List Decoding of Crisscross Error Patterns

Antonia Wachter-Zeh

Computer Science Department
Technion—Israel Institute of Technology

April 27, 2014

Coding Seminar Technion
We consider data stored in arrays (matrices) over finite fields.

### Crisscross Errors

Crisscross errors corrupt rows and columns occur in several applications:

- memory arrays
- magnetic tapes
- FSK demodulation
- OFDM and FDM transmissions
Outline

1. Codes for Crisscross Errors
   - Cover Metric
   - Coding for Crisscross Errors
   - Known Results
   - Our Contribution

2. Johnson-like Upper Bound on the List Size

3. Efficient List Decoding Algorithm

4. Conclusion and Outlook
Outline

1. Codes for Crisscross Errors
   - Cover Metric
   - Coding for Crisscross Errors
   - Known Results
   - Our Contribution

2. Johnson-like Upper Bound on the List Size

3. Efficient List Decoding Algorithm

4. Conclusion and Outlook
Cover Metric

- **cover** $\text{cov}(A)$ of a matrix $A$: set of rows and columns such that all non-zero elements of the matrix are contained
- **cover weight** $\text{wt}_C(A)$: minimum cardinality of any cover

Example of $5 \times 7$ binary matrix:

$$A = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 1 & 1 & 1 & 1 & 1 & 1 \\
3 & 1 & 1 & 1 & 1 & 1 & 1 \\
4 & 1 & 1 & 1 & 1 & 1 & 1 \\
5 & 1 & 1 & 1 & 1 & 1 & 1 \\
6 & 1 & 1 & 1 & 1 & 1 & 1 \\
7 & 1 & 1 & 1 & 1 & 1 & 1 \\
8 & 1 & 1 & 1 & 1 & 1 & 1 \\
9 & 1 & 1 & 1 & 1 & 1 & 1 \\
10 & 1 & 1 & 1 & 1 & 1 & 1 \\
11 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{bmatrix}$$

$\text{rk}(A) = 2$

$$\text{wt}_C(A) = 3$$

$$\text{wt}_H(a) = 5$$ (where $a$ is representation of $A$ as vector in $\mathbb{F}_7^5$)

$\Rightarrow \text{wt}_H(a) \geq \text{wt}_C(A) \geq \text{rk}(A)$
Cover Metric

- **cover** $\text{cov}(A)$ of a matrix $A$: set of rows and columns such that all non-zero elements of the matrix are contained
- **cover weight** $\text{wt}_C(A)$: minimum cardinality of any cover

Example of $5 \times 7$ binary matrix:

$$A = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 \\
1 & & & & \\
2 & & 1 & 1 & \\
3 & & 1 & 1 & \\
4 & & & & 
\end{bmatrix}$$

$\text{rk}(A) = 2$

$\text{wt}_H(a) = 5$ (where $a$ is representation of $A$ as vector in $F_7^5$)

$\implies \text{wt}_H(a) \geq \text{wt}_C(A) \geq \text{rk}(A)$
**Cover Metric**

- **cover** $\text{cov}(A)$ of a matrix $A$: set of rows and columns such that all non-zero elements of the matrix are contained
- **cover weight** $\text{wt}_C(A)$: minimum cardinality of any cover

**Example of $5 \times 7$ binary matrix:**

$$A = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 1 & 1 & 1 & 1 & 1 & 1 \\
3 & 1 & 1 & 1 & 1 & 1 & 1 \\
4 & 1 & 1 & 1 & 1 & 1 & 1 \\
5 & 1 & 1 & 1 & 1 & 1 & 1 \\
6 & 1 & 1 & 1 & 1 & 1 & 1 \\
7 & 1 & 1 & 1 & 1 & 1 & 1 \\
8 & 1 & 1 & 1 & 1 & 1 & 1 \\
9 & 1 & 1 & 1 & 1 & 1 & 1 \\
10 & 1 & 1 & 1 & 1 & 1 & 1 \\
11 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{bmatrix}$$

