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

Corrects $1-\sqrt{2R}$ frac of errors

Guruswami-Sudan Improvement

Generalization

$1-\sqrt{R}$ frac. of errors

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

D changes

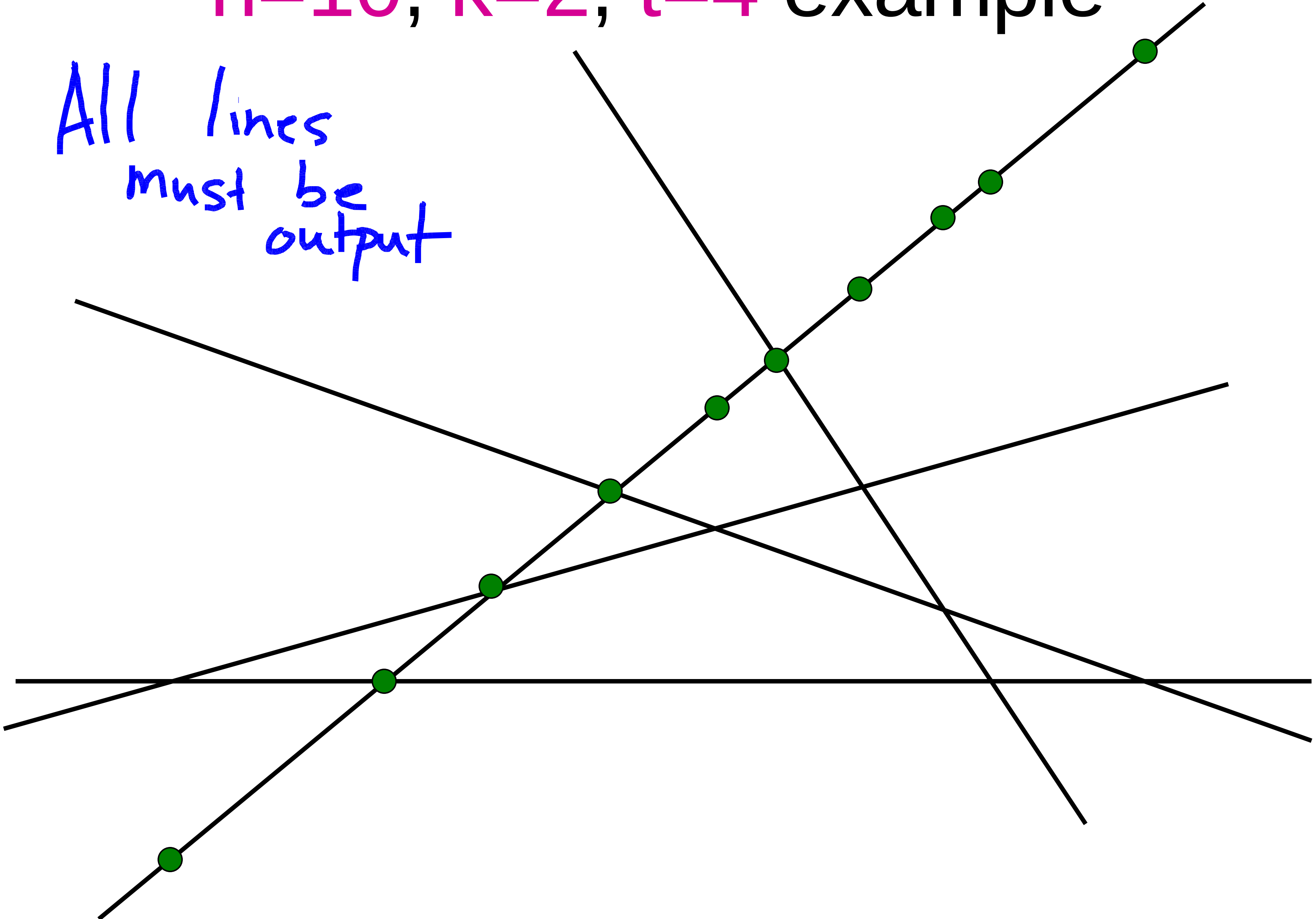
Have multiplicity $r \ge 1$ for each i

- 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

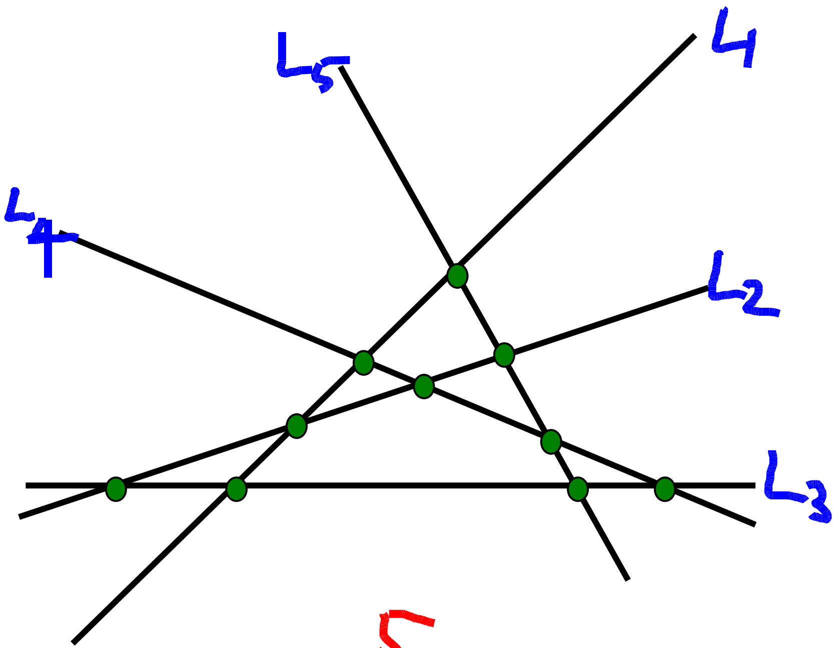
same as Sudan

n=10, k=2, t=4 example

All lines must be output



$n=10$, $k=2$, $t=4$ example



$\rightarrow$ All $L_i(X,Y)$ $1 \le i \le 5$ should be factors of $Q(X,Y)$

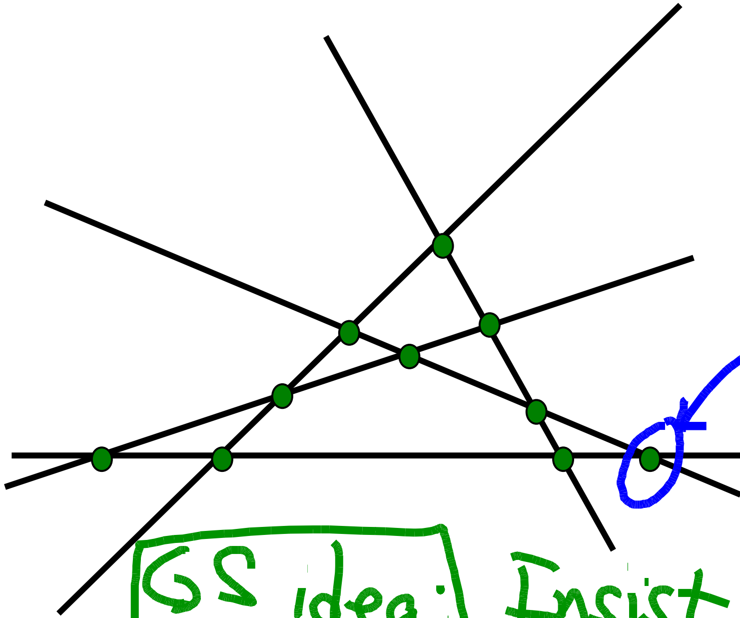
$\Rightarrow$ $\deg(Q) \geq 5$

but $L_i(X,Y)$ intersects $Q(X,Y)$ in 4 positions!

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

$\Rightarrow$ By Sudan's idea cannot prove that $L_i(X,Y)$ are factors of any $Q(X,Y)$ of deg 5.

n=10, k=2, t=4 example



Q^* = product of the 5 lines.

Any special property of Q^*?

Q^* passes thru all pts twice

Can't guarantee this with a degree bound

$\boxed{\text{GS idea:}}$ Insist on $Q(X,Y)$ passing thru (α_i, y_i) twice $\forall i$

+ $\deg(Q) \le 5$

Each L_i intersects $Q(X,Y)$ $2 \times 4 = 8$ times $> \deg(Q)$

Saving of $\sqrt{2} \Rightarrow 1-\sqrt{2R} \longrightarrow 1-\sqrt{R}$

Saving (will see)

