List Decoding of Crisscross Error Patterns

Antonia Wachter-Zeh

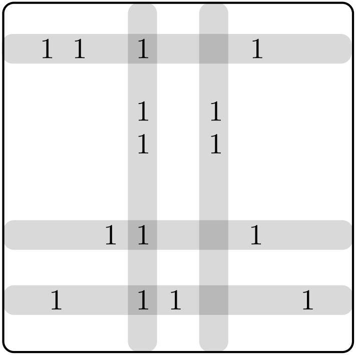
Computer Science Department
Technion—Israel Institute of Technology

April 27, 2014

Coding Seminar Technion

Crisscross Errors

We consider data stored in *arrays* (matrices) over finite fields.



Crisscross errors

- corrupt rows and columns
- occur in several applications:
  - memory arrays
  - magnetic tapes
  - FSK demodulation
  - OFDM and FDM transmissions

Outline

Outline

Cover Metric

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

Example of 5×7 binary matrix:

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

Cover Metric

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

Example of 5×7 binary matrix:

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

Cover Metric

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

Example of 5×7 binary matrix:

$$A = \begin{array}{c|ccccccc|} & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \hline 0 & 1 & 1 & & 1 & & & 1 \\ 1 & & & & & & & \\ 2 & & & & 1 & & 1 & \\ 3 & & & & 1 & & 1 & \\ 4 & & & & & & & \\ \hline \end{array}$$

minimum covers:
$\{0, 8, 10\}$

Cover Metric

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

Example of 5×7 binary matrix:

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

minimum covers:
$\{0, 8, 10\}$ and $\{0, 2, 3\}$

Cover Metric

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

Example of 5×7 binary matrix:

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

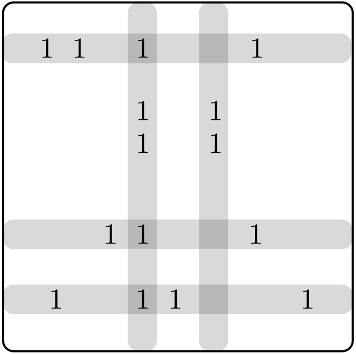
minimum covers:
$\{0, 8, 10\}$ and $\{0, 2, 3\}$

- $\mathrm{wt}_{\mathsf{C}}(A) = 3$
- $\mathrm{rk}(A) = 2$
- $\mathrm{wt}_{\mathsf{H}}(a) = 5$ (a is representation of A as vector in $\mathbb{F}_{q^5}^7$)

$\implies \mathrm{wt}_{\mathsf{H}}(a) \geq \mathrm{wt}_{\mathsf{C}}(A) \geq \mathrm{rk}(A)$

Coding for Crisscross Errors

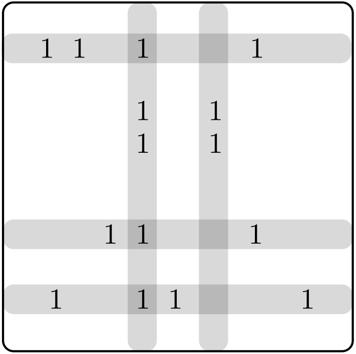
- [Gabidulin, 1985], [Roth, 1991]: use rank-metric codes for crisscross error correction $d_{\mathsf{R}}(A, B) = \mathrm{rk}(A - B)$
- [W., 2013]: list decoding of rank-metric codes difficult
- [Roth, 1991]: construction of codes in cover metric based on codes in Hamming metric



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 $d_{\mathsf{R}}(A, B) = \mathrm{rk}(A - B)$
- [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

Code in Cover Metric

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

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

$$d = \min_{\substack{A,B \in \mathbb{C}, \\ A \neq B}} d_{\mathsf{C}}(A, B) \stackrel{\text{def}}{=} \min_{\substack{A,B \in \mathbb{C}, \\ A \neq B}} \mathrm{wt}_{\mathsf{C}}(A - B) \,.$$

- $[m \times n, k, d]_q^{\mathsf{C}}$ 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]

Codes in Cover Metric

Code in Cover Metric

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

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

$$d = \min_{\substack{A,B \in \mathbb{C}, \\ A \neq B}} d_{\mathsf{C}}(A, B) \stackrel{\text{def}}{=} \min_{\substack{A,B \in \mathbb{C}, \\ A \neq B}} \mathrm{wt}_{\mathsf{C}}(A - B) \, .$$

