**REMINDERS**

- Video due in ~1.5 weeks (11:59pm, Tue April 30)
- Autolab is now accepting video submissions
- 3rd proof reading schedule is up

---

**List decoding RS codes**

**Generic RS decoder**

**Step 1 (Interpolation):** Compute non-zero

\[ Q(x,y) \text{ s.t. } Q(d_i, y_i) = 0 \quad i \in \mathbb{N} \]

**Step 2 (Root finding):** Compute all factors \( Y-P(x) \) of \( Q(x,y) \) and output all \( b \) such \( P(x) \) w/ (1) \( \deg(P) < k \)

(2) \( P(d_i) = y_i \) for \( i \geq t \) values of \( i \in \mathbb{N} \)

**Welch-Berlekamp algo**

\[ Q(x, y) = Y \cdot E(x) - N(x) \]

\[ \begin{align*}
&Q(x, y) = Y \cdot E(x) - N(x) \\
&\text{monic degree } e
\end{align*} \]

**Computational considerations**

(Step 1) Feasible if \# vars > \# eqns. Solved e.g. by GE (see Q2 on HW 0)

(Step 2) \( \exists \) poly-time algo to factorize any bi-variate poly

Assume as a black box

\[ Q(x, y) \]

\[ \text{Aalg 1: } 1 - 2\sqrt{R} \]

\[ \text{Aalg 2: } 1 - \sqrt{2R} \]

\[ \text{Aalg 3: } 1 - \sqrt{R} \]

Diff algs put diff degree constraints on \( Q(x, y) \)

<table>
<thead>
<tr>
<th>Algo 1</th>
<th>Algo 2</th>
<th>Algo 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>face in</td>
<td>( t )</td>
<td>( 2\sqrt{nk}(R^{-1}) )</td>
</tr>
<tr>
<td>( 2\sqrt{nk}(R^{-1}) )</td>
<td>( 2\sqrt{nk}(R^{-1}) )</td>
<td>( \sqrt{nk}(R^{-1}) )</td>
</tr>
</tbody>
</table>

**TODAY** (Proofreader: Yash)

- Algo 1 (Sudan '96)
- Algo 2 (Sudan '98)
- Algo 3 (Guruswami-Sudan '98)
Recall: \( \deg_x (xY^2 + x^3Y) = 3 \)  
\( \deg_y (\quad ) = 2 \)

\[ \text{Ago} 1 ! \]

\( \mathbb{C} \): \( 1 \leq k \leq n \), \( \mathbb{L} \geq 1 \), \( c = n-t \) \( n \) pairs \((x_i, y_i)\)

\( \forall \mathbb{L} \): A list of \( P(x) \) of \( \deg \geq k \)

1. Compute non-zero \( Q(x, y) \) s.t \( \deg_x (Q) \leq \mathbb{L} \), \( \deg_y (Q) \leq \frac{n}{\mathbb{L}} \)

\( \forall \mathbb{L} \) \( c \leq \mathbb{L} \) \( \exists Q(\mathbb{L}, y_i) \equiv 0 \)

2. \( \mathbb{L} \leftarrow \emptyset \)

3. For every \( Y - P(x) \mid Q(x, y) \)

   If \( \deg (P) < k \) and \( \Delta (X, (P(x_i))_{i=1}^n) \leq c \)

4. Output \( \mathbb{L} \)

Add \( P \) to \( \mathbb{L} \)

\[ Q = (X, Y) = \sum_{i=0}^{\frac{n}{\mathbb{L}}} \sum_{j=0}^{\mathbb{L}} c_{ij} X^i Y^j \]

Correctness:

1. If a non-zero \( Q(x, y) \) that satisfies Step 1:

   \( \# \text{coeff} = (\mathbb{L}+1) (\frac{n}{\mathbb{L}}+1) > n = \# \text{equations} \)

   \( \Rightarrow \) at least one non-zero \( Q(x, y) \).