Minimum covers:

$\{0, 8, 10\}$

$\text{rk}(A) = 2$

$\text{wt}_H(a) = 5$ ($a$ is representation of $A$ as vector in $\mathbb{F}_7^5$)

$\Rightarrow \text{wt}_H(a) \geq \text{wt}_C(A) \geq \text{rk}(A)$
**Cover Metric**

- **cover** $\text{cov}(A)$ of a matrix $A$: set of rows and columns such that all non-zero elements of the matrix are contained
- **cover weight** $\text{wt}_C(A)$: minimum cardinality of any cover

**Example of $5 \times 7$ binary matrix:**

$$A = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 \\
2 & 1 & 1 & 1 & 1 & 0 & 0 \\
3 & 1 & 1 & 1 & 1 & 0 & 0 \\
4 & 1 & 1 & 1 & 1 & 0 & 0 \\
\end{bmatrix}$$

Minimum covers:
$$\{0, 8, 10\} \text{ and } \{0, 2, 3\}$$
Cover Metric

- **cover** $\text{cov}(A)$ of a matrix $A$: set of rows and columns such that all non-zero elements of the matrix are contained
- **cover weight** $\text{wt}_C(A)$: minimum cardinality of any cover

Example of $5 \times 7$ binary matrix:

$$
A = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 \\
1 & & & & \\
2 & & 1 & 1 & \\
3 & & 1 & 1 & \\
4 & & & & \\
\end{bmatrix}
$$

- $\text{wt}_C(A) = 3$
- $\text{rk}(A) = 2$
- $\text{wt}_H(a) = 5$ ($a$ is representation of $A$ as vector in $F_{q^5}$)

$\implies \text{wt}_H(a) \geq \text{wt}_C(A) \geq \text{rk}(A)$
Coding for Crisscross Errors

- [Gabidulin, 1985], [Roth, 1991]: use rank-metric codes for crisscross error correction
  \[ d_R(A, B) = \text{rk}(A - B) \]
- [W., 2013]: list decoding of rank-metric codes difficult
- [Roth, 1991]: construction of codes in cover metric based on codes in Hamming metric

Question: Can we do list decoding of crisscross errors in the cover metric?
Coding for Crisscross Errors

- [Gabidulin, 1985], [Roth, 1991]: use rank-metric codes for crisscross error correction
  \[ d_R(A, B) = \text{rk}(A - B) \]

- [W., 2013]: list decoding of rank-metric codes difficult

- [Roth, 1991]: construction of codes in cover metric based on codes in Hamming metric

**Question:** Can we do list decoding of crisscross errors in the cover metric?
Codes in Cover Metric

$$(m \times n, M, d)_{q}^{C} \text{ code } C:$$

- set of matrices in $\mathbb{F}_{q}^{m \times n}$
- cardinality $M$
- minimum cover distance $d$

$$d = \min_{A, B \in C, A \neq B} d_{C}(A, B) \overset{\text{def}}{=} \min_{A, B \in C, A \neq B} \text{wt}_{C}(A - B).$$

- $[m \times n, k, d]_{q}^{C} \text{ code: } \mathbb{F}_{q}\text{-linear code in cover metric (a linear subspace of } \mathbb{F}_{q}^{m \times n} \text{ of dimension } k)$
- Singleton-like upper bound: $k \leq m(n - d + 1)$, when $m \geq n$

[Gabidulin, 1985], [Roth, 1991]
Codes in Cover Metric

$(m \times n, M, d)_q^C$ code $\mathbb{C}$:

- set of matrices in $\mathbb{F}_q^{m \times n}$
- cardinality $M$
- minimum cover distance $d$

$$d = \min_{A,B \in \mathbb{C}, \ A \neq B} d_C(A, B) \overset{\text{def}}{=} \min_{A,B \in \mathbb{C}, \ A \neq B} \text{wt}_C(A - B).$$