$Q_r(X,Y) \uparrow \frac{r}{\sqrt{2}}$

GS algorithm

$r=1 \Rightarrow$ Sudan

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

\# constr. $\uparrow r$

$Q_1(X,Y)$ for $r=1$

$Q_r(X,Y) = (Q_1(X,Y))^r$

deg $\uparrow r$

- 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

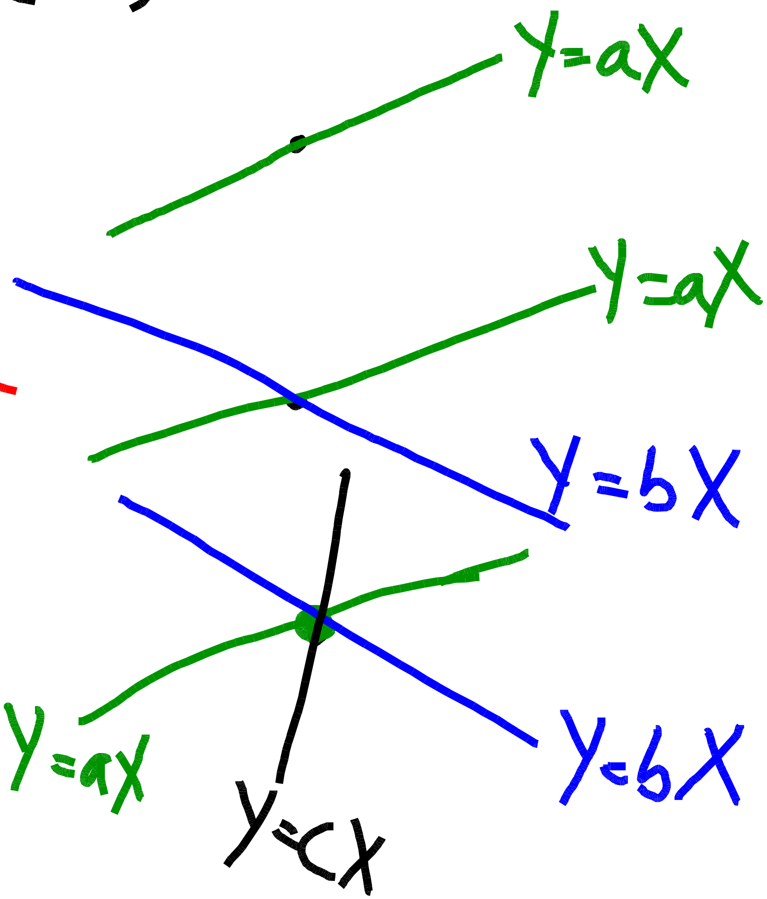
Definition of Multiplicity

at $(0,0)$

r=1

r=2

r=3



$Y-aX \rightarrow$ no term of deg 0

$(Y-aX)(Y-bX) \rightarrow$ no monomial of deg ≤ 1

$(Y-aX)(Y-bX)(Y-cX)$ no deg ≤ 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 (α,β) if $Q_{\alpha,\beta}(X,Y) \overset{\text{def}}{=} Q(\alpha+X, \beta+Y)$ 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 $< k-1$ & $P(\alpha_i)=y_i$ for $t > \frac{D}{r}$ positions then $Y-P(X) \mid Q(X,Y)$

By Lemma 1 done if $\#\text{coeffs} \geq \frac{D^2}{\cancel{2}(k-1)} > \frac{n\, r(r+1)}{\cancel{2}} \Leftarrow D = \sqrt{r(r+1)nk}$

Lemma 2 $\Rightarrow t > \frac{D}{r} > \sqrt{(1+\frac{1}{r})nk} \geq \sqrt{nk}$ by picking $r = 2nk$

Pf of Lemma 1 [$n\binom{r+1}{2}$ constraints on coeff of $Q(X,Y)$]

$\binom{r+1}{2}$ constraints for each (α_i, y_i)

$$Q(X,Y) = \sum_{0 \le i+(k-1)j \le D} q_{ij} X^i Y^j$$

$$Q_{\alpha_i,y_i}(X,Y) \stackrel{def}{=} Q(X+\alpha_i, Y+y_i)$$

$$= \sum_{i,j} q'_{i,j} X^i Y^j$$

by defn

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

$Q_{\alpha_i,y_i}(X,Y)$ has no term $X^i Y^j$ s.t. $i+j \le r-1 \Rightarrow$ $\forall (i,j)$ s.t. $i+j \le r-1$, $q'_{i,j} = 0$

linear constraint on $q_{i,j}$'s.

$$\#\text{constraints} = |\{(i,j) \mid i+j \le r-1\}|$$

$$= \sum_{j=0}^{r-1} (r-j-1+1) = \sum_{j=0}^{r-1} r-j = \sum_{j=1}^{r} j = \binom{r+1}{2} \qquad \blacksquare$$

Lemma 2: If $P(\alpha_i) = y_i$ for $> \frac{D}{r}$ i's $\Rightarrow$ $Y - P(X)$ is a factor

$\Uparrow$ $\deg(R) \le (1, k-1)\deg$ of $Q \le D$
but # roots of $R = t \cdot r > \frac{D}{r} \cdot r = D$ $\Big\} \Rightarrow R(X) \equiv 0$

