May 1 | 1 min checkin

REMINDERS

(•) Video due in bit less than 2 weeks (11:59pm, Sun, May 14)
→ Make sure to follow ALL instructions

RECAP

(•) List decoding RS codes
(→) Input: $(\alpha_1, y_1), (\alpha_2, y_2), \dots, (\alpha_n, y_n) \in \mathbb{F}_q^2$
(→) Output: ALL poly $P(X)$ of deg $< k$ s.t. $P(\alpha_i) = y_i$ for at least t values of $i \in [n]$

(•) 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 $Q(X,Y)$ and output all such $P(X)$ with (i) $\deg(P) < k$ (ii) $P(\alpha_i) = y_i$ for at least t values of $i \in [n]$

(•) Welch-Berlekamp algo: $Q_{WB}(X,Y) = Y E(X) - N(X)$
monic $\deg = e$; $\deg \le k+e-1$

(•) Algo 1: Pick $Q(X,Y)$ that satisfies step 1 with $\deg_X(Q) \le \ell$, $\deg_Y(Q) \le \frac{n}{\ell}$
[→ #vars $= (\ell+1)(\frac{n}{\ell}+1) > n = $ #eqns $\Rightarrow$ a non-zero Q satisfying step 1 always $\exists$

Plan for today (•) Correctness of step 2 (for Algo 1) $1-2\sqrt{R}$ (•) Algo 2: $1-\sqrt{2R}$

Computational consideration:
(Step 1) Feasible if # vars/coeffs $> n$. Solve this via Gaussian Elimination (Q2 on HW0)
$O(n^3)$ time/ops $\Leftarrow$ #vars is $O(n)$

(Step 2) $\exists$ a poly time algo to factorize any $Q(X,Y)$ (w/ poly(n) $\deg_X(Q)$, $\deg_Y(Q)$)
use as a black box
$Q(X,Y)$ poly(n)
Q need not have any linear factors
over $\mathbb{F}_3$ $X^4 + 2X^2Y^2 + Y^4 = (X^2+Y^2)^2$

$\Rightarrow$ Algo 1, 2, 3 run in poly(n) time

Changed the properties of $Q(X,Y)$ ←	Algo 1	Algo 2	Algo 3
frac of errors	$1-2\sqrt{R}$	$1-\sqrt{2R}$	$1-\sqrt{R}$
t	$2\sqrt{nk}$	$\sqrt{2nk}$	$\sqrt{nk}$
R for which frac of errors $> \frac{1-R}{2}$	$R < 0.07$	$R < \frac{1}{3}$	$R < 1$

(Algo 1) After Step 1, $\exists$ a non-zero $Q(X,Y)$ w/ $\deg_X(Q) \le l$, $\deg_Y(Q) \le \frac{n}{l}$ & $\forall i \in [n]$ $Q(\alpha_i, y_i) = 0$

Correctness of Step 2: For ANY $Q(X,Y)$ s.t. ↑ if $P(X)$ has deg $< k$ and $P(\alpha_i) = y_i$ for at least t values of $i \in [n] \Rightarrow$

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

Pf: $R(X) \overset{\text{def}}{=} Q(X, P(X))$ Goal: Show $R(X) = 0$

Goal: show $R(X)$ has $> \deg(R)$ roots.

Count the roots of $R(X)$:

$$R(\alpha_i) = Q(\alpha_i, P(\alpha_i)) \underset{\text{if } P(\alpha_i) = y_i}{=} Q(\alpha_i, y_i) = 0$$

$\Rightarrow$ $R(X)$ has $\ge t$ roots

$a \le l$

$b \le \frac{n}{l}$

Degree of $R(X)$:

$$X^a Y^b \text{ in } Q(X,Y) \xrightarrow{Y \leftarrow P(X)} \underbrace{X^a (\underbrace{P(X)}_{\le k-1})^b}_{\le (k-1)b + a}$$

$\le \frac{n}{l}(k-1) + l$

$\Rightarrow \deg(R) \le l + \frac{n}{l}(k-1)$

pick l s.t. $l = \frac{n(k-1)}{l}$

$\Leftrightarrow l^2 = n(k-1) \Leftrightarrow l = \sqrt{n(k-1)}$

$$\Rightarrow \deg(R) \le \sqrt{n(k-1)} + \frac{n(k-1)}{\sqrt{n(k-1)}} = 2\sqrt{n(k-1)} < 2\sqrt{nk}$$

$$\Rightarrow \# \text{roots of } R \ge t \ge 2\sqrt{nk} > \deg(R) \xRightarrow[\text{degree mantra}]{\text{by}} R(X) = 0$$

Note: $X^a Y^b$ in $Q(X,Y)$ $\xrightarrow{Y \leftarrow P(X)}$ $X^a (P(X))^b$ $\le a + (k-1) b$, $a \le \ell$, $b \le \frac{n}{\ell}$

Def. $(1,w)$ - wt degree of a $X^a Y^b$ $= a + w \cdot b$

Def. $(1,w)$ - wt degree of $Q(X,Y)$ is max $(1,w)$-wt degree of any monomial in Q.