- $[m \times n, k, d]_q^C$ code: $\mathbb{F}_q$-linear code in cover metric (a linear subspace of $\mathbb{F}_q^{m \times n}$ of dimension $k$)

Singleton-like upper bound: $k \leq m(n - d + 1)$, when $m \geq n$ [Gabidulin, 1985], [Roth, 1991]
(Further) Known Results

<table>
<thead>
<tr>
<th>Reference</th>
<th>Result Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Gabidulin, Korzhik, 1972]</td>
<td>Introduced cover metric and codes of distance 2 and $n$</td>
</tr>
<tr>
<td>[Sidorenko, 1976]</td>
<td>Codes with cover distance 2, 3, 4 and $n$</td>
</tr>
<tr>
<td>[Roth, 1991]</td>
<td>(Optimal) construction based on codes in Hamming metric &amp; unique decoding</td>
</tr>
<tr>
<td>[Roth, 1997]</td>
<td>Probabilistic decoding for a class of codes with smaller redundancy</td>
</tr>
<tr>
<td>[Lund, Gabidulin, Honary, 2000]</td>
<td>Optimal codes with cover distance 3 and $n - 1$</td>
</tr>
<tr>
<td>[Blaum, Bruck, 2000]</td>
<td>One-error-correcting codes and their (low-complexity) decoding</td>
</tr>
<tr>
<td>[Sidorenko, Bossert, Gabidulin, 2010]</td>
<td>GMD decoding of codes in cover metric</td>
</tr>
</tbody>
</table>
Let $m \geq n$ and define a code $C(C, m)$ over $\mathbb{F}_q$ by the following set of $m \times n$ matrices:

\[
C \overset{\text{def}}{=} \left\{ \begin{pmatrix}
    c_0^{(0)} & c_1^{(m-1)} & \cdots & c_{n-1}^{(n)} \\
    c_0^{(1)} & c_1^{(0)} & \cdots & \vdots \\
    \vdots & c_1^{(1)} & \cdots & c_{n-1}^{(m-1)} \\
    c_0^{(n-1)} & \cdots & \cdots & c_{n-1}^{(0)} \\
    c_0^{(n)} & c_1^{(n-1)} & \cdots & c_{n-1}^{(1)} \\
    \vdots & \vdots & \cdots & \vdots \\
    c_0^{(m-1)} & \cdots & c_{n-2}^{(n)} & c_{n-1}^{(n-1)} \\
\end{pmatrix}
: c^{(i)} \in C, \forall i \in \langle m \rangle \right\},
\]

where $C$ is an $(n, M_H, d)_q^H$ code.
Properties of this Construction and Unique Decoding

- error of cover weight $t$ affects $\leq t$ positions of each diagonal
- $(n, M_H, d)^H_q$ code $C$ with Hamming distance $d \geq 2t + 1$ can decode uniquely on each diagonal

Properties of $C(C, m)$

- $C(C, m)$ is an $(m \times n, (M_H)^m, d)^C_q$ code
- if $C$ is a linear MDS code, then $C(C, m)$ is an optimal $[m \times n, m(n - d + 1), d]^C_q$ code
Properties of this Construction and Unique Decoding

- error of cover weight $t$ affects $\leq t$ positions of each diagonal
- $(n, M_H, d)_q^H$ code $C$ with Hamming distance $d \geq 2t + 1$ can decode uniquely on each diagonal

Properties of $C(C, m)$
- $C(C, m)$ is an $(m \times n, (M_H)^m, d)_q^C$ code
- if $C$ is a linear MDS code, then $C(C, m)$ is an optimal $[m \times n, m(n - d + 1), d]_q^C$ code
Properties of this Construction and Unique Decoding

- Error of cover weight $t$ affects $\leq t$ positions of each diagonal
- $(n, M_H, d)_q^H$ code $C$ with Hamming distance $d \geq 2t + 1$ can decode uniquely on each diagonal

