Apr 27

REMINDERS

(•) Video due in 2 WEEKS! 11:59pm on Wed, May 11

(•) Delay in HW 6 grading + HW5 re-grading

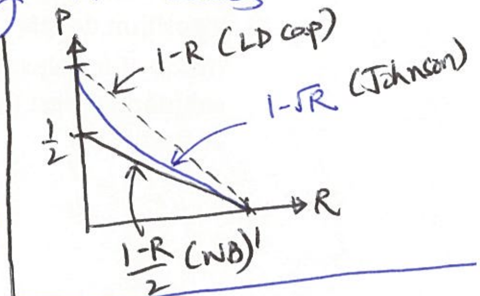
(•) Lag in grading of proof reading

RECAP — List decoding RS codes

Generic RS (list) decoder

Step 1 (Interpolation) Compute non-zero $Q(X,Y)$ with "some properties" s.t. $\forall i \in [n]$, $Q(\alpha_i, y_i) = 0$

Step 2 (Root finding) Compute all factors $Y - P(X)$ of $Q(X,Y)$ s.t. (i) $\deg(P) < k$; (ii) $P(\alpha_i) = y_i$ for at least t values $i \in [n]$



i/p: $(\alpha_1, y_1), \ldots, (\alpha_n, y_n)$

o/p: ALL $P(X)$ of deg $< k$ s.t. $P(\alpha_i) = y_i$ for at least t values of $i \in [n]$

Generic RS decoder is poly runtime:

(Step 1) Use Gaussian elimination (need #vars > #eqns)

(Step 2) Use poly time factoring algo for $Q(X,Y)$ as a black box (App D.7.3 in the book)

Algo 1	$1 - 2\sqrt{R}$	$t \geq 2\sqrt{nk}$	$\deg_X(Q) \leq \sqrt{n(k-1)}$, $\deg_Y(Q) \leq \sqrt{\frac{n}{k-1}}$
Algo 2	$1 - \sqrt{2R}$	$t \geq \sqrt{2nk}$	$(1, k-1)$ wt. deg of $Q \leq \sqrt{\boxed{2}n(k-1)}$
Algo 3	$1 - \sqrt{R}$	$t \geq \sqrt{nk}$	TODAY

Def: $(1,\omega)$ wt deg of $X^i Y^j$ is $i + \omega j$

$(1,\omega)$ ____ $Q(X,Y)$ is largest $(1,\omega)$-wt deg of any monomial in $Q(X,Y)$

TODAY

(•) Proof readers: Christopher, Larry

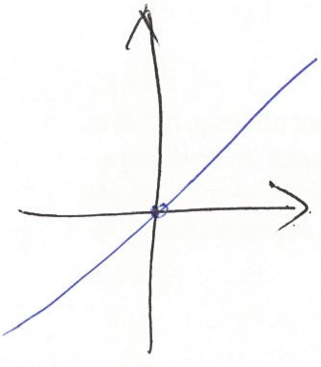
(•) Algo 3 (Guruswami, Sudan '98)

(•) List decoding beyond $1-\sqrt{R}$ ($\rightarrow 1-R$ frac. of errors)

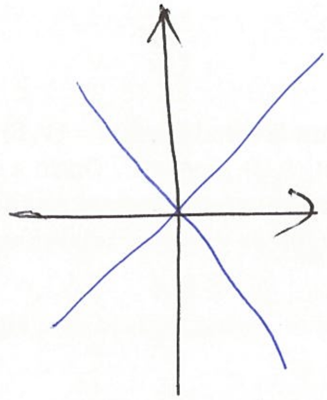
Idea behind Algo 3: still look at $(1,k-1)$ wt deg of $Q \leq D$

+ make sure $Q(X,Y)$ "passes through" each (α_i, y_i) r times

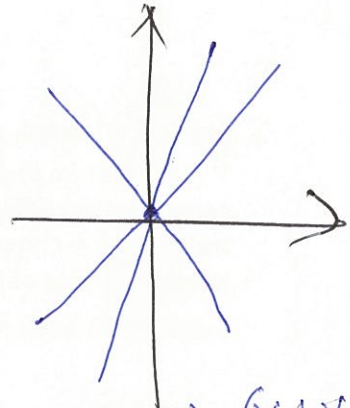
$\Rightarrow$ affects $D \uparrow r$ & #equations $\uparrow r$



$Q(X,Y) = Y - X$
passes through $(0,0)$ once



$Q(X,Y) = (Y+X)(Y-X) = Y^2 - X^2$
passes thru $(0,0)$ 2 time



$Q(X,Y) = (Y+X)(Y-X)(Y-2X) = Y^3 - 2XY^2 + 2X^3$
passes thru $(0,0)$ 3 times

Def: $Q(X,Y)$ passes through $(0,0)$ r times if it doesn't have any monomial of total deg $\le r-1$ $\Rightarrow \binom{r+1}{2}$ such monomials

Def: $Q(X,Y)$ has a <u>root</u> at (α,β) with multiplicity of r if $Q_{\alpha,\beta}(X,Y) = Q(X+\alpha, Y+\beta)$ passes through $(0,0)$ r times

---

Algo 3: Step 1: Compute non-zero $Q(X,Y)$ w/ $(1,k-1)$ wt. deg $\le D$ s.t. $Q(X,Y)$ has root at (α_i, y_i) with mult. of r for ALL $i \in [n]$.