Lemma 3: $P(\alpha_i) = y_i \Rightarrow (X - \alpha_i)^r$ divides $\Big\{$ α_i is a root of R with multiplicity r

$R(X) \stackrel{def}{=} Q(X, P(X))$

Pf of Lemma 3 $r = 1 \rightarrow$ "obvious"

(*) $R_{\alpha_i, y_i}(X) \stackrel{def}{=} R(X + \alpha_i)$

$\underset{=0}{R_{\alpha_i, y_i}(0)} \Leftrightarrow R(\alpha_i) = 0$ or $X \mid R_{\alpha_i, y_i}(X) \Leftrightarrow (X - \alpha_i) \mid R(X)$

$\Rightarrow$ show $X^r \mid R_{\alpha_i, y_i}(X)$

$$\boxed{X^r \mid R_{\alpha_i, y_i}(X)}$$

$P_{\alpha_i, y_i}(X) \overset{\text{def}}{=} P(X+\alpha_i) - y_i$

$P(\alpha_i) = y_i \Rightarrow P_{\alpha_i, y_i}(0) = 0 \Rightarrow P_{\alpha_i, y_i}(X) = X \underbrace{g(X)}_{\text{some poly}}$

<u>Claim:</u> $R_{\alpha_i, y_i}(X) = Q_{\alpha_i, y_i}(X, P_{\alpha_i, y_i}(X))$

$\Rightarrow R_{\alpha_i, y_i}(X) = \sum_{i,j} q'_{i,j} X^i (\underbrace{P_{\alpha_i, y_i}(X)}_{X^j g(X)^j})^j$

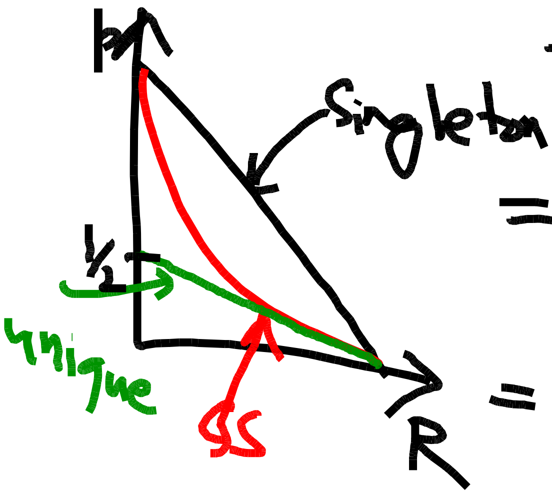
By defn of mult, $q'_{i,j} = 0$ if $i+j \le r-1$

$= \sum_{i,j} \underbrace{q'_{i,j}}_{\neq 0 \text{ if } i+j \ge r} \overbrace{X^{i+j} g(X)^j}$

$\Rightarrow$ every term has X^r in it

Pf of Claim:

$$R_{\alpha_i,y_i}(X) = R(X+\alpha_i)$$



$$= Q(X+\alpha_i, P(X+\alpha_i))$$

$$= Q(X+\alpha_i, P_{\alpha_i,y_i}(X)+y_2)$$

$$= Q_{\alpha_i,y_2}(X, P_{\alpha_i,y_i}(X))$$

def

R_{α_i,y_i}

R

P_{α_i,y_i}

Q_{α_i,y_2}

THM: RS codes can be list decoded up to $1-\sqrt{R}$ frac. of errors in poly time.

Folded RS

$f(X)$

$f(\alpha_1)$	$f(\alpha_2)$	$\cdots$	$f(\alpha_n)$

$\downarrow \; \alpha_i = \beta^{i-1}$

$f(1)$	$f(\beta)$	$f(\beta^2)$ $\cdots$	$f(\beta^{n-1})$

$\underbrace{f(1) \;\; f(\beta)}_{\text{one symbol}}$

$\downarrow$ folding parameter $s=2$

$f(1)$	$f(\beta^2)$		$f(\beta^{n-2})$
$f(\beta)$	$f(\beta^3)$	$\cdots$	$f(\beta^{n-1})$

$2/n$

folding with s:

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

s/n $\downarrow$

$f(1)$		
$f(\beta)$	$\cdots$	
$f(\beta^{s-1})$		

β is generator of $\mathbb{F}_q \setminus \{0\}$

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

$n = q-1$

$K = \frac{k}{s}$

$N = \frac{n}{s}$

$\Rightarrow \frac{K}{N} = \frac{k}{n}$

$RS: \mathbb{F}_q^k \to \mathbb{F}_q^n$, $FRS^{(s)}: \underbrace{\mathbb{F}_q^k}_{\mathbb{F}_{q^s}^{k/s}} \longrightarrow \mathbb{F}_{q^s}^{n/s}$