Properties of $C(C, m)$

- $C(C, m)$ is an $(m \times n, (M_H)^m, d)_q^C$ code
- if $C$ is a linear MDS code, then $C(C, m)$ is an optimal $[m \times n, m(n - d + 1), d]_q^C$ code
Properties of this Construction and Unique Decoding

- error of cover weight $t$ affects $\leq t$ positions of each diagonal
- $(n, M, d)_q^H$ code $C$ with Hamming distance $d \geq 2t + 1$ can decode uniquely on each diagonal

Properties of $\mathbb{C}(C, m)$

- $\mathbb{C}(C, m)$ is an $(m \times n, (M_H)^m, d)_q^C$ code
- if $C$ is a linear MDS code, then $\mathbb{C}(C, m)$ is an optimal $[m \times n, m(n - d + 1), d]_q^C$ code
Our Contribution: List Decoding of Crisscross Errors

Motivation: Efficient list decoding of crisscross errors in the rank metric seems to be hard!

Here: List Decoding in the Cover Metric

- Johnson-like upper bound on the list size (for any code in cover metric)
- Decoding algorithm for known code construction
- Decoder is based on the decoders of the constituent code

⇒ list decoding up to our bound
Outline

1. Codes for Crisscross Errors
   - Cover Metric
   - Coding for Crisscross Errors
   - Known Results
   - Our Contribution

2. Johnson-like Upper Bound on the List Size

3. Efficient List Decoding Algorithm

4. Conclusion and Outlook
Motivation: worst-case list size directly determines complexity of decoding algorithm.

Is **polynomial-time** list decoding in the cover metric possible?

**Problem (Maximum List Size)**

\[(m \times n, M, d)_{q}^{C} \text{ code } C\]

*decoding radius* \(\tau < d\)

Find (polynomial) upper bound on

\[\ell \overset{\text{def}}{=} \max_{R \in \mathbb{F}_{q}^{m \times n}} \left\{|C \cap B_{C}^{(\tau)}(R)|\right\}.\]
Let $q \geq 2$ and let an integer $\tau < d \leq n, m$ be given. Denote

$$\eta \overset{\text{def}}{=} \frac{(n + m)^2}{m \frac{q^n}{q^n - 1} + n \frac{q^m}{q^m - 1}}.$$ 

Then, for any $(m \times n, M, d)_q^C$ code $C$ and any $\tau$ such that

$$\tau < \tau_C(q; \eta, d) \overset{\text{def}}{=} \eta - \sqrt{\eta(\eta - d)},$$

the list size $\ell$ is bounded from above by

$$\ell = \max_{R \in \mathbb{F}_q^{m \times n}} \left\{ |C \cap B_C^{(\tau)}(R)| \right\} \leq \ell_C(q; \eta, d, \tau) \overset{\text{def}}{=} \frac{d \eta}{\tau^2 - (2\tau - d)\eta},$$

where $B_C^{(\tau)}(R)$ denotes a ball around $R$ of cover radius $\tau$. 
Corollary (Alphabet-free Johnson-like Bound)

For any \((m \times n, M, d)_q^C\) code \(C\) and any integer \(\tau\) such that

\[
\tau < \tau_C \overset{\text{def}}{=} n + m - \sqrt{(n + m)(n + m - d)},
\]

the list size \(\ell\) is bounded from above by

\[
\ell \leq \ell_C \overset{\text{def}}{=} \frac{(n + m)d}{\tau^2 - (2\tau - d)(n + m)}.
\]

Differences to Hamming & rank metric:

- compared to Hamming metric: replace \(n\) by \(n + m\) and \(q\) by a weighting of \(q^m\) and \(q^n\)
- in rank metric, there cannot exist a polynomial upper bound depending only on \(m, n, d\)
Figure: Normalized Johnson-like radius $\tau_C / n$, as a function of the normalized minimum cover distance $\delta = d/n$. 

