Today
- Multiplicity Codes - II.

CS5.318.1
Coding Theory
Lecture 24 (2022-11-23)
Instructor: Prahladh Harsha.

List-decoding univariate multiplicity codes

Kopparty, Guruswami-Wang

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

Problem: Given n data points

$(\alpha_1, \beta_1), (\alpha_2, \beta_2) \ldots (\alpha_n, \beta_n) \in \mathbb{F}_q \times \mathbb{F}_q^s$

find all (univariate) polynomials P of deg $\leq d$ s.t.

$$\left| \{ i \in [n] \mid P^{(<s)}(\alpha_i) = \beta_i \} \right| \geq T$$

Warmup: Recall the Guruswami-Sudan setting $\beta_i \in \mathbb{F}$ (poly evaluation)

GS Algorithm

Step 1: Find a non-zero poly $Q \in \mathbb{F}[X,Y]$ s.t

(i) $(1,d)$-wt degree of $Q \leq D$

(ii) Q vanishes w/ multiplicity M at (α_i, β_i), $\forall i \in [n]$.

Step 2: Output all polynomials P of deg $\leq d$ s.t

$$Q(X, P(X)) \equiv 0.$$

Analysis: Step 1: Doable as long as #vars > #cons

Step 2: Let P be a candidate poly that has agreement at least T

$$R(X) \equiv Q(X, P(X))$$

For each pt of agreement (α_i, β_i)

R had M roots at α_i.

If $D < TM \Rightarrow R \equiv 0$

Idea: [Kopparty] Extend the above plan to the multiplicity setting.

$Q(X, Y_0, Y_1 \ldots Y_r) \in \mathbb{F}[X, Y_0, \ldots Y_r]$

Design choice: $0 \le r \le s-1$

$Y_i \approx P^{(i)}(X)$

wt of Y_i in Q - $(d-i)$

#vars $(1, d, d-1, \ldots, d-r)$-wt deg of $Q \le D$

(i.e. for each monomial $X^e Y_0^{e_0} Y_1^{e_1} \ldots Y_r^{e_r}$

$$e + \sum_{j=0}^{r} (d-j) e_j \le D.$$

#vars $= \#\{(e, e_0, \ldots, e_r) \mid e + \sum (d-j) e_j \le D\}$

- Estimate number of such monomials.

#cons: $n \cdot$ #cons of "Q has mult M at pt (α, β)"

(α_i, β_i) $\qquad P^{(<s)}(\alpha_i) = \beta_i$

$$R_i(X) \triangleq \sum_{j=0}^{s-1} (\beta_i)_j (X - \alpha_i)^j$$

Observe: If P agrees w/ data at (α_i, β_i)

$$P(X) \equiv R_i(X) \pmod{(X-\alpha_i)^s}$$

$\forall j < s \qquad P^{(j)}(X) \equiv R_i^{(j)}(X) \pmod{(X-\alpha_i)^{s-j}}$

$\underline{\text{Pf:}}$ $P(x) = R_i(x) + Q(x)(x-\alpha_i)^s$

$\forall i$, The following is a basis for $\mathbb{F}[X, Y_0 \dots Y_r]$

$$\mathcal{B}_i := \left\{ (X-\alpha_i)^e \prod_{j=0}^{r} \left(Y_j - R_i^{(j)}(X)\right)^{e_j} \;\middle|\; e, e_0, \dots e_r \in \mathbb{Z}_{\geq 0} \right\}$$

For each P & an agreement (α_i, β_i)

$$R(x) = Q(x, P^{(\leq r)}(X))$$

At a point of agreement

$$R_i^{(j)}(x) = P^{(j)}(x) \pmod{(x-\alpha_i)^{s-j}}$$

Reverse-Engineering the multiplicity requirement

Coeffs of $\{(e, e_0 \dots e_r) \mid e + \sum (s-j) e_j < M\} = \mathcal{B}_i(M)$ are zero

then $R(x)$ has multiplicity $\geq M$ at α_i.

