Apr 28 — 1 min checkin

REMINDER

(•) Project video due in bit more than 2 weeks (11:59pm Sun, May 14)

RECAP

(•) Reformulation of WB algo

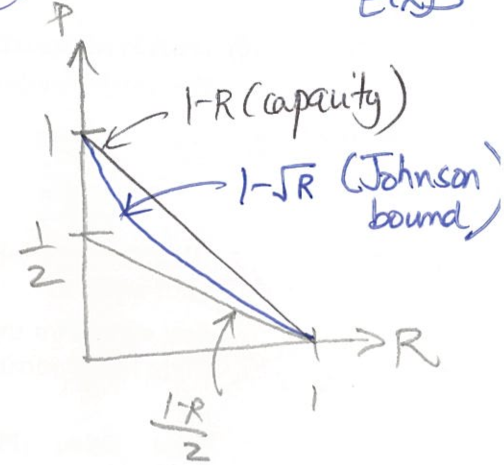
(Step 1) Compute $N(X)$ and $E(X)$ [with degree constraints] s.t. $\forall i \in [n]$, $N(\alpha_i) = y_i E(\alpha_i)$

(Step 2) If $Y - P(X)$ divides $\underbrace{Y E(X) - N(X)}$ $\{\equiv P = \frac{N(X)}{E(X)}\}$ output $P(X)$

(•) List decoding of RS codes

Input: $(\alpha_1, y_1), (\alpha_2, y_2), \ldots, (\alpha_n, y_n) \in \mathbb{F}_q^2$

Output: ALL polys $P(X)$ of deg $\le k-1$ s.t. $P(\alpha_i) = y_i$ for at least t values of $i \in [n]$



Plan for today

(•) List decoding algo for $p = 1 - 2\sqrt{R}$ frac. of errors

$\underbrace{\text{(Yet another) WB reformulation}}$

(Step 1) Compute $\underline{Q(X,Y)} = Y \, E(X) - N(X)$ s.t. $\forall i \in [n]$ $Q(\alpha_i, y_i) = 0$

$N(X)$: deg $\le k+e-1$

$E(X)$: monic + deg $= e$

$\Rightarrow Q(\alpha_i, y_i) = y_i E(\alpha_i) - N(\alpha_i) = 0$

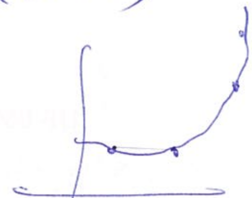
(Step 2) If $Y - P(X) \mid Q(X,Y)$ $\Rightarrow$ output $P(X)$

$\mid$: divides

$Q(X,Y)$: Q as a poly in Y with coefficients themselves being polys in X.

Generic LD algo skeleton

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



(Step 2) [Root finding] $\forall$ polys $P(X)$ s.t $\deg(P) < k$ s.t $Y - P(X) \mid Q(X,Y)$ add $P(X)$ to the output list.

Thm: $\exists$ a poly time algorithm to factorize any bivariate poly.

Ex: $Y^2 + 4XY + (4X^2 - 1)$

Factor $\hookrightarrow$ $(Y + (2X+1))(Y + (2X-1))$

$= Y^2 + (2X-1)Y + (2X+1)Y + (2X+1)(2X-1)$

$= Y^2 + 4XY + 4X^2 - 1$

factorization algo: i/p $\to$ $Q(X,Y)$ o/p $\to$ list of all irr factors

(Step 2) (Root finding step)

1. Run this algo to compute all irr factor of $Q(X,Y)$
2. Only keep "linear factor" $Y - P(X)$

$\leftarrow$ poly assuming degree of $Q(X,Y)$ is poly(n)

