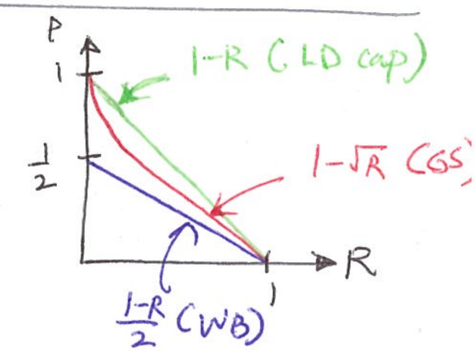
April 18, 2019

REMINDERS

(•) Video due in ~1.5 weeks (11:59pm, Tue April 30)
  ↳ Autolab is now accepting video submissions
(•) 3^{rd} proof reading schedule is up

List decoding RS codes



Generic RS decoder

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

Step 2 (Root finding): Compute all factors $Y - P(X)$ of $Q(X,Y)$ and output all such $P(X)$ w/ ① $\deg(P) < k$ & ② $P(\alpha_i) = y_i$ for $\geq t$ 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 of i

Welch-Berlekamp algo

$$Q_{WB}(X,Y) = Y \cdot E(X) - N(X)$$

$E(X)$: monic deg e; $N(X)$: deg $\leq e+k-1$

$\longleftarrow$ $Y - P(X)$ divides $Q_{WB}(X,Y)$ $\iff P(X) = \frac{N(X)}{E(X)}$

Computational considerations ~~difficulty~~

(Step 1) Feasible if # vars > # eqns. Solved e.g. by GE (see Q2 on HW 0)

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

need not have linear factors.
Eg over $\mathbb{F}_3$: $X^4 + 2X^2Y^2 + Y^4 = (X^2+Y^2)^2$

~~Algo~~	Algo 1	Algo 2	Algo 3
frac. of error	$1-2\sqrt{R}$	$1-\sqrt{2R}$	$1-\sqrt{R}$
t	$2\sqrt{nk}$ $(k-1)$	$\sqrt{2nk}$ $(k-1)$	$\sqrt{nk}$ $(k-1)$

⟹ Diff algos put diff degree constraints on $Q(X,Y)$

$1-2\sqrt{R} > \frac{1-R}{2}$ (R<0.

$1-\sqrt{2R} > \frac{1-R}{2}$ (R<0.

$1-\sqrt{R} > \frac{1-R}{2}$ (R<1

TODAY (Proofreader: Yash)

(•) Algo 1
(•) Algo 2 (Sudan '96)
(•) Algo 3 (Guruswami-Sudan '98)

Recall: $\deg_X(XY^2 + X^3Y) = 3$

$\deg_Y(\text{———}) = 2$

$\deg(P) = 1$

~~Arguments~~ Correctness argument

$\deg(R) \le 3 + 1.2 = 5$

$\deg(Q(X, P(X)) = 4$

Algo 1 :

I/p: $1 \le k \le n$, $\ell \ge 1$, $e = n - t$, n-pairs (α_i, y_i)

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

O/p: A list of $P(X)$ of deg $< k$

1. Compute non-zero $Q(X,Y)$ s.t $\deg_X(Q) \le \ell$, $\deg_Y(Q) \le \frac{n}{\ell}$ & $\forall i \in [n]$ $Q(\alpha_i, y_i) = 0$
2. $L \leftarrow \phi$ ← poly time bivariate poly factorization algo.
3. For every $Y - P(X) \mid Q(X,Y)$
   If $\deg(P) < k$ and $\Delta(\bar{y}, (P(\alpha_i))_{i=1}^{n}) \le e$
   Add P to L
4. Output L

$$Q(X,Y) = \sum_{i=0}^{\ell} \sum_{j=0}^{n/\ell} c_{ij} X^i Y^j$$

Correctness:

1. $\exists$ a non-zero $Q(X,Y)$ that satisfies Step 1

   $\#\text{coeff} = (\ell+1)(\frac{n}{\ell}+1) > n = \#\text{equations}.$

   $\Rightarrow > 1$ solutions $\Rightarrow$ atleast one - non zero $Q(X,Y)$.

2. If $P(X)$ s.t $P(\alpha_i) = y_i$ for $\ge t$ locations i

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

Define $R(X) = Q(X, P(X))$

$\forall i$ s.t $P(\alpha_i) = y_i \rightarrow R(\alpha_i) = Q(\alpha_i, P(\alpha_i)) = Q(\alpha_i, y_i) = 0$

$\Rightarrow R$ has $\ge t$ roots

Otoh $\boxed{\deg(R) \le \deg_X(Q) + (k-1)\cdot\deg_Y(Q)} = \ell + (k-1)\frac{n}{\ell}$ $\quad \ell = \sqrt{(k-1)n}$

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

Want $t > 2\sqrt{n(k-1)} \Rightarrow R(X) = 0.$

Main idea for Algo 2:

weighted degree of Q that gives a better ub on deg of $Q(X, P(X))$ $\leftarrow$ deg $\le k-1$

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

$(1,1)$-degree $=$ (total) degree

$Q(X,Y) = \max$ $(1,w)$-wt degree of its monomials.