$\underline{\text{For}}$ the monomial (basis elt)

$$(X-\alpha_i)^e \prod_{j=0}^{r} \left(Y_j - R_i^{(j)}(X)\right)^{e_j}$$

- multiplicity $e + \sum_{j=0}^{r} (s-j) e_j = t$

$$\#\text{cons} = n \cdot \#\left\{(e, e_0 \dots e_r) \mid e + \sum_{j=0}^{r} (s-j) e_j < M\right\}$$

Counting number of integral pts under a hyperplane

k - dimensions

ω - $(\omega_1 \dots \omega_k) \in \mathbb{Z}_{>0}$ weight vector.

t - target

$$N(\omega, t) = \{(a_1 \dots a_k) \mid \sum \omega_i a_i \leq t\}.$$

$$n(\omega, t) = |N(\omega, t)|$$

Claim: $\dfrac{\binom{t+k}{k}}{\prod \omega_i} \leq n(\omega, t) \leq \dfrac{\binom{t+\sum\omega_i + k}{k}}{\prod \omega_i}$

Pf: For any integer l

$$P(l) = \{\underset{\in \mathbb{Z}^k_{\geq 0}}{(x_1 \dots x_k)} \mid \sum x_i \leq l\} \; ; \; |P(l)| = \binom{l+k}{k}$$

$$B(a_1 \dots a_k) = \{(x_1 \dots x_k) \in \mathbb{Z}^k_{\geq 0} \mid \omega_i a_i \leq x_i < \omega_i(a_i+1) \;\; \forall i\}$$

$$|B(a)| = \prod \omega_i$$

$x \in P(t) \Rightarrow \exists\, \bar{a}$ s.t. $x \in B(\bar{a})$ & $a \in N(\omega, t)$

$$\Rightarrow \bigcup_{\bar{a} \in N(\omega,t)} B(\bar{a}) \supseteq P(t) \quad \dots \quad (*)$$

$$n(\omega, t) \cdot \prod \omega_i \geq \binom{t+k}{k}$$

$$P(t + \sum \omega_i) \supseteq \bigcup_{\bar{a} \in N(\omega,t)} B(\bar{a})$$

$$n(\omega, t) \cdot \prod \omega_i \leq \binom{t + \sum \omega_i + k}{k}$$

$\boxtimes$

Step 1: Find a non-zero $Q \in \mathbb{F}[X, Y_0, \ldots, Y_r]$

(i) $(1, d, d-1, \ldots, d-r)$-wt deg of $Q \leq D$

(ii) For each $i \in [n]$, Q when written in the basis B_i has 0 coefficients of $B_i(M)$.

Step 1 is guaranteed to find a Q if #cons < #vars.

Analysis of

Step 2: Let P be a polynomial that agrees w/ T points of the data.

$$R(X) \equiv Q(X, P^{(\leq r)}(X)) \quad (\deg(R) \leq D)$$

has $\geq TM$ roots w/ multiplicities

Hence if $D < TM$, $R \equiv 0$.

Step 2: Find every polynomial P of $\deg \leq d$ s.t $Q(X, P^{(\leq r)}(X)) \equiv 0$.

Extracting P from $Q(X, Y_0 \dots Y_r)$

i.e. find $P(X) = \sum_{i=0}^{d} P_i X^i$ s.t. $Q(X, P(X), P^{(1)}(X) \dots, P^{(r)}(X)) \equiv 0.$

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

Guess $P_0, P_1 \dots, P_r \in \mathbb{F}_q^{r+1}$

lets find P_{r+1}

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

$$Q(X, P_0 + P_1 X, P_1 + 2P_2 X, \dots, \alpha \cdot P_{r-1} + \beta P_r X) \equiv 0 \pmod{X^2}$$

$$Q(\overbrace{(0, P_0, P_1 \dots}^{\tilde{P}}) + X(\overbrace{\quad\quad}^{P'}))$$

$$= Q(\tilde{P}) + \left(\frac{\partial Q}{\partial X}\right)_{\tilde{P}} X + \sum_{j=0}^{r} \left(\frac{\partial Q}{\partial Y_j}\right)_{\tilde{P}} P'_j X$$

$$\pmod{X^2}$$

Can extract P_r if its accompanying coefficient is non-zero.

Accompanying Coefficient $= \left(\frac{\partial Q}{\partial Y_r}\right)_{\tilde{P}} \binom{r+1}{r}$

Choose char of field large enough st all the binomial coefficients are non-zero

$$\frac{\partial Q}{\partial Y_n}\left(x, P^{(\leq n)}(x)\right) \equiv 0$$

Work w/ $\frac{\partial Q}{\partial Y_n}$ instead of Q.

$\boxtimes$

Guruswami-Wang. Find Q of the form

$$A(x) + A_0(x) Y_0 + A_1(x) Y_1 + \dots + A_n(x) Y_n$$

(several steps become easier).