- $[m \times n, k, d]_q^{\mathsf{C}}$ 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

[Gabidulin, Korzhik, 1972]	introduced cover metric and codes of distance 2 and n
[Sidorenko, 1976]	codes with cover distance 2, 3, 4 and n
[Roth, 1991]	(optimal) construction based on codes in Hamming metric & unique decoding
[Roth, 1997]	probabilistic decoding for a class of codes with smaller redundancy
[Lund, Gabidulin, Honary, 2000]	optimal codes with cover distance 3 and $n-1$
[Blaum, Bruck, 2000]	one-error-correcting codes and their (low-complexity) decoding
[Sidorenko, Bossert, Gabidulin, 2010]	GMD decoding of codes in cover metric

Known (Optimal) Code Construction

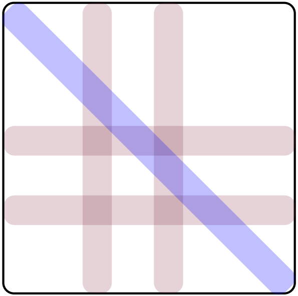
Definition (Cover-Metric Codes, [Roth, 1991])

Let $m \geq n$ and define a code $\mathbb{C}(\mathcal{C}, m)$ over $\mathbb{F}_q$ by the following set of $m \times n$ matrices:

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

where $\mathcal{C}$ is an $(n, M_{\mathsf{H}}, d)_q^{\mathsf{H}}$ code.

Properties of this Construction and Unique Decoding

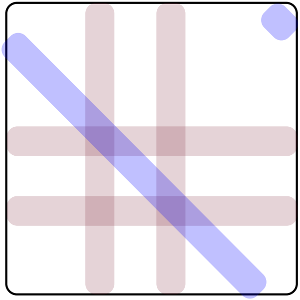


- error of cover weight t affects $\leq t$ positions of each diagonal
- $(n, M_{\mathsf{H}}, d)_q^{\mathsf{H}}$ code $\mathcal{C}$ with Hamming distance $d \geq 2t+1$ can decode uniquely on each diagonal

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

- $\mathbb{C}(\mathcal{C}, m)$ is an $(m \times n, (M_{\mathsf{H}})^m, d)_q^{\mathsf{C}}$ code
- if $\mathcal{C}$ is a linear MDS code, then $\mathbb{C}(\mathcal{C}, m)$ is an optimal $[m \times n, m(n-d+1), d]_q^{\mathsf{C}}$ code

Properties of this Construction and Unique Decoding

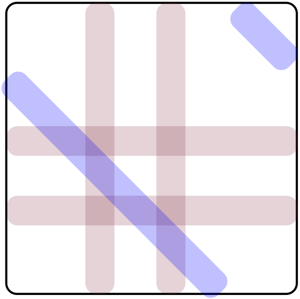


- error of cover weight t affects $\leq t$ positions of each diagonal
- $(n, M_{\mathsf{H}}, d)_q^{\mathsf{H}}$ code $\mathcal{C}$ with Hamming distance $d \geq 2t+1$ can decode uniquely on each diagonal

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

- $\mathbb{C}(\mathcal{C}, m)$ is an $(m \times n, (M_{\mathsf{H}})^m, d)_q^{\mathsf{C}}$ code
- if $\mathcal{C}$ is a linear MDS code, then $\mathbb{C}(\mathcal{C}, m)$ is an optimal $[m \times n, m(n-d+1), d]_q^{\mathsf{C}}$ code

Properties of this Construction and Unique Decoding

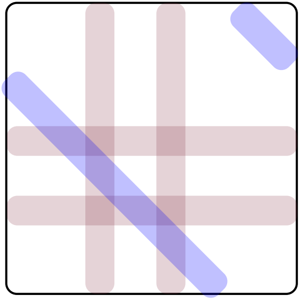


- error of cover weight t affects $\leq t$ positions of each diagonal
- $(n, M_{\mathsf{H}}, d)_q^{\mathsf{H}}$ code $\mathcal{C}$ with Hamming distance $d \geq 2t + 1$ can decode uniquely on each diagonal

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

- $\mathbb{C}(\mathcal{C}, m)$ is an $(m \times n, (M_{\mathsf{H}})^m, d)_q^{\mathsf{C}}$ code
- if $\mathcal{C}$ is a linear MDS code, then $\mathbb{C}(\mathcal{C}, m)$ is an optimal $[m \times n, m(n-d+1), d]_q^{\mathsf{C}}$ code