Johnson-like Bound
1. Codes for Crisscross Errors
   - Cover Metric
   - Coding for Crisscross Errors
   - Known Results
   - Our Contribution

2. Johnson-like Upper Bound on the List Size

3. Efficient List Decoding Algorithm

4. Conclusion and Outlook
**Brute-Force Exponential-Time List Decoding**

**Given:**

\[ R = \text{vecdiag}(r^{(0)}, \ldots, r^{(m-1)}) \]

\[
\begin{pmatrix}
    r_0^{(0)} & r_1^{(m-1)} & \ldots & r_{n-1}^{(n)} \\
    r_0^{(1)} & r_1^{(0)} & \ddots & \vdots \\
    \vdots & r_1^{(1)} & \ddots & r_{n-1}^{(m-1)} \\
    r_0^{(n-1)} & \ddots & \ddots & r_0^{(0)} \\
    r_0^{(n)} & r_1^{(n-1)} & \ddots & r_1^{(1)} \\
    \vdots & \ddots & \ddots & \vdots \\
    r_0^{(m-1)} & \ldots & r_{n-2}^{(n)} & r_{n-1}^{(n-1)}
\end{pmatrix}
\]

**Task**

Given \( R \) and the decoding radius \( \tau \), find all \( \Gamma_i \in \mathbb{C} \), \( i \in 0, \ldots, \ell_C - 1 \), such that \( \text{wt}_C(R - \Gamma_i) \leq \tau \).

(if possible, efficiently)
Brute-Force Exponential-Time List Decoding

**Given:**

\[ R = \text{vecdiag}(r^{(0)}, \ldots, r^{(m-1)}) \]

\[ \text{def} = \begin{pmatrix}
  r^{(0)}_0 & r^{(m-1)}_1 & \cdots & r^{(n)}_{n-1} \\
  r^{(1)}_0 & r^{(0)}_1 & \cdots & \vdots \\
  \vdots & r^{(1)}_1 & \cdots & r^{(m-1)}_{n-1} \\
  r^{(n-1)}_0 & \cdots & r^{(0)}_{n-1} \\
  r^{(n)}_0 & r^{(n-1)}_1 & \cdots & r^{(1)}_{n-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  r^{(m-1)}_0 & \cdots & r^{(n-2)}_{n-1} & r^{(n-1)}_{n-1}
\end{pmatrix} \]

**Task**

Given \( R \) and the decoding radius \( \tau \), find all \( \Gamma_i \in \mathbb{C}, i \in 0, \ldots, \ell_C - 1 \), such that \( \text{wt}_C(R - \Gamma_i) \leq \tau \).

(if possible, efficiently)

\[ r^{(i)} = c^{(i)} + e^{(i)} \]

- \( c^{(i)} \in \mathbb{C} \) is \( (\tau_H, \ell_H)_H \)-list decodable
- If \( \text{wt}_C(E) = t \), then \( \text{wt}_H(e^{(i)}) \leq t \)
Brute-Force Exponential-Time List Decoding

Given:

\[ R = \text{vecdiag}(r^{(0)}, \ldots, r^{(m-1)}) \]

\[
\begin{pmatrix}
  r^{(0)}_0 & r^{(m-1)}_1 & \cdots & r^{(n)}_{n-1} \\
  r^{(1)}_0 & r^{(0)}_1 & \cdots & \vdots \\
  \vdots & r^{(1)}_1 & \cdots & r^{(m-1)}_{n-1} \\
  r^{(n-1)}_0 & \cdots & r^{(0)}_{n-1} \\
  r^{(n)}_0 & r^{(n-1)}_1 & \cdots & \vdots \\
  \vdots & \vdots & \cdots & \vdots \\
  r^{(m-1)}_0 & \cdots & r^{(n)}_{n-2} & r^{(n-1)}_{n-1}
\end{pmatrix}
\]

Brute-force list decoding:

1. Choose \( \tau \leq \tau_H \).
2. List decode each diagonal of \( R \) in \( C \) in Hamming metric up to \( \tau \leq \ell_H \) codewords for each diagonal.
3. Examine all \( \leq (\ell_H)^m \) matrices \( C \) and keep only those with \( \text{wt}_C(R - C) \leq \tau \).

