May 3 | 1 min checkin

REMINDER

(·) Video (+ peer survey) due in ~1.5 weeks (11:59pm Sun, May 14)

RECAP

Input: $(\alpha_1, y_1), \ldots, (\alpha_n, y_n) \in \mathbb{F}_q^2$
Output: All $P(X)$ of deg $< k$ s.t. $P(\alpha_i) = y_i$ for $\geq t$ 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 $Q(X,Y)$ s.t. (i) $\deg(P) < k$ and (ii) $P(\alpha_i) = y_i$ for at least t values $i \in [n]$

Generic RS decoder is poly runtime

(Step 1) Use Gaussian Elimination (#vars > #eqns)

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

Algorithm 2 (Sudan '96)

(Step 1) Compute non-zero $Q(X,Y)$ with $(1, k-1)$ wt. degree $\leq D$ ← TBD
s.t. $\forall i \in [n]$, $Q(\alpha_i, y_i) = 0$

Plan for today | (·) Prove correctness of Algo 2 (·) Algo 3 → $1-\sqrt{R}$ frac of errors

Algo 2: runtime is poly(n) as the generic RS ld algo is poly(n)

Correctness: Step 1: #vars > n

$$Q(X,Y) = \sum_{\substack{a,b \\ 0 \leq a+(k-1)b \leq D}} q_{ab} X^a Y^b$$

const $Q(\alpha_i, y_i)$

α_i y_i

variables

We need $\boxed{\#\text{coeff} > n}$ ($\Rightarrow$ Step 1 is correct ✓)

Claim: # coefficients $\geq \dfrac{D(D+2)}{2(k-1)}$

$(1,w)$-wt deg $\leq D$: $\dfrac{D(D+2)}{2w}$

$$\Leftarrow \frac{D(D+2)}{2(k-1)} > n \Leftrightarrow D(D+2) > 2n(k-1)$$

$$D = \sqrt{2n(k-1)} \quad \Leftarrow D^2 \geq 2n(k-1)$$

Step 2: Iff $P(X)$ s.t $\deg(P) < k$ & $P(\alpha_i) = y_i$ for atleast t values of $i \in [n]$ $\Rightarrow$ $Y - P(X) \mid Q(X,Y)$

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

Lemma 1: If $\deg(P(X)) \leq w$, $(1,w)$-wt deg of $Q(X,Y) \leq D$
$\Rightarrow \deg(Q(X,P(X))) \leq D$

$R(X) = Q(X, P(X))$ Goal: $R(X) = 0$

(Lemma 1) $\Rightarrow \deg(R) \leq D$

Roots: Let $i \in [n]$ be s.t

~~if~~ $P(\alpha_i) = y_i$ Step 1

$$R(\alpha_i) = Q(\alpha_i, P(\alpha_i)) = Q(\alpha_i, y_i) \stackrel{\downarrow}{=} 0$$

$\Rightarrow R$ has $\geq t$ roots

By degree mantra   if # roots $>$ deg $\Rightarrow R(X) = 0$

$$\Leftarrow t > D \geq \deg(R)$$

We want $\underset{\text{\# roots of } R \geq}{t} > D = \sqrt{2n(k-1)}$

$\Leftarrow t \geq \sqrt{2nk}$ $\Rightarrow$ frac of errors $= \dfrac{n - \sqrt{2nk}}{n} = 1 - \sqrt{2R}$

Lemma 2: # coeff of a poly of $(1,w)$ wt deg $\leq D$ is $\geq \dfrac{D(D+2)}{2w}$

Pf:

$$\text{\# coeff} = \left| \{ (a,b) \mid a,b \geq 0, a + wb \leq D \} \right|$$

implicit $a \leq D - bw$

$a + wb \leq D \Rightarrow b \leq \left\lfloor \frac{D}{w} \right\rfloor \stackrel{\text{def}}{=} l$ $l + 1 \geq \frac{D}{w}$ $l \leq \frac{D}{w}$ $\Rightarrow wl \leq D$ $\Rightarrow D - wl \geq 0$

$$\text{\# coeff} = \sum_{b=0}^{l} \sum_{a=0}^{D-bw} 1 = \sum_{b=0}^{l} (D - bw + 1)$$

$$= \sum_{b=0}^{l} (D+1) - w \sum_{b=0}^{l} b = (D+1)(l+1) - w\frac{l(l+1)}{2}$$

$$= \frac{l+1}{2}\left(2D + 2 - wl\right)$$

$$\geq \frac{(\ell+1)}{2}(D+2) \geq \frac{D(D+2)}{2w} \qquad \blacksquare$$

Algo 3 (Guruswami–Sudan '98) $1-\sqrt{R}$

$(X-2)$ $(X-2)^2$

↑

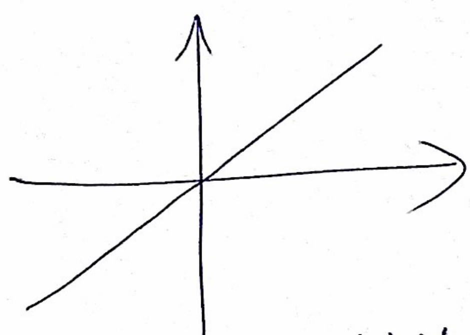
1 root

Note: Degree mantra holds even when we count roots with multiplicities

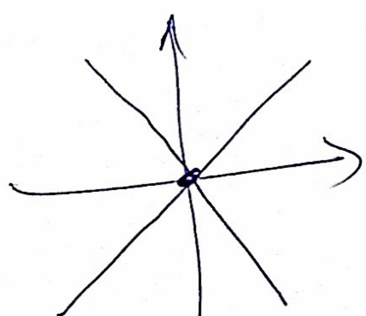
Idea behind Algo 3 (Step 1) still look at $(1,k-1)$ wt deg of $Q \leq D$

(Step 2 & is the same) + make $Q(X,Y)$ pass through each (α_i, y_i) r times

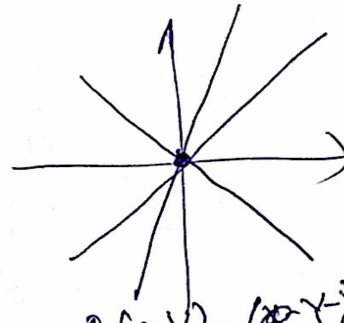
→ both degree & roots of $R(X)$ increase but at different rates $1-\sqrt{2R} \to 1-\sqrt{R}$



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



$Q(X,Y) = (Y-X)(X+Y) = Y^2 - X^2$ passes through $(0,0)$ twice



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

Def: $Q(X,Y)$ passes through $(0,0)$ r times if it doesn't have any monomial $X^a Y^b$ s.t. $a+b \leq r-1$

Def: $Q(X,Y)$ has a root at (α,β) with multiplicity 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 $Q(X,Y)$ of $(1, k-1)$ wt. deg $\leq D$ s.t for all $i \in [n]$ $Q(X,Y)$ has (α_i, y_i) as a root with multiplicity r.

TBD

Correctness (Step 1) $\exists$ a non-zero $Q(X,Y)$ s.t

$$\# \text{coeff} \geq \frac{D(D+2)}{2(k-1)}$$

$\#$ ~~roots~~ equation $\Rightarrow$ $n \cdot$ function of (r)

$$n \cdot \binom{r+1}{2}$$

$a, b \geq 0$

$\#(a,b)$ s.t $a+b \leq r-1$

$$\binom{r+1}{2}$$