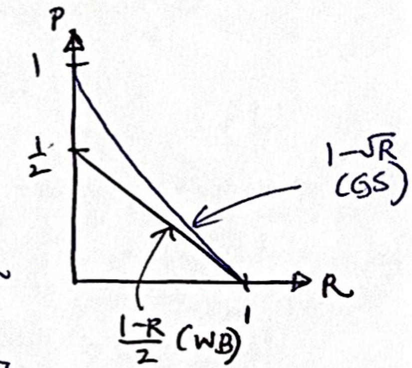
Apr 25

(•) Video due in ~ 2.5 weeks (11:59pm, Wed, May 11)
→ Autolab is accepting video submissions
→ Make sure you follow ALL instructions

REMINDERS

RECAP List Decoding RS codes

Generic RS decoder



Step 1 (Interpolation): Compute non-zero $Q(X,Y)$ 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 $P(X)$ ~~s.t.~~ with
① $\deg(P) < k$ and ② $P(\alpha_i) = y_i$ for at least t values of $i \in [n]$

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 $i \in [n]$

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

(•) 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 ⇒ a non-zero Q satisfying Step 1 + $\deg_X$ & $\deg_Y$ constraints always ∃)

Computational considerations

(Step 1) Feasible if # vars > # eqns. Solved e.g. by Gaussian Elimination (see Q2 on HW0)

(Step 2) $\underbrace{\exists \text{ poly time algo}}_{\text{Use as a black box}}$ to factorize any bi-variate poly (with poly(n) degree) $Q(X,Y)$

need not only have linear factors

E.g. over $\mathbb{F}_3$ $X^4 + 2X^2Y^2 + Y^2 = (X^2+Y^2)^2$

⇒ Algos 1-3 are poly time

Only conditions on Q change ⟸	Algo 1	Algo 2	Algo 3
fraction of errors	$1-2\sqrt{R}$	$1-\sqrt{2R}$	$1-\sqrt{R}$
t	$2\sqrt{nk}$	$\sqrt{2nk}$	$\sqrt{nk}$

(•) $1-2\sqrt{R} > \frac{1-R}{2}$ for $R < 0.07$

(•) $1-\sqrt{2R} > \frac{1-R}{2}$ for $R < \frac{1}{3}$

(•) $1-\sqrt{R} > \frac{1-R}{2}$ for all $R < 1$

TODAY:

(•) Proof readers: Yuyang, Ashish
(•) Finish correctness of Algo 1
(•) Algo 2 (Sudan '96)
(•) If there's time, Algo 3 (Guruswami, Sudan '98)

Apr 25 Argue correctness of Step 2

If $P(x)$ is of deg $< k$ s.t. $P(\alpha_i) = y_i$
for $t \geq 2\sqrt{nk}$ positions $i \in [n]$

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

divides

for any non-zero Q that satisfies those properties

$(\deg_X(Q) \leq \ell, \quad \mathrm{Deg}_Y(Q) \leq \frac{n}{\ell}$

$\forall i \in [n], \quad Q(\alpha_i, y_i) = 0)$

$R(X) = Q(X, P(X))$ [note: non-zero $Q(X,Y)$]

$X^i Y^j \to X^i (P(X))^j$

$\Rightarrow \forall i$ s.t. $P(\alpha_i) = y_i$

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

$\Rightarrow \forall i$ s.t. $P(\alpha_i) = y_i \quad R(\alpha_i) = 0$

$\Rightarrow t$ roots

Argue next: $\deg(R) \leq \ell + \left(\frac{n}{\ell}\right)(k-1)$

$\ell = \sqrt{n(k-1)}$

$= \sqrt{n(k-1)} + \frac{n(k-1)}{\sqrt{n(k-1)}}$

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

R has deg $\leq 2\sqrt{n(k-1)}$

$< 2\sqrt{nk}$

Ofsh R has $\geq t \geq 2\sqrt{nk}$ roots

$\Longrightarrow$ $R(X) = 0$.

degree mantra

$\Rightarrow$ Alg 1 corrects $1 - 2\sqrt{R}$ frac of errors.

