May 4 — 1 min checkin

REMINDERS

(•) Video (+peer survey) due in ~1 week (11:59pm, Sun, May 14)

RECAP

(•) **Def** $Q(X,Y)$ passes through $(0,0)$ r times if it doesn't have any monomial of total degree $\leq r-1$

(•) **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 thru $(0,0)$ r times

Algorithm 3 (Guruswami, Sudan '98)

(Step 1) Compute non-zero $Q(X,Y)$ with $(1,k-1)$ wt degree $\leq D$ (TBD) s.t. for all $i \in [n]$, $Q(X,Y)$ has root at (α_i, y_i) with mult r.

(Step 2) Compute all factors $Y-P(X)$ of $Q(X,Y)$ s.t. (i) $\deg(P) < k$ and (ii) $P(\alpha_i) = y_i$ for atleast t values $i \in [n]$

Plan for today (•) Correctness of Algo 3 (•) Towards correcting $1-R$ frac. of errors

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

$\Leftarrow$ # vars > # eqns

$$Q(X,Y) = \sum_{\substack{a,b \\ a+(k-1)b \leq D}} q_{a,b} X^a Y^b \qquad \# \text{ vars} = \# \text{ coeff} \geq \frac{D(D+2)}{2(k-1)}$$

$$\# \text{eqns} = n \cdot \binom{r+1}{2} = \frac{n \cdot r(r+1)}{2}$$

fix $i \in [n]$. $Q(X,Y)$ has r roots at (α_i, y_i)

$\equiv$ $Q(X+\alpha_i, Y+y_i)$ has no monomials of ~~weighted~~ total degree $\leq r-1$

$$q_{a,b} \cdot X^a Y^b \rightarrow q_{ab} (X+\alpha_i)^a \cdot (Y+\beta_i)^b$$

$$q_{ab} \left(\sum_{\ell=0}^{a} \binom{a}{\ell} X^{\ell} (\alpha_i)^{a-\ell} \right) \cdot \left(\sum_{\ell=0}^{b} \binom{b}{\ell} Y^{\ell} \cdot (y_i)^{b-\ell} \right)$$

$$= q_{a,b} \cdot (X^a Y^b + \dots)$$

Claim: $(1,k-1)$ wt degree of $Q(X+\alpha_i, Y+\beta_i) \le D$

$$Q_{\alpha_i,y_i}(X,Y) = \sum_{\substack{a,b \\ a+(k-1)b \le D}} c_{ab} X^a Y^b$$

$$\boxed{c_{a,b} = 0 \quad \forall \quad a+b \le r-1}$$

Since $Q_{\alpha_i,y_i}(X,Y)$ passes through $(0,0)$ r times.

Each $c_{a,b}$ is a linear function of $q_{a,b}$

$\Rightarrow$ I get as many linear equations as # pairs (a,b) s.t $a+b \le r-1$

$\Rightarrow$ Overall $n \cdot \binom{r+1}{2}$ equations.

want # vars $>$ # eqns.

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

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

Correctness of Step 2: If $P(X)$ s.t $\deg(P) \le k-1$ & $P(\alpha_i) = y_i$ for at least $t \ge \sqrt{nk}$ values of $i \in [n]$

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

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

Lemma: If $P(\alpha_i) = y_i \Rightarrow (X-\alpha_i)^r \mid R(X)$

(prev: $r=1$) $\rightarrow (X-\alpha_i) \mid R(X) \equiv R(\alpha_i) = 0$)

$\Rightarrow$ for each i s.t $P(\alpha_i) = y_i$, $R(X)$ has a root at α_i with mult r

$\Rightarrow$ # roots $\ge rt$

By the degree mantra if $\underset{\#\text{roots}}{\ge} rt > D \ge \deg(R)$

$\Leftarrow rt > \sqrt{n(k-1)r(r-1)} \Leftrightarrow t > \sqrt{\frac{n(k-1)\cancel{r}(r-1)}{r^{\cancel{2}}}} = \sqrt{n(k-1)(1-\frac{1}{r})}$

Pick $r = 2n(k-1)$ (since t is an integer)

$\Leftarrow t > \sqrt{n(k-1)} \Leftarrow t \ge \sqrt{nk} \Rightarrow$ $1-\sqrt{R}$ fraction errors

Obs 1: ~~Doesn't~~ We never used the fact that $\alpha_i \neq \alpha_j$.

