Reminders

• Wikipedia entry due by midnight, next Monday
  – Inline reference support does not work
    - Can still use refs, just follow Wikipedia style

• Am still waiting on some lecture notes
Sudan’s list decoding algo

- Given $(\alpha_i, y_i)$, $1 \leq i \leq n$
  - Interpolation Step
    - Compute non zero $Q(X,Y)$
      - $(1,k-1)$ weighted degree $D = (2kn)^{1/2}$
      - $Q(\alpha_i, y_i) = 0$ for $1 \leq i \leq n$
  - Factorization Step
    - Compute all factors $Y - P(X)$ of $Q(X,Y)$
      - $P(X)$ needs to be of deg at most $k-1$
      - $P(\alpha_i) = y_i$ for at least $t$ values of $i$
Guruswami-Sudan Improvement

- Given \((\alpha_i, y_i) \ 1 \leq i \leq n\)

- Interpolation Step
  - Compute non zero \(Q(X, Y)\)
    - \((1, k-1)\) weighted degree \(D = (2kn)^{1/2}\)
    - \(Q(\alpha_i, y_i) = 0\) for \(1 \leq i \leq n\)

- Factorization Step
  - Compute all factors \(Y - P(X)\) of \(Q(X, Y)\)
    - \(P(X)\) needs to be of deg at most \(k-1\)
    - \(P(\alpha_i) = y_i\) for at least \(t\) values of \(i\)
n=10, k=2, t=4 example

All lines must be output
n=10, k=2, t=4 example

$Q^*(x, y) = \prod_{i=1}^{5} L_i(x, y)$

$\Rightarrow$ All $L_i(x, y), 1 \leq i \leq 5$ should be factors of $Q(x, y)$

$\Rightarrow \deg(Q) \geq 5$

But $L_i(x, y)$ intersects $Q(x, y)$ in 4 positions!

$\Rightarrow$ By Sudan's idea cannot prove that $L_5(x, y)$ are factors of any $Q(x, y)$ of deg 5.
n = 10, k = 2, t = 4 example

\( Q^* = \text{product of the 5 lines} \)

Any special property of \( Q^* \)?

\( Q^* \) passes thru all pts twice.

Can't guarantee this with a degree bound

\[ \text{GS idea: Insist on } Q(x, y) \text{ passing thru } (x_i, y_i) \]

\[ + \deg(Q) \leq 5 \]

Each \( L_i \) intersects \( Q(x, y) \) 2 x 4 = 8 times

\[ > \deg(Q) \]
GS algorithm

- Given \((\alpha_i, y_i) \, 1 \leq i \leq n\)

- Interpolation Step
  - Compute non zero \(Q(X, Y)\)
  - \((1, k-1)\) weighted degree \(D = (k-1)^{1/2}\)
  - \(Q(\alpha_i, y_i) = 0\) with multiplicity \(r\) for \(1 \leq i \leq n\)

- Factorization Step
  - Compute all factors \(Y - P(X)\) of \(Q(X, Y)\)
    - \(P(X)\) needs to be of deg at most \(k-1\)
    - \(P(\alpha_i) = y_i\) for at least \(t\) values of \(i\)
Definition of Multiplicity

At $(0,0)$:

- $r = 1$:  
  $y = ax$

- $r = 2$:  
  $y = bx$

- $r = 3$:  
  $y = cx$

$(y-ax)(y-bx) \implies$ no monomial of degree $\leq 1$

$(y-ax)(y-bx)(y-cx) \implies$ no term of degree $\leq 2$
Def 1: $Q(X, Y)$ has mult. $r$ at $(0, 0)$ if it has no monomial of deg $\leq r-1$

Def 2: $Q(X, Y)$ has mult. $r$ at $(\alpha, \beta)$ if $\mathcal{Q}_{\alpha, \beta}(X, Y) \triangleq Q(\alpha + x, \beta + y)$ has no mon. of deg $\leq r-1$

Lemma 1: In step 1, we have $n \binom{r+1}{2}$ constraints.