$Q(X,Y) \rightsquigarrow X^i Y^j \xrightarrow[Y \leftarrow P(X)]{} X^i (P(X))^j$

$\deg \boxed{i + (k-1) j}$

$i \leq \ell$, $j \leq \frac{n}{\ell}$

$\leq \ell + (k-1)\frac{n}{\ell}$

Def: $(1, w)$-weighted degree of $X^i Y^j$ is $i + w \cdot j$

Def $(1, w)$-wt degree of a poly $Q(X,Y)$ is the max $(1,w)$-wt degree of all monomials in $Q(X,Y)$

$\boxed{(1,1) \text{ is total degree}}$

Ex: $X^5 Y + X Y^2$

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

$(1,5)$ wt deg $= \max(5+5\times 1, 1+2\times 5) = 11$

Lem 1: Let $\deg(P(X)) \le w$ & let $Q(X,Y)$ have $(1,w)$ wt deg $\le D$

$\Rightarrow \underline{Q(X,P(X))}$ has degree $\le D$

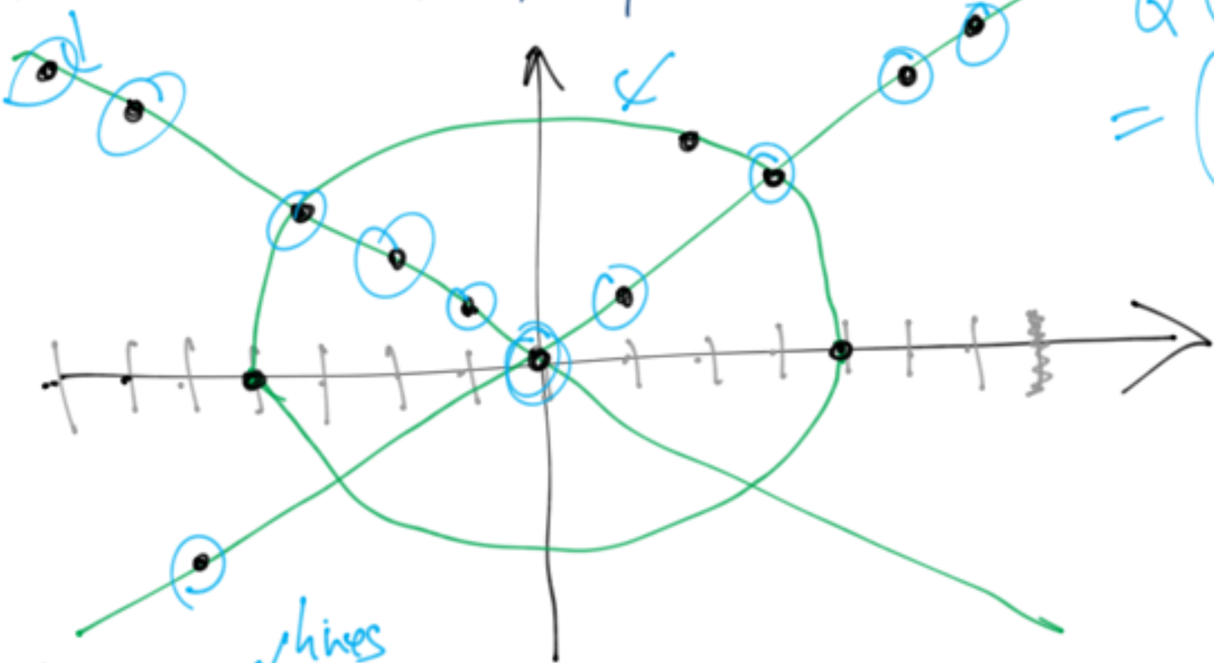
[in our case we want $(1,k-1)$ wt degree]

Algo 2 idea: Bound $(1,k-1)$ wt. degree of Q

Step 1: Compute a non-zero $Q(X,Y)$ s.t its $\underline{(1,k-1) \text{ wt. deg}} \le D$ s.t $\forall i \in [n]$

$$P(\alpha_i, y_i) = 0$$

Back to RS LD example



$Q(X,Y) = (Y-X)(Y+X)\left(\frac{X^2}{?}+\frac{Y^2}{?}\right)$

$n=14$, $k=2$, $e=9$, $t=n-e=5$

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

Step 1: Compute a non-zero $Q(X,Y)$ s.t. its $(1,k-1)$ wt. deg $\le D$ s.t. $\forall i \in [n]$

$P(\alpha_i, y_i) = 0$

Runtime: poly(n) as per our generic runtime analysis

Correctness

Step 1: # vars $> n$

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

variables

Claim: # coefficient $\ge \frac{D(D+2)}{2(k-1)}$ 2w for $(1,w)$ wt deg.

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

Step 2: $P(X)$ s.t. $\deg(P) \le k-1$ & $P(\alpha_i) = y_i$ for atleast $t \ge \sqrt{2nk} \Rightarrow Y - P(X) \mid Q(X,Y)$

Pf: $R(X) = Q(X, P(X))$

$\Longrightarrow \deg(R) \le D$

By Lemma $R(X)$ has $\ge t$ roots (same argument as in Alg 1)

By degree mantra $R(X) = 0$ if $t > D$

$t = \sqrt{2n(k)} > \sqrt{2n(k-1)} = D$