Properties of this Construction and Unique Decoding



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

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

- $\mathbb{C}(\mathcal{C}, m)$ is an $(m \times n, (M_{\mathsf{H}})^m, d)_q^{\mathsf{C}}$ code
- if $\mathcal{C}$ is a linear MDS code, then $\mathbb{C}(\mathcal{C}, m)$ is an optimal $[m \times n, m(n-d+1), d]_q^{\mathsf{C}}$ code

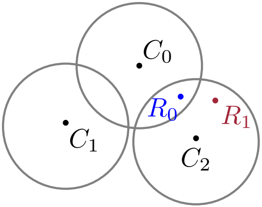
Our Contribution: List Decoding of Crisscross Errors

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

$\Longrightarrow$ list decoding up to our bound



Outline

Motivation & Problem Statement

Motivation: worst-case list size directly determines complexity of decoding algorithm.

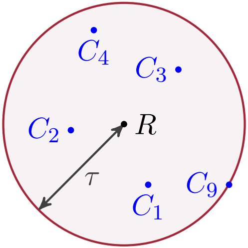
Is **polynomial-time** list decoding in the cover metric possible?

Problem (Maximum List Size)

- *$(m \times n, M, d)_q^{\mathsf{C}}$ code $\mathbb{C}$*
- *decoding radius $\tau < d$*

Find (polynomial) upper bound on

$$\ell \stackrel{\text{def}}{=} \max_{R \in \mathbb{F}_q^{m \times n}} \left\{ \left| \mathbb{C} \cap \mathcal{B}_{\mathsf{C}}^{(\tau)}(R) \right| \right\}.$$



Johnson-like Upper Bound

Theorem (Johnson-like Upper Bound)

Let $q \geq 2$ and let an integer $\tau < d \leq n, m$ be given. Denote

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

Then, for any $(m \times n, M, d)_q^{\mathsf{C}}$ code $\mathbb{C}$ and any τ such that

$$\tau < \tau_{\mathsf{C}}(q; \eta, d) \stackrel{\text{def}}{=} \eta - \sqrt{\eta(\eta - d)},$$

the list size ℓ is bounded from above by

$$\ell = \max_{R \in \mathbb{F}_q^{m \times n}} \left\{ \left| \mathbb{C} \cap \mathcal{B}_{\mathsf{C}}^{(\tau)}(R) \right| \right\} \leq \ell_{\mathsf{C}}(q; \eta, d, \tau) \stackrel{\text{def}}{=} \frac{d\eta}{\tau^2 - (2\tau - d)\eta},$$

where $\mathcal{B}_{\mathsf{C}}^{(\tau)}(R)$ denotes a ball around R of cover radius τ.

Alphabet-free Johnson-like Upper Bound

Corollary (Alphabet-free Johnson-like Bound)

For any $(m \times n, M, d)_q^{\mathsf{C}}$ *code* $\mathbb{C}$ *and any integer* τ *such that*

$$\tau < \tau_{\mathsf{C}} \overset{\text{def}}{=} n + m - \sqrt{(n+m)(n+m-d)},$$

the list size ℓ *is bounded from above by*

$$\ell \leq \ell_{\mathsf{C}} \overset{\text{def}}{=} \frac{(n+m)d}{\tau^2 - (2\tau - d)(n+m)}.$$

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

Johnson-like Bound

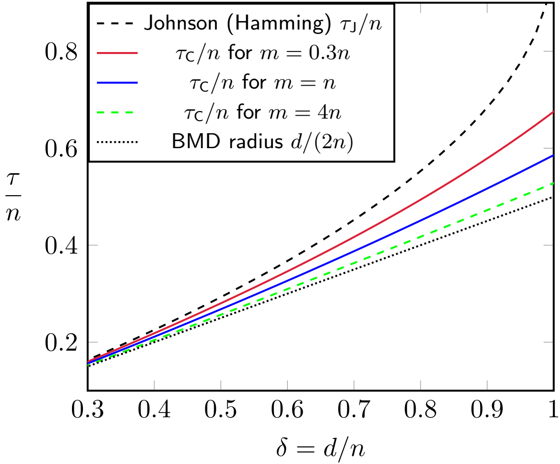


Figure : Normalized Johnson-like radius τ_{C}/n, as a function of the normalized minimum cover distance $\delta = d/n$.