Lemma 2: $P(x)$ of deg $< k-1$ & $P(d_i) = y_i$ for $t > \frac{D}{r}$ positions then $Y - P(X) \mid Q(X, Y)$

By Lemma 1 done if $\# \text{coeff} \geq \frac{D^2}{2(k-1)} > \frac{n \cdot r(r+1)}{2} \leq D = \sqrt{r(r+1)nk}$

Lemma 2 $\Rightarrow t > \frac{D}{r} > \sqrt{d+\frac{r}{2}nk}$ $2\sqrt{nk}$ by picking $r = 2nk$
Pf of Lemma 1: \[ \sum_{i \leq r} \binom{m}{i} \text{constraints on \ \coeffs{Q(X,Y)}} \]

\[
Q(X,Y) = \sum_{0 \leq \binom{i+j}{i} \leq D} q_{i,j} X^i Y^j
\]

\[
Q_{x_i, y_j}(X,Y) \overset{\text{def}}{=} Q(X + x_i Y + y_j)
\]

\[
q'_i,j \overset{\text{by defn.}}{=} \sum_{(ij)} q_{i,j}
\]

q'_{i,j} is linear comb of q_{i,j} s.

Q_{x_i, y_j}(X,Y) has no term X^i Y^j \iff i+j \leq r-1 \Rightarrow q'_{i,j} = 0

\[
\# \text{constraints} = \sum_{i=0}^{r-1} \sum_{j=0}^{r-1-i} 1 = \sum_{j=0}^{r-1} j = \binom{r}{2}
\]

\[
\implies \frac{r^2 - r}{2}
\]

linear constraint on q_{i,j} s.
Lemma 2: If \( P(x_i) = y_i \) for \( i = \frac{D}{r} \) is a factor \( \Rightarrow Y - P(x) \) is a factor

\[ \deg(R) \leq (1, k+1) \deg Q \leq D \]

but \# roots of \( R = \epsilon : r > \frac{D}{r} \)

Lemma 3: \( P(x_i) = y_i \Rightarrow (x - x_i)^r \) divides \( R(x) \)

\[ R(x) \overset{\text{def}}{=} Q(x, P(x)) \]

\( \alpha_i \) is a root of \( R \) with multiplicity \( r \)

Pf of Lemma 3: \( r = 1 \rightarrow \) "obvious"

\[ (*) \overset{\text{def}}{=} R_{y_i y_i}(x) \]

\[ R_{y_i y_i}(0) \iff R(x) = 0 \ or \ X \mid R_{y_i y_i}(x) \iff (x - x_i) \mid R(x) \]

\( \Rightarrow \text{show } X^r \mid R_{y_i y_i}(x) \)
\[ P_{\text{diy}_i}(x) \overset{\text{def}}{=} p(x + \alpha_i) - y_i \]

\[ p(\alpha_i) = y_i \implies P_{\alpha_i,y_i}(0) = 0 \implies P_{\text{diy}_i}(x) = x \cdot g(x) \]

**Claim:**

\[ R_{\text{diy}_i}(x) = Q(x, P_{\text{diy}_i}(x)) \]

\[ \implies R_{\alpha_i,y_i}(x) = \sum_{ij} q'_{ij} x^j \left( P_{\alpha_i,y_i}(x) \right)^j \]

\[ = \sum_{ij} q'_{ij} x^j g(x)^j \]

\[ \neq 0 \text{ if } \alpha_i \geq r \]

\[ \implies \text{every term has } x^r \text{ in it} \]
Proof of Claim:

$$R_{a;i,y_i}(x) = R(x + a_i)$$

$$= Q(x + a_i, P(x + a_i))$$

$$= Q(x + a_i, P_{a;i,y_i}(x) + y_i)$$

$$R = Q_{a;i,y_i}(x, P_{a;i,y_i}(x))$$

Theorem: RS codes can be list-decoded up to $$1 + \epsilon$$ fraction of errors in polynomial time.
Folded RS

\[ f(x) \]

folding with s:

\( (f(1), f(\beta), \ldots) \)

\[ s/h \]

\[ f(1) \]
\[ f(\beta) \]
\[ \ldots \]
\[ f(\beta^{s-1}) \]

RS: \( \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n \)

FRS(s): \( \mathbb{F}_q^k \rightarrow \mathbb{F}_q^{n/s} \)

\[ \beta \text{ is generator of } \mathbb{F}_q \backslash \mathbb{F}_q^* \]

\[ \mathbb{F}_q^* = \{1, \beta, \beta^2, \ldots, \beta^{q-2}\} \]

n = q - 1

K = \( \frac{k}{s} \)

N = \( \frac{n}{s} \)

\[ 2/h \]

\[ \Rightarrow \frac{K}{N} = \frac{k}{n} \]