\[ \implies \text{Works, but has exponential time complexity.} \]
Lemma (Bound for Two Diagonals)

- Given $r^{(0)}, r^{(1)} \in \mathbb{F}_q^n$, let $R_2 = \text{vecdiag}(r^{(0)}, r^{(1)}) \in \mathbb{F}_q^{m \times n}$,
- let $C$ be a $(n, M_H, d)_q^H$ code,
- let $C_2 = \left\{ \text{vecdiag}(c^{(0)}, c^{(1)}) : c^{(0)}, c^{(1)} \in C \right\} \subseteq \mathbb{F}_q^{m \times n}$,
- let $\eta_2 = (n + m)(q^2 - 1)/q^2$ and let $\ell_C(q; \eta_2, d, \tau)$ be defined as in our bound with $\eta_2$.

Then, for any $\tau < \tau_C(q; \eta_2, d)$:

$$|C_2 \cap B_C^{(\tau)}(R_2)| \leq \ell_C(q; \eta_2, d, \tau),$$

where $B_C^{(\tau)}(R_2)$ denotes a ball of cover radius $\tau$ around $R_2$.

Note: $\tau_C(q; \eta_2, d) \geq \tau_C(q; \eta_0, d)$, where $\eta_0 = n + m$. 
Polynomial-Time List Decoding Idea

Given:
\[ R = \text{vecdiag}(r^{(0)}, \ldots, r^{(m-1)}) \]

\[
\begin{pmatrix}
  r_0^{(0)} & r_1^{(m-1)} & \cdots & r_n^{(n)} \\
  r_0^{(1)} & r_1^{(0)} & \ddots & \vdots \\
  \vdots & r_1^{(1)} & \ddots & r_{n-1}^{(m-1)} \\
  r_0^{(n-1)} & \vdots & \ddots & r_{n-1}^{(0)} \\
  r_0^{(n)} & r_1^{(n-1)} & \cdots & r_{n-1}^{(1)} \\
  \vdots & \ddots & \ddots & \vdots \\
  r_0^{(m-1)} & \cdots & r_{n-2}^{(n)} & r_{n-1}^{(n-1)}
\end{pmatrix}
\]

Task

Given \( R \) and the decoding radius \( \tau \), find all \( \Gamma_i \in \mathbb{C}, \ i \in 0, \ldots, \ell_C - 1 \), efficiently such that \( \text{wt}_C(R - \Gamma_i) \leq \tau \).

\[ r^{(i)} = c^{(i)} + e^{(i)} \]

- \( c^{(i)} \in \mathcal{C} \) is \((\tau_{H}, \ell_{H})^{H}\)-list decodable
- If \( \text{wt}_C(E) = t \), then \( \text{wt}_H(e^{(i)}) \leq t \)
Polynomial-Time List Decoding Idea

Given:
\[
R = \text{vecdiag}(r^{(0)}, \ldots, r^{(m-1)})
\]

**Efficient list decoding:**

1. Choose \( \tau \leq \min\{\tau_H, \lceil \tau_C \rceil - 1\} \)
2. List decode each diagonal of \( R \) \( \leq \ell_H \) codewords for each diagonal
3. Examine all \( \leq (\ell_H)^2 \) matrices \( C_2 \) with two (fixed) non-zero diagonals; keep only those with \( \text{wt}_C(R - C_2) \leq \tau \) \( \leq \ell_C \) matrices
4. add another diagonal and examine all \( \leq \ell_H \cdot \ell_C \) matrices \( \leq \ell_C \) matrices
5. ...