Correctness (Step 1): ie $\exists$ non-zero $Q(X,Y)$ that satisfies Step 1 $\Leftarrow$ if #vars > #eqns

$\#\text{vars} \ge \frac{D(D+1)}{2(k-1)}$ (same argument as in Algo 2)

$\#\text{eqns} = n \cdot \binom{r+1}{2}$ $\rightarrow$ fix $i \in [n]$ $Q_{\alpha_i, y_i}(X,Y)$ has no monomial X^iY^j s.t. $i+j \le r-1$

$$Q(X,Y) = \sum_{\substack{i,j \ge 0 \\ i+(k-1)j \le D}} c_{ij} X^i Y^j$$

coeff of X^iY^j is a linear combination of c_{ij}'s

Want: $\frac{D(D+1)}{2(k-1)} > n\binom{r+1}{2} \Leftarrow \boxed{D = \sqrt{n(k-1)r(r-1)}}$

<u>Correctness of Step 2</u>: If $\deg(P) \le k-1$ & $P(\alpha_i) = y_i$ for $t \ge \sqrt{nk}$ locations $i \in [n]$

$$\Rightarrow Y - P(X) \mid Q(X,Y) \equiv Q(X, P(X)) = 0$$

<u>Lem:</u> If $P(\alpha_i) = y_i \Rightarrow (X-\alpha_i)^r \mid R(X) = Q(X, P(X))$

(recall: $R(\alpha_i) = Q(\alpha_i, P(\alpha_i)) = Q(\alpha_i, y_i) = 0$)

$\Rightarrow$ # roots $\ge rt$

By degree mantra we have $R(X) \equiv 0$ if $rt > D \ge \deg(R)$

By choice of D from step 1 we're good if $rt > \sqrt{n(k-1)r(r-1)}$

$$\Leftrightarrow t > \sqrt{n(k-1)\left(1-\tfrac{1}{r}\right)}$$

Pick $r = 2(k-1)n \Rightarrow$ we need $t > \sqrt{n(k-1)}$

But above is true if $t \ge \sqrt{nk}$ $\blacksquare$

<u>So far in LD</u>

(•) Best efficient LD algo corrects $1-\sqrt{R}$ frac of errors (still best for RS codes)

(•) $\exists$ $\left(1-R-\varepsilon, O\left(\frac{1}{\varepsilon}\right)\right)$-list decodable of rate R w/ $q \ge 2^{\Omega(1/\varepsilon)}$

<u>Q</u>: Can we LD <u>$1-R-\varepsilon$</u> frac of errors in poly time for some code of rate R? $L \le \mathrm{poly}(n)$?

A: <u>Yes</u> $\rightarrow$ Folded RS (Parvaresh–Vardy '05, Guruswami, R. '06)

<u>Folded RS codes</u>: Consider $[n,k]_q$ RS codes where eval pts are $1, \gamma, \gamma^2, \ldots, \gamma^{n-1}$ where γ generates $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$

folding $m=2$

$f(1)$	$f(\gamma)$	$f(\gamma^2)$	$\cdots$	$f(\gamma^{n-1})$

$\Downarrow$ $m=2$

$f(1)$ $f(\gamma)$	$f(\gamma^2)$ $f(\gamma^3)$	$\cdots$	$f(\gamma^{n-2})$ $f(\gamma^{n-1})$

For general $m \ge 1$ s.t. $m \mid n$

$f(1)$	$f(\gamma)$	$\cdots$	$f(\gamma^{n-1})$

$$\left[\begin{array}{c|c|c|c} f(1) & f(r^m) & & f(r^{n-m}) \\ f(r^2) & f(r^{m+1}) & & \vdots \\ \vdots & \vdots & \cdots & \vdots \\ f(r^{m-1}) & f(r^{2m-1}) & & f(r^{n-1}) \end{array}\right]$$

$$[n,k]_q \longrightarrow [\quad] \left(\frac{n}{m}, \frac{k}{m}\right)_{q^m}$$

$$(q^m)^{\frac{k}{m}} = q^k$$