① List recovery $(\alpha_1, y_1), (\alpha_2 = \alpha_1, y_2) \dots, -$

② Soft recovery

$\downarrow$ 90% $\quad\quad$ $\downarrow$ 10%

$(\alpha_1, y_1, \underline{w_1}) \quad \dots \quad (\alpha_i, y_i, w_i)$

If $p(\alpha_i) = y_i \Rightarrow \underline{w_i}$ in agreement

All codewords whose weighted agreem $\geq W$

GS algo: $Q(X,Y)$ has w_i roots at (α_i, y_i)

So far in list decoding: As of 3 week back, $\exists$ ly RS codes can correct $1-R-\varepsilon$ frac of errors.

(•) Best efficient l.d. algo for RS codes corrects from $1-\sqrt{R}$ frac. of errors

Best algorithmic result for RS codes.

(•) By LD capacity result $\exists$ $\left(1-R-\varepsilon, O\left(\frac{1}{\varepsilon}\right)\right)$ - l.d. code of rate R $\exists$ w/ $q \geq 2^{\Omega(1/\varepsilon)}$

Q: Can we ~~get~~ LD $(1-R-\varepsilon)$ fraction of errors in poly time for some code of rate R?

A: Yes (Parvaresh - Vardy '05, Guruswami R '08)

Folded RS

Folded RS Codes: RS codes $[n,k]_q$ with eval $\gamma^0 = 1, \gamma, \gamma^2, \dots, \gamma^{n-1}$ where γ generates $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ $= \{1, \gamma, \dots, \gamma^{q-2}\}$

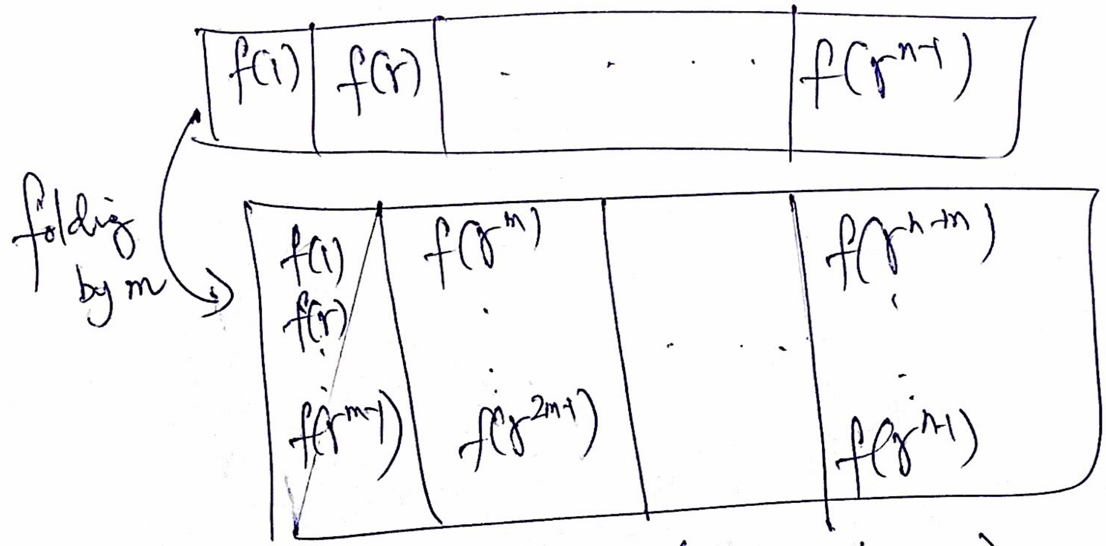
$\boxed{\text{folding} \quad m=2}$ message poly $f(X)$ (deg $< k$)

$f(1)$	$f(\gamma)$	$f(\gamma^2)$	$\dots$	$f(\gamma^{n-1})$

$\Downarrow$ $m=2$

$f(1)$ $f(\gamma)$	$f(\gamma^2)$ $f(\gamma^3)$	$\dots$	$f(\gamma^{n-2})$ $f(\gamma^{n-1})$

for general $m \geq 1$ s.t $m \mid n$



$$(q^m)^{\frac{k}{m}} = q^k$$

RS : $[n,k]_q \xrightarrow[m\text{-fold}]{} \left(\frac{n}{m}, \frac{k}{m}\right)_{q^m}$

(o) FRS wle can correct from $1-\sqrt{R}$ frac. of errors

$\Rightarrow$ unfold + use SS algorithm.