\[= \Rightarrow \text{has polynomial time complexity!} \]
Decoding Algorithm

Input: $R = \text{vecdiag}(r^{(0)}, r^{(1)}, \ldots, r^{(m-1)}) \in \mathbb{F}_q^{m \times n}$

parameters of constituent code $C$: $q$, $n$, $d$, $\tau_H$

integer $\tau$ with $\tau < \min\{\tau_H, \lceil \tau_C \rceil - 1\}$

Initialize: $\mathcal{L}^C \leftarrow \emptyset$, $\mathcal{L}^C_i \leftarrow \emptyset$, $\forall i \in \langle m \rangle$

for $i = 0$ to $m - 1$ do

$\mathcal{L}_i^H = \{e_0^{(i)}, e_1^{(i)}, \ldots, e_{\ell_i}^{(i)}\} \leftarrow \text{ListDecodingConstituent}(C; r^{(i)}; \tau)$

if $\mathcal{L}_i^H = \emptyset$ then

return $\mathcal{L}^C = \emptyset$

foreach $e^{(0)} \in \mathcal{L}_0^H$ do

$\mathcal{L}_0^C \leftarrow \mathcal{L}_0^C \cup \{\text{vecdiag}(e^{(0)})\}$

for $i = 1$ to $m - 1$ do

foreach $\text{vecdiag}(e^{(0)}, \ldots, e^{(i-1)}) \in \mathcal{L}_i^C$ do

foreach $e^{(i)} \in \mathcal{L}_i^H$ do

$E \leftarrow \text{vecdiag}(e^{(0)}, \ldots, e^{(i-1)}, e^{(i)})$

if $\text{wt}_C(E) \leq \tau$ then

$\mathcal{L}_i^C \leftarrow \mathcal{L}_i^C \cup \{E\}$

if $\mathcal{L}_i^C = \emptyset$ then

return $\mathcal{L}^C = \emptyset$

end if

end if

end if

end foreach

$\mathcal{L}^C \leftarrow \mathcal{L}_m^C$

Output: List of error matrices: $\mathcal{L}^C$

← list decoding radius $\tau$

← list decoding of constituent code

← sort out matrices

← output list
List decoding: Summary

Theorem (List Decoding)

Let the code $C(C, m)$ be as before, suppose $C$ is $(\tau_H, \ell_H)^H$-list decodable with complexity $D_H(C)$, let $R \in \mathbb{F}^m_{q \times n}$ be given.

Then, for any integer $\tau \leq \min\{\tau_H, \lceil \tau_C \rceil - 1\}$, our algorithm returns all $E \in \mathbb{F}^m_{q \times n}$ such that

$$\text{wt}_C(E) \leq \tau \text{ and } (R - E) \in C.$$  

The complexity of this decoder is

$$O(m \cdot D_H(C) + m \cdot \ell_H \cdot \ell_C \cdot W_C(m, n)),$$

and the list size is at most $\ell_C$.

Cover weight calculation $W_C(m, n) = O((n + m)n^2)$
Outline

1. Codes for Crisscross Errors
   - Cover Metric
   - Coding for Crisscross Errors
   - Known Results
   - Our Contribution

2. Johnson-like Upper Bound on the List Size

3. Efficient List Decoding Algorithm

4. Conclusion and Outlook
Conclusion and Outlook

Contributions

- Johnson-like upper bound in cover metric
  - shows that list decoding is possible in cover metric
  - holds for any $m \times n$ code with cover distance $d$
- polynomial-time list decoding of a known code construction
  - decodes up to our bound

Open Questions

- How to decrease the complexity of our decoder?
- How to list decode errors in cover metric with MRD codes?
- Other list-decodable codes with small field size?
- New applications?
Conclusion and Outlook

Contributions

- Johnson-like upper bound in cover metric
  \[ \Rightarrow \text{shows that list decoding is possible in cover metric} \]
  \[ \Rightarrow \text{holds for any } m \times n \text{ code with cover distance } d \]
- Polynomial-time list decoding of a known code construction
  \[ \Rightarrow \text{decodes up to our bound} \]

Open Questions

- How to decrease the complexity of our decoder?
- How to list decode errors in cover metric with MRD codes?
- Other list-decodable codes with small field size?
- New applications?
Thank you...

...for your attention!