Degree: Recall for univariate $\to$ largest exponent of any term

$\deg(-X^3 + 5X + 100) = 3$

Def: $\mathrm{Deg}_X(Q(X,Y))$ is largest exponent of X in any term

$\mathrm{Deg}_X(X^3Y + X^1Y^4) = 3$

Def: $\mathrm{Deg}_Y(Q(X,Y))$ ——— Y ———

$\mathrm{Deg}_Y(X^3Y + XY^4) = 4$

Idea of Algo 1: Impose bounds on $\deg_X(Q)$ & $\deg_Y(Q)$

Step 1: Compute non-zero $Q(X,Y)$ s.t ① $\deg_X(Q) \le \ell$ ← TBD

② $\deg_Y(Q) \le \frac{n}{\ell}$ s.t $\forall i \in [n]$ $Q(\alpha_i, y_i) = 0$

Note $Q(X,Y)=0$ is a valid soln to these eqns BUT we exclude it.

$$Q(X,Y) = \sum_{a=0}^{\ell} \sum_{b=0}^{n/\ell} q_{a,b} X^a Y^b$$

fixed

$$Q(\alpha_i, y_i) = \sum_{a=0}^{\ell} \sum_{b=0}^{n/\ell} q_{a,b} (\alpha_i)^a (y_i)^b = 0$$

unknowns / vars

$\Rightarrow n$ linear equations in variables $q_{a,b}$ $\quad 0 \le a \le \ell$, $0 \le b \le \frac{n}{\ell}$

$\rightarrow$ Use Gaussian Elimination to compute $q_{a,b}$ from the n linear equations.

$$\#\text{variables} = \left|\{q_{ab} \mid 0 \le a \le \ell,\ 0 \le b \le \tfrac{n}{\ell}\}\right|$$

$$= (\ell+1)\left(\tfrac{n}{\ell}+1\right)$$

$$= \cancel{\ell} \cdot \frac{n}{\cancel{\ell}} + \ell + \frac{n}{\ell} + 1$$

$$= n + \frac{n}{\ell} + \ell > n$$

$\Rightarrow$ we have n linear equations in $> n$ vars (& we know $Q(X,Y)=0$ is a valid solution)

↳ $q^{\#\text{vars}-n} > 1$ solutions

$\Rightarrow \exists$ a non-zero $Q(X,Y)$ that satisfies (step 1) s.t $\deg_X(Q) \le \ell$, $\deg_Y(Q) \le \frac{n}{\ell}$ } compute such a Q in poly time

---

$\boxed{\text{Algo 1}}$ $\quad t = 2\sqrt{kn}$

i/p: $1 \le k \le n$, $\ell = \sqrt{(k-1)n}$, $e = n - t$, n pairs (α_i, y_i) $i \in [n]$

o/p: list of polys of deg $< k$

1) Compute non-zero $Q(X,Y)$ w/ $\deg_X(Q) \le \ell$, $\deg_Y(Q) \le \frac{n}{\ell}$ ← Solve using Gaussian elimination $O(n^3)$

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

2) $L \leftarrow \phi$

3) For every $Y - P(X) \mid Q(X,Y)$ ← bivariate poly factorization

If $\deg(P) \le k-1$, $\Delta(\bar{y}, (P(\alpha_i))_{i=1}^{n}) \le e$

Add $P(X)$ to L

overall: poly(n)

4) Output L

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

② If $\exists$ $P(X)$ s.t. $\deg(P) < k$, $P(\alpha_i) = y_i$ for at least t values of $i \in [n]$, then $P(X) \in L$.

① + ② $\Rightarrow$ Algo 1 correctly does L.D. ~~for~~ up to e errors

$$e = n - t = n - 2\sqrt{nk}$$

$$\equiv \frac{e}{n} = \frac{n - 2\sqrt{nk}}{n} = 1 - \frac{2\sqrt{nk}}{n} = 1 - 2\sqrt{\frac{nk}{n^2}} = 1 - 2\sqrt{\frac{k}{n}}$$

$$= 1 - 2\sqrt{R}$$

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

$$\equiv Q(X,Y) = \underbrace{(Y - P(X))\,\cdot}_{}\ Q'(X,Y)$$