2. If \( P(x) \mid Q(x, y) \)

   \( \Rightarrow Y - P(x) \mid Q(x, y) \equiv Q(x, P(x)) = 0 \)

   \( \text{Define} \ R(x) = Q(x, P(x)) \)

   \( \forall i : P(x_i) = y_i \rightarrow R(x_i) = Q(x_i, P(x_i)) = Q(x_i, y_i) = 0 \)

   \( \Rightarrow R \) has \( \geq t \) roots

\( \text{Otah} \): \( \deg (R) \leq \deg_x (Q) + (k-1) \cdot \deg_y (Q) \leq \mathbb{L} + (k-1) \cdot \frac{n}{\mathbb{L}} \)

Want \( t > 2 \sqrt{n(k-1)} \Rightarrow R(x) = 0 \), \( t = \sqrt{n(k-1)} + \frac{(k-1)n}{\sqrt{n(k-1)}} = 2 \sqrt{n(k-1)} \)
Main idea for Alg 2:

weighted degree of $Q$ that gives a better ub on deg $Q(x,p(x))$ of deg $≤ k - 1$

Definition: $(1, w)$ - weighted degree $B \ x^i y^j = i + w_j$

$(1, 1)$ - degree = (total) degree $Q(x, y) = \max (1, w)$ - wt degree of its monomials.

Lemma 2. Let $p(x)$ of deg $≤ w$ & $Q(x, y)$ has $(1, w)$ - wt deg $≤ D$.

$\Rightarrow \deg (Q(x, p(x))) ≤ D$.

(In our case $(1, k - 1)$ - wt degree $Q(x, y)$ has $(1, w)$ - wt deg $≤ D$ $Q(x, y) = \sum_{i,j≥0} c_{ij} x^i y_j$ $\sum_{i+w_j ≤ D}$ $Q = \prod (y + x) (y - x)$ $\prod (x^2 + y^2)$)

Claim: # coeff $≥ \frac{D (D + 2)}{12w}$

$\prod (y + x) (y - x)$ $\prod (x^2 + y^2)$

Alg 2:

1. Compute non-zero $Q(x, y) \ s.t (1, k - 1)$ - wt deg of $Q ≤ D$ $s.t. \ Q(x_i, y_i) = 0 \ \forall i ∈ [n]$

Correctness:

1. $\exists a$ non-zero $Q$

$\#coeff > n \iff \frac{D (D + 2)}{12(k - 1)} > n \Rightarrow D = \sqrt{12n(c - 1)}$

2. $p(x) \ s.t. \ deg (p) ≤ k - 1$ $p(x_i) = y_i \ \forall (occurs i)$ $R(x) = Q(x, p(x))$ # roots of $R$ $t ≥ \epsilon$ (same as in Alg 1)

$\deg (R) ≤ D$ (by lemma) $t > D \Rightarrow t > \sqrt{2n(k - 1)}$
Idea in Alg 3:

Make \( Q(X,Y) \) pass through each \((x_i, y_i)\) \(r\) times.

\( Q(X,Y) = Y - X \)

passes through \((0,0)\)

1

\( Q(X,Y) = (Y - X)(Y + X) \)

passes through \((0,0)\)

2

\( Q(X,Y) = (Y - X)(Y + X)(Y + 2X) \)

passes through \((0,0)\)

3 times.

Def: \( Q(X,Y) \) passes through \((0,0)\) \(r\) times if it does not have any monomial of degree \( \leq r-1 \).

\( \Rightarrow \binom{r+1}{2} \) such monomials.

Def: \( Q(X,Y) \) has root \( w/r \) or multiplicity \( r \) at \((\alpha, \beta)\) if \( Q_{\alpha \beta}(X,Y) \) passes through \((0,0)\) \(r\) times.

---

**Alg 3:**

1. Compute non-zero \( Q(X,Y) \) with \((1, k-1) \) at \( \text{deg } D \) s.t. \( Q(X,Y) \) has root at \((x_i, y_i)\) with multiplicity \( r \) at \( c \in \mathbb{N} \).

---

**Lemma 2:**

(i) Non-zero \( \& \) \( \exists \).

\# ops = \( n \cdot \binom{r+1}{2} \)

\# coeff \( \geq \frac{D(CD+2)}{2(k-1)} \)

Want: \( \frac{D(CD+2)}{2(k-1)} > n \cdot \binom{r+1}{2} \)

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

We're done if \( rt > D = \sqrt{(k-1)n \cdot r \cdot (r-1)} \)

\( t > \sqrt{nk (k-1)} \)