Lemma: Let $\bar{P}(X)$ of deg $\le w$ & $Q(X,Y)$ has $(1,w)$-wt deg of D

$\Rightarrow \deg(Q(X, \bar{P}(X))) \le D$.

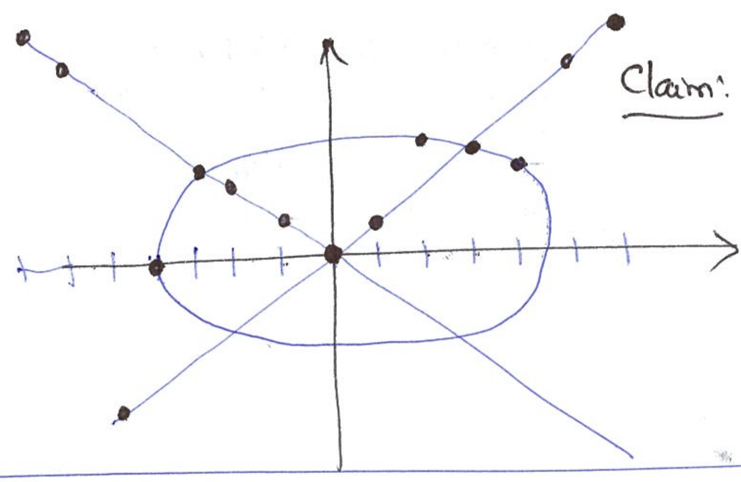
(In our case $(1, k-1)$-wt degree)

$Q(X,Y)$ has $(1,w)$-wt deg $\le D$ $\quad Q(X,Y) = \sum_{\substack{i,j \ge 0 \\ i + wj \le D}} c_{ij} X^i Y^j$

Claim: # coff $\ge \frac{D(D+2)}{\boxed{2} w}$

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

$n = 14$
$k = 2$
$e = 9$
$(t = 5)$
Unique decoding agree $\ge \frac{n+k}{2} = 7$



Algo 2:

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

Correctness:

① $\exists$ a non-zero Q $\quad$ # coeff $> n$

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

② $P(X)$ s.t $\deg(P) \le k-1$ $\quad P(\alpha_i) = y_i$ $\ge t$ location i

$R(X) = Q(X, P(X))$ $\quad$ # roots of $R \ge t$ (same as in Algo 1)

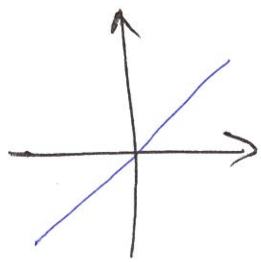
$\deg(R) \le D$ (by lemma) $\quad t > D \equiv t > \sqrt{2n(k-1)}$

Idea in Algo 3:

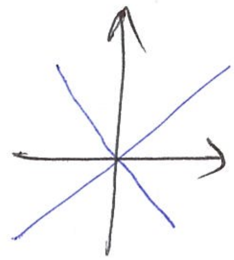
$(1, k-1)$ wt deg of $Q \le D$

Make $Q(X,Y)$ pass through each (α_i, y_i) r times

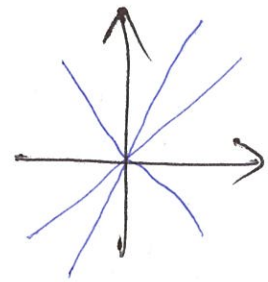
$\Rightarrow$ increas $D \uparrow 2r$ increase # roots of $R(X) \uparrow r$



$Q(X,Y) = Y - X$
passes through $(0,0)$
1



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



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

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

Def: $Q(X,Y)$ has root w/ mult r at (α, β) if $Q_{\alpha,\beta}(X,Y) = Q(X+\alpha, Y+\beta)$ passes thru $(0,0)$ r times.

Algo 3:

1. Compute non-zero $Q(X,Y)$ w/ $(1,k-1)$ wt deg D s.t. $Q(X,Y)$ has root at (α_i, y_i) with multiplicity r $\forall\, i \in [n]$

Lemma 2: (i) Non-zero Q $\exists$.

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

coeff $\ge \dfrac{D(D+2)}{2(k-1)}$

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

Want: $\dfrac{D(D+2)}{2(k-1)} > n \cdot \binom{r+1}{2} \Leftarrow$

Lemma 2: $P(\alpha_i) = y_i$, $R(\alpha_i) = 0$ "r times"

$\Rightarrow (X-\alpha_i)^r \mid Q(X, P(X))$

We're done if $rt > D = \sqrt{(k-1) n r (r-1)}$

$\Leftarrow t > \sqrt{(k-1) n (1 - \frac{1}{r})}$

Pick $r = 2(k-1)n$

$\boxed{t > \sqrt{n(k-1)}}$