Outline

Brute-Force Exponential-Time List Decoding

Given:

$R = \mathsf{vecdiag}(r^{(0)}, \dots, r^{(m-1)})$

$$\stackrel{\text{def}}{=} \begin{pmatrix} r_0^{(0)} & r_1^{(m-1)} & \cdots & r_{n-1}^{(n)} \\ r_0^{(1)} & r_1^{(0)} & \ddots & \vdots \\ \vdots & r_1^{(1)} & \ddots & r_{n-1}^{(m-1)} \\ r_0^{(n-1)} & \ddots & \ddots & r_{n-1}^{(0)} \\ r_0^{(n)} & r_1^{(n-1)} & \ddots & r_{n-1}^{(1)} \\ \vdots & \ddots & \ddots & \vdots \\ r_0^{(m-1)} & \cdots & r_{n-2}^{(n)} & r_{n-1}^{(n-1)} \end{pmatrix}$$

Task

Given R and the decoding radius τ, find all $\Gamma_i \in \mathbb{C}$, $i \in 0, \dots, \ell_{\mathsf{C}} - 1$, such that $\mathrm{wt}_{\mathsf{C}}(R - \Gamma_i) \leq \tau$.
(if possible, efficiently)

Brute-Force Exponential-Time List Decoding

Given:

$R = \mathrm{vecdiag}(r^{(0)}, \dots, r^{(m-1)})$

$$\stackrel{\text{def}}{=} \begin{pmatrix} r_0^{(0)} & r_1^{(m-1)} & \dots & r_{n-1}^{(n)} \\ r_0^{(1)} & r_1^{(0)} & \ddots & \vdots \\ \vdots & r_1^{(1)} & \ddots & r_{n-1}^{(m-1)} \\ r_0^{(n-1)} & \ddots & \ddots & r_{n-1}^{(0)} \\ r_0^{(n)} & r_1^{(n-1)} & \ddots & r_{n-1}^{(1)} \\ \vdots & \ddots & \ddots & \vdots \\ r_0^{(m-1)} & \dots & r_{n-2}^{(n)} & r_{n-1}^{(n-1)} \end{pmatrix}$$

Task

Given R and the decoding radius τ, find all $\Gamma_i \in \mathbb{C}$, $i \in 0, \dots, \ell_{\mathsf{C}} - 1$, such that $\mathrm{wt}_{\mathsf{C}}(R - \Gamma_i) \leq \tau$.
(if possible, efficiently)

$r^{(i)} = c^{(i)} + e^{(i)}$

- $c^{(i)} \in \mathcal{C}$ is $(\tau_{\mathsf{H}}, \ell_{\mathsf{H}})^{\mathsf{H}}$-list decodable
- If $\mathrm{wt}_{\mathsf{C}}(E) = t$, then $\mathrm{wt}_{\mathsf{H}}(e^{(i)}) \leq t$

Brute-Force Exponential-Time List Decoding

Given:

$R = \mathsf{vecdiag}(r^{(0)}, \dots, r^{(m-1)})$

$$\stackrel{\text{def}}{=} \begin{pmatrix} r_0^{(0)} & r_1^{(m-1)} & \cdots & r_{n-1}^{(n)} \\ r_0^{(1)} & r_1^{(0)} & \ddots & \vdots \\ \vdots & r_1^{(1)} & \ddots & r_{n-1}^{(m-1)} \\ r_0^{(n-1)} & \ddots & \ddots & r_{n-1}^{(0)} \\ r_0^{(n)} & r_1^{(n-1)} & \ddots & r_{n-1}^{(1)} \\ \vdots & \ddots & \ddots & \vdots \\ r_0^{(m-1)} & \cdots & r_{n-2}^{(n)} & r_{n-1}^{(n-1)} \end{pmatrix}$$

Brute-force list decoding:

1. Choose $\tau \leq \tau_{\mathsf{H}}$.
2. List decode each diagonal of R in $\mathcal{C}$ in Hamming metric up to τ $\leq \ell_{\mathsf{H}}$ codewords for each diagonal
3. Examine all $\leq (\ell_{\mathsf{H}})^m$ matrices C and keep only those with $\mathrm{wt}_{\mathsf{C}}(R - C) \leq \tau$

$\Longrightarrow$ Works, but has exponential time complexity.