Note: $(1,1)$-wt degree of $Q(X,Y)$ is total degree / degree.

Ex: $\underline{X^5 Y} + XY^2$

$(1,1)$ wt deg $= \max(5+1=6, 1+2=3) = 6$

$(1,5)$ wt deg $= \max(5+5\times1=10, 1+2\times5=11) = 11$

Lemma: Let $\deg(P(X)) \le w$ & let $Q(X,Y)$ has $(1,w)$-wt. degree $\le D$
$\Rightarrow Q(X, P(X))$ has degree $\le D$.

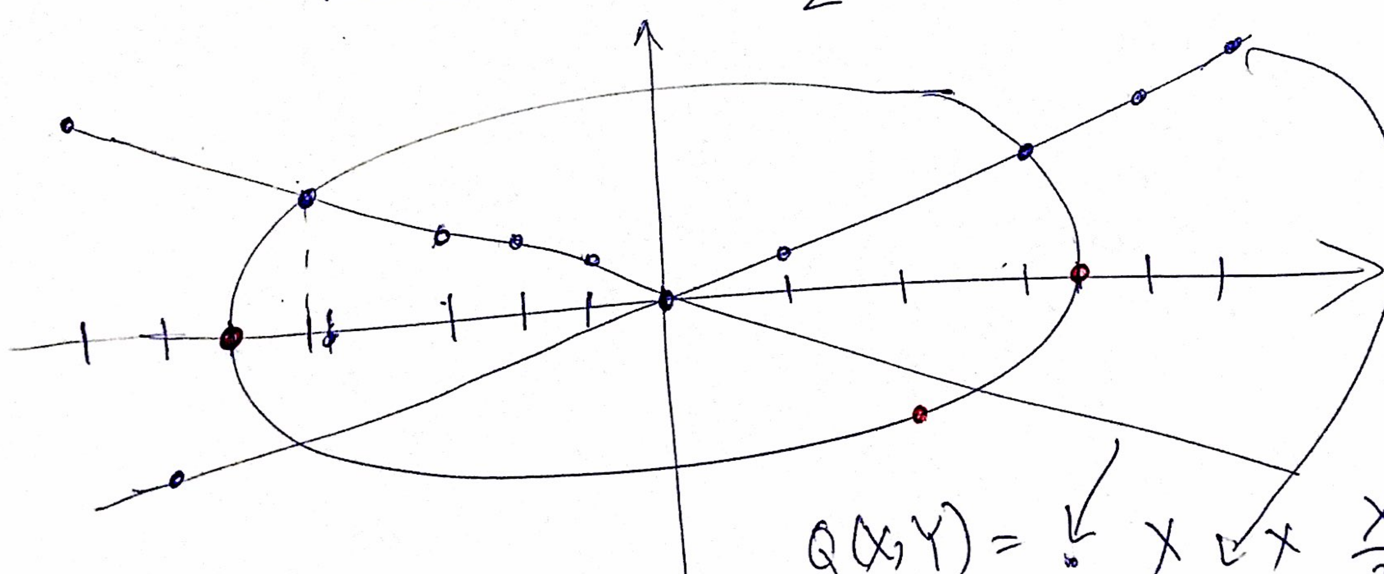
$X^a Y^b \to X^a P(X)^b$, deg $\le a + w \cdot b$

In our case: $(1, k-1)$ wt. degree

Algo 2 idea! Compute a non-zero $Q(X,Y)$ s.t. its $(1,k-1)$ wt deg $\le D$ s.t. $\forall i \in [n]$ $Q(\alpha_i, y_i) = 0$

Back to an example: $n = 14$, $k = 2$ (lines), $e = 9$, $t = n - e = 5$

Unique decoding $t > \frac{n+k}{2} = \frac{16}{2} = 8$



$Q(X,Y) = 1 \cdot X \cdot X \cdot \frac{X^2}{?} + \frac{Y^2}{?}$

$\to$ Algo 2: runtime is poly(n).