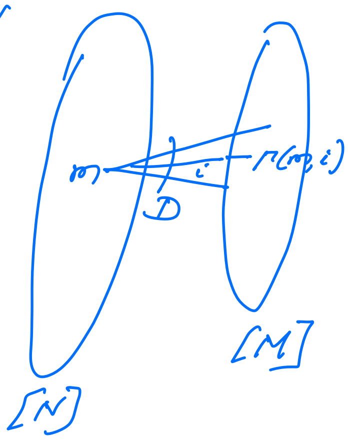
—

List-decoding & Combinatorial Constructions

$\mathcal{C} : [N] \longrightarrow \Sigma^D$ $\quad |\Sigma| = q.$

$M = D \cdot q. \quad [M] = [D] \times \Sigma$

Construct bipartite graph D-left regular



$\Gamma : [N] \times [D] \to [M]$

$(m, i) \longmapsto (i, \mathcal{C}(m)_i)$

Zero-error list-recovery of $\mathcal{C} \Rightarrow$ Expansion of Γ.

(L, R, E) is a (K, A)-expander if

$\forall S \subseteq L, \quad |S| \le K \Rightarrow |\Gamma(S)| \ge A|S|$

Desired expansion $\quad A > 1 + \delta$

Best possible expansion $\quad A \approx D(1 - \delta)$

(lossless expansion) $\quad$ where D- left regularity.

Unbalanced Expander: $M \ll N$

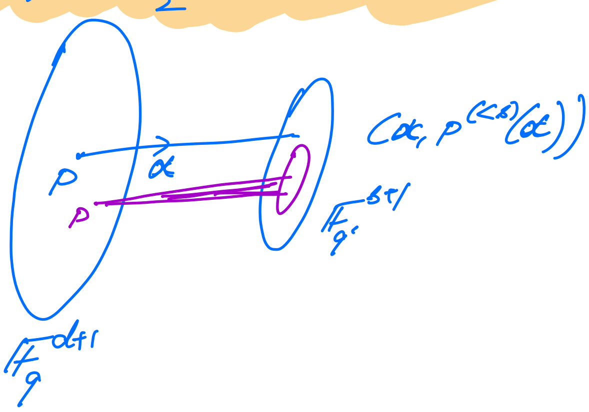
Guruswami-Umans-Vadhan:
Variant Folded-RS codes $\rightarrow$ lossless unbalanced expanders
w/ deg - polylog n.

Kalev. Ta-Shma
Multiplicity codes also suffice.

<u>Thm</u> $\forall \mathbb{F}_q$, s, d such $15 \leq s+1 \leq d \leq \operatorname{char}(\mathbb{F}_q)$
there exists an explicit graph

$$\Gamma: \mathbb{F}_q^{d+1} \times \mathbb{F}_q \longrightarrow \mathbb{F}_q \times \mathbb{F}_q^{s}$$

which is a (K, A)-expander for every $K > 0$
& $A = q - \frac{d(s+1)}{2} (qK)^{\frac{1}{s+1}}$



For any set $W \subseteq \mathbb{F}_q^{s+1}$

$$LIST(W) = \{ p \in \mathbb{F}_q^{d+1} \mid \Gamma(p) \subseteq W \}$$

To prove expansion factor of A for sets of size K suffices to prove the following:

$$\forall\, W \subseteq \mathbb{F}_q^{s+1} \text{ s.t } |W| \leq AK-1 \Rightarrow LIST(W) < K$$

Step 1: Find a $Q(X, Y_0, \ldots Y_{s-1})$ s.t

(i) $\forall (\alpha, \bar{\beta}) \in W, \quad Q(\alpha, \bar{\beta}) = 0$

(ii) $(1, d, d-1, \ldots, d-(s-1))$-wt deg of $Q \leq D$.