Decoding Idea

Lemma (Bound for Two Diagonals)

- *Given* $r^{(0)}, r^{(1)} \in \mathbb{F}_q^n$*, let* $R_2 = \mathrm{vecdiag}(r^{(0)}, r^{(1)}) \in \mathbb{F}_q^{m\times n}$*,*
- *let* $\mathcal{C}$ *be a* $(n, M_{\mathsf{H}}, d)_q^{\mathsf{H}}$ *code,*
- *let* $\mathbb{C}_2 = \left\{\mathrm{vecdiag}(c^{(0)}, c^{(1)}) : c^{(0)}, c^{(1)} \in \mathcal{C}\right\} \subseteq \mathbb{F}_q^{m\times n}$*,*
- *let* $\eta_2 = (n+m)(q^2-1)/q^2$ *and let* $\ell_{\mathsf{C}}(q;\eta_2,d,\tau)$ *be defined as in our bound with* η_2*.*

Then, for any $\tau < \tau_{\mathsf{C}}(q;\eta_2,d)$*:*

$$\left|\mathbb{C}_2 \cap \mathcal{B}_{\mathsf{C}}^{(\tau)}(R_2)\right| \leq \ell_{\mathsf{C}}(q;\eta_2,d,\tau),$$

where $\mathcal{B}_{\mathsf{C}}^{(\tau)}(R_2)$ *denotes a ball of cover radius* τ *around* R_2*.*

Note: $\tau_{\mathsf{C}}(q;\eta_2,d) \geq \tau_{\mathsf{C}}(q;\eta_0,d)$, where $\eta_0 = n+m$.

Polynomial-Time List Decoding Idea

Given:
$R = \text{vecdiag}(r^{(0)}, \dots, r^{(m-1)})$

$$\stackrel{\text{def}}{=} \begin{pmatrix} r_0^{(0)} & r_1^{(m-1)} & \cdots & r_{n-1}^{(n)} \\ r_0^{(1)} & r_1^{(0)} & \ddots & \vdots \\ \vdots & r_1^{(1)} & \ddots & r_{n-1}^{(m-1)} \\ r_0^{(n-1)} & \ddots & \ddots & r_{n-1}^{(0)} \\ r_0^{(n)} & r_1^{(n-1)} & \ddots & r_{n-1}^{(1)} \\ \vdots & \ddots & \ddots & \vdots \\ r_0^{(m-1)} & \cdots & r_{n-2}^{(n)} & r_{n-1}^{(n-1)} \end{pmatrix}$$

Task

Given R and the decoding radius τ, find all $\Gamma_i \in \mathbb{C}$, $i \in 0, \dots, \ell_{\mathsf{C}} - 1$, efficiently such that $\text{wt}_{\mathsf{C}}(R - \Gamma_i) \leq \tau$.

$r^{(i)} = c^{(i)} + e^{(i)}$

- $c^{(i)} \in \mathcal{C}$ is $(\tau_{\mathsf{H}}, \ell_{\mathsf{H}})^{\mathsf{H}}$-list decodable
- If $\text{wt}_{\mathsf{C}}(E) = t$, then $\text{wt}_{\mathsf{H}}(e^{(i)}) \leq t$

Polynomial-Time List Decoding Idea

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

$$\stackrel{\text{def}}{=} \begin{pmatrix} r_0^{(0)} & r_1^{(m-1)} & \cdots & r_{n-1}^{(n)} \\ r_0^{(1)} & r_1^{(0)} & \ddots & \vdots \\ \vdots & r_1^{(1)} & \ddots & r_{n-1}^{(m-1)} \\ r_0^{(n-1)} & \ddots & \ddots & r_{n-1}^{(0)} \\ r_0^{(n)} & r_1^{(n-1)} & \ddots & r_{n-1}^{(1)} \\ \vdots & \ddots & \ddots & \vdots \\ r_0^{(m-1)} & \cdots & r_{n-2}^{(n)} & r_{n-1}^{(n-1)} \end{pmatrix}$$

Efficient list decoding:

1. Choose $\tau \leq \min\{\tau_{\mathsf{H}}, \lceil \tau_{\mathsf{C}} \rceil - 1\}$
2. List decode each diagonal of R
   $\leq \ell_{\mathsf{H}}$ codewords for each diagonal
3. Examine all $\leq (\ell_{\mathsf{H}})^2$ matrices C_2 with two (fixed) non-zero diagonals;
   keep only those with $\mathrm{wt}_{\mathsf{C}}(R - C_2) \leq \tau$
   $\leq \ell_{\mathsf{C}}$ matrices
4. add another diagonal and examine all
   $\leq \ell_{\mathsf{H}} \cdot \ell_{\mathsf{C}}$ matrices
   $\leq \ell_{\mathsf{C}}$ matrices
5. ...

