Apr 22

REMINDER

(•) Video due on Wed last week of classes
↳ All submissions done by 11:59pm last day of classes

RECAP:

(•) Welch-Berlekamp algo

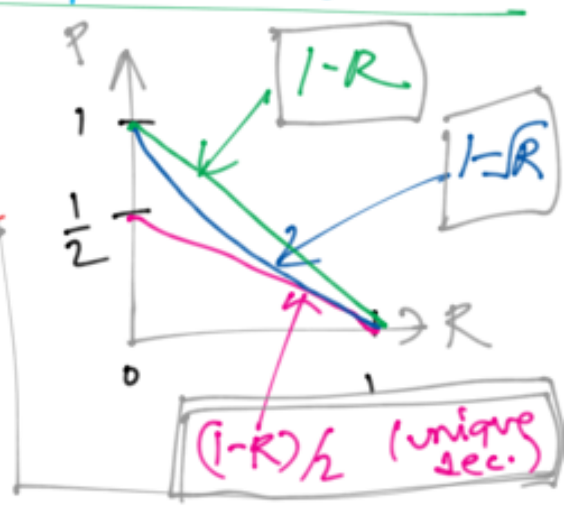
Reformulation of WB:

$\boxed{\text{Step 1:}}$ Compute $N(X)$, $E(X)$ ($\deg \le e+k-1$, $\deg = e$)
s.t. $\forall i \in [n]$ $N(\alpha_i) = y_i \cdot E(\alpha_i)$

Step 2: If $Y - P(X)$ divides $YE(X) - N(X) = Q(X,Y)$
$\Rightarrow$ output $P(X)$

$\equiv \boxed{P(X) = \frac{N(X)}{E(X)}}$

$E(X)\left(Y - \frac{N(X)}{E(X)}\right)$



TODAY:

(•) Proof readers: Rafi, Joseph
(•) Generalize WB to list decoding algos for RS codes.
(→) Algo 1 : $1 - 2\sqrt{R}$
(→) Algo 2 (Sudan '96) : $1 - \sqrt{2R}$
(→) Algo 3 (Guruswami, Sudan '98): $1 - \sqrt{R}$

WB algo reformulation

Step 1: Compute $\boxed{Q(X,Y) = Y \cdot N(X) - E(X)}$

deg $\le k+e-1$ deg $= e$

s.t. $\forall i \in [n]$, $Q(\alpha_i, y_i) = \boxed{(y_i N(\alpha_i) - E(\alpha_i))}$

$\boxed{Q(\alpha_i, y_i) = 0}$ $= 0$

$\boxed{\text{Step 2:}}$ If $Y - P(X) \mid Q(X,Y)$

divides

Q as a poly in Y with coefficients being poly in X.

$\Rightarrow$ output $P(X)$

List decoding algo skeleton

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

diff choices of properties $\Rightarrow$ Algo 1/2/3

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

Use factoring

Thm: $\exists$ a poly time algo to factorize any bivariate poly $Q(X,Y)$

$\hookrightarrow (Y+(2X+1))^2 = Y^2 + 2(2X+1)Y + (2X+1)^2$

$= Y^2 + (4X+2)Y + (4X^2+4X+1)\cdot Y^0$

$\hookrightarrow$ (factorization algo)

$(Y+(2X+1)), (Y+(2X+1))$

(Step 2) root finding

1. Factorize $Q(X,Y)$
2. Only keep "linear" factor i.e. $Y-P(X)$.

$\Rightarrow$ Step 2 can be done in poly time (assuming $\# P(X)$ is poly(n))

Def: $\mathrm{Deg}_X(Q)$ is the largest exponent of X in any monomial

Univariate poly
$P(X) = X^3 + 5X + 3$
$\deg(P) = 3$

$$\mathrm{Deg}_X(X^3Y + XY^2) = 3$$

Def: $\mathrm{Deg}_Y(Q)$ is the largest exponent of Y in any monomial

$$\mathrm{Deg}_Y(X^3Y + XY^2) = 2$$

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

for Step 1: Compute NON-ZERO $Q(X,Y)$ s.t

(1) $\deg_X(Q) \le \ell$ (2) $\deg_Y(Q) \le \frac{n}{\ell}$

s.t $\boxed{\forall i \in [n] \quad Q(\alpha_i, y_i) = 0}$ fix later.

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

variables

$$Q(\alpha_i, y_i) = \sum_{j=0}^{n/\ell} \sum_{m=0}^{\ell} (\alpha_i)^m (y_i)^j \cdot q_{mj} = 0$$
$\forall i \in [n]$

Known

variables

$\forall i \in [n]$ $\quad \displaystyle\sum_{j=0}^{n/\ell} \sum_{m=0}^{\ell} (\alpha_i)^m (y_i)^j \cdot q_{mj} = 0$

fixed / known $\qquad$ fixed / known

n

Linear equations in variables q_{mj}.

$\Rightarrow$ Use Gaussian elimination to solve for q_{mj}'s.

$\#\text{variables} = \left| \left\{ q_{mj} \,\middle|\, 0 \le m \le \ell,\ 0 \le j \le \frac{n}{\ell} \right\} \right|$

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

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

$> n$.

$q^{\#\text{vars} - \#\text{eqns}}$

#variables $>$ # equations.

Fact: A system of linear equations with # variables $>$ # eqns has > 1 solution. $q_{mj} = 0$.

(HW0 problem 2)

$\Rightarrow \exists$ one solution where not all $\Rightarrow Q(X,Y)$ non-zero

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

$deg_X(Q) \le l$, $deg_Y(Q) \le \frac{n}{l}$

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

$t = 2\sqrt{kn}$

Algorithm 1

i/p: $1 \le k \le n$, $l = \sqrt{(k-1)n}$, $e = n - t$

n pairs (α_i, y_i) $i \in [n]$

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

1) Compute non-zero $Q(X,Y)$ s.t. $deg_X(Q) \le l$

$deg_Y(Q) \le \frac{n}{l}$ & $i \in [n]$ $Q(\alpha_i, y_i) = 0$.

Gaussian Elimination

2) $L \leftarrow \phi$

poly time bivariate factorization

3) For every $Y - P(X) \mid Q(X,Y)$

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

Add $P(X)$ to L

4) Output L. $\Rightarrow$ overall is poly(n) time.

Correctness:

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

2) If $P(X)$ s.t $deg(P) < k$ & $P(\alpha_i) = y_i$ for at least $t (= 2\sqrt{nk})$ values $i \in [n]$

Correctness:

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

(2) If $P(X)$ s.t. $\deg(P) < k$ & $P(\alpha_i) = y_i$ for at least $t \left(= 2\sqrt{nk}\right)$ values $i \in [n]$

want $Y - P(X) \mid Q(X,Y)$

(1) + (2) $\Rightarrow$ Alg 1 does list decoding up to

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

$$\equiv \frac{e}{n} \le 1 - \frac{2\sqrt{nk}}{n} = 1 - 2\sqrt{\frac{k}{n}} = 1 - 2\sqrt{R}.$$