Step 1 works if $\#\text{cons} = |W| \leq \#\text{vars}$

$$\#\text{vars} \geq \frac{\binom{D+s+1}{s+1}}{\prod_{j=0}^{s-1}(d-j)} \geq \frac{D^{s+1}}{(s+1)!\, d^s}$$

Choose $D > \left(d^s \cdot |W| \cdot (s+1)!\right)^{\frac{1}{s+1}}$

For every P s.t $\Gamma(P) \subseteq W$

$R(X) \equiv Q(X, P^{(<s)}(X))$

$\forall \alpha \in \mathbb{F}_q; \quad R(\alpha) = 0 \quad \& \quad D < q. \Rightarrow R \equiv 0$

P satisfies $Q(X, P^{(<s)}(X)) \equiv 0$

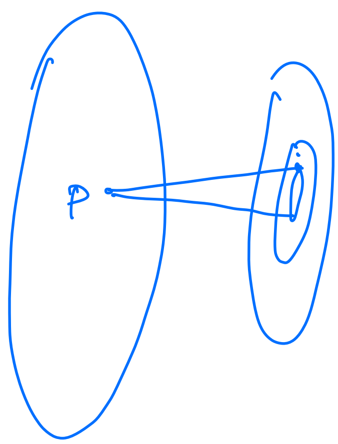
We need to carefully find

$\#\{P \mid Q(x, P^{(<s)}(x)) \equiv 0\}$.

Recall Extraction of P from Q.

- Can extract if $\exists$ pt $\alpha \in \mathbb{F}_q$ s.t.

$$\left(\frac{\partial Q}{\partial Y_{s-1}}\right)(\underbrace{\alpha, P^{(<s)}(\alpha)}_{(\alpha,\beta)}) \not\equiv 0$$



W

<u>Solve (W, Q)</u>

(1) $Q \in \mathbb{F}[X, Y_0 \dots Y_{s-1}]$

(2) Let s^* be the largest var in $[0,..s-1]$ that Q depends on.
If no such s^* exists output $\mathcal{L} \leftarrow \emptyset$

(3). $\mathcal{L}_1 \leftarrow \emptyset$

(4) $W_1 \leftarrow \{(\alpha,\bar{\beta}) \in W \mid \left(\frac{\partial Q}{\partial Y_{s-1}}\right)(\alpha,\beta) \neq 0\}$.

(5) For each $(\alpha,\bar{\beta}) \in W_1$
extract P from Q. s.t.
(i) $P^{(<s)}(\alpha) = \beta$
(ii) $Q(x, P^{(<s)}(x)) \equiv 0$
If $\Gamma(P) \subset W_1$ add P to $\mathcal{L}_1$

(6) Set $W_0 \leftarrow W \setminus W_1$

(7) $\mathcal{L}_0 \leftarrow \text{Solve}\left(\frac{\partial Q}{\partial Y_{s-1}}, W_0\right)$

(8) Output $\mathcal{L}_1 \cup \mathcal{L}_0$.

— Bounding list-size:

Claim: $|\mathcal{L}| \leq \frac{|W|}{q-D}$

Pf: By induction on $(0,1,1,\ldots,1)$-deg of Q.

By Induction $|\mathcal{L}_0| \leq \frac{|W_0|}{q-D}$

Suffices for us to prove $|\mathcal{L}_1| \leq \frac{|W_1|}{q-D}$

Qn: For a given $P \in \mathcal{L}_1$, how many $(\alpha,\beta) \in W_1$ give raise to P.

Every $(\alpha, P^{(<s)}(\alpha))$ s.t $\left(\frac{\partial Q}{\partial Y_{s-1}}\right)(\alpha, P^{(<s)}(\alpha)) \neq 0$

gives raise to P.

$\deg\left(\frac{\partial Q}{\partial Y_s}(X, P^{<s}(X))\right) \leq D$

Hence, there are at least $(q-D)$ non-zeros

of $\left(\frac{\partial Q}{\partial Y_s}\right)(X, P^{(<s)}(X))$

Hence $|\mathcal{L}_1| \leq |W_1|/q-D$ ☒.