$\Longrightarrow$ has polynomial time complexity!

Decoding Algorithm

Input: $\mathbf{R} = \text{vecdiag}(r^{(0)}, r^{(1)}, \ldots, r^{(m-1)}) \in \mathbb{F}_q^{m\times n}$
parameters of constituent code $\mathcal{C}$: q, n, d, τ_{H}
integer τ with $\tau < \min\{\tau_{\mathsf{H}}, \lceil \tau_{\mathsf{C}} \rceil - 1\}$ ← list decoding radius τ

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

for $i = 0$ **to** $m-1$ **do**
- $\mathcal{L}_i^{\mathsf{H}} = \{e_0^{(i)}, e_1^{(i)}, \ldots, e_{\ell_i}^{(i)}\} \leftarrow$ $\textsc{ListDecodingConstituent}\big(\mathcal{C};\, r^{(i)};\, \tau\big)$ ← list decoding of constituent code
- **if** $\mathcal{L}_i^{\mathsf{H}} = \emptyset$ **then**
  - **return** $\mathcal{L}^{\mathsf{C}} = \emptyset$

foreach $e^{(0)} \in \mathcal{L}_0^{\mathsf{H}}$ **do**
- $\mathcal{L}_0^{\mathsf{C}} \leftarrow \mathcal{L}_0^{\mathsf{C}} \cup \{\text{vecdiag}(e^{(0)})\}$

for $i = 1$ **to** $m-1$ **do**
- **foreach** $\text{vecdiag}(e^{(0)}, \ldots, e^{(i-1)}) \in \mathcal{L}_{i-1}^{\mathsf{C}}$ **do**
  - **foreach** $e^{(i)} \in \mathcal{L}_i^{\mathsf{H}}$ **do**
    - $E \leftarrow \text{vecdiag}(e^{(0)}, \ldots, e^{(i-1)}, e^{(i)})$ ← sort out matrices
    - **if** $\mathrm{wt}_{\mathsf{C}}(E) \leq \tau$ **then**
      - $\mathcal{L}_i^{\mathsf{C}} \leftarrow \mathcal{L}_i^{\mathsf{C}} \cup \{E\}$
- **if** $\mathcal{L}_i^{\mathsf{C}} = \emptyset$ **then**
  - **return** $\mathcal{L}^{\mathsf{C}} = \emptyset$

$\mathcal{L}^{\mathsf{C}} \leftarrow \mathcal{L}_{m-1}^{\mathsf{C}}$

Output: List of error matrices: $\mathcal{L}^{\mathsf{C}}$ ← output list

List decoding: Summary

Theorem (List Decoding)

- *Let the code* $\mathbb{C}(\mathcal{C}, m)$ *be as before,*
- *suppose* $\mathcal{C}$ *is* $(\tau_{\mathsf{H}}, \ell_{\mathsf{H}})^{\mathsf{H}}$*-list decodable with complexity* $\mathcal{D}_{\mathsf{H}}(\mathcal{C})$*,*
- *let* $R \in \mathbb{F}_q^{m \times n}$ *be given.*

Then, for any integer $\tau \leq \min\{\tau_{\mathsf{H}}, \lceil \tau_{\mathsf{C}} \rceil - 1\}$*, our algorithm returns all* $E \in \mathbb{F}_q^{m \times n}$ *such that*

$$\mathrm{wt}_{\mathsf{C}}(E) \leq \tau \text{ and } (R - E) \in \mathbb{C}.$$

The complexity of this decoder is

$$\mathcal{O}\big(m \cdot \mathcal{D}_{\mathsf{H}}(\mathcal{C}) + m \cdot \ell_{\mathsf{H}} \cdot \ell_{\mathsf{C}} \cdot \mathcal{W}_{\mathsf{C}}(m, n)\big),$$

and the list size is at most ℓ_{C}*.*

cover weight calculation $\mathcal{W}_{\mathsf{C}}(m, n) = \mathcal{O}((n + m)n^2)$

Outline

Conclusion and Outlook

Contributions

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