Generic Decoding in the Cover Metric

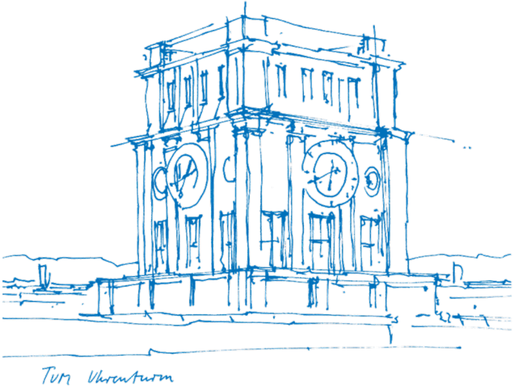
Sebastian Bitzer, Julian Renner,

Antonia Wachter-Zeh, Violetta Weger

Technical University of Munich

Institute for Communications Engineering

April 26, 2023



Post-Quantum Cryptography

- Quantum computer breaks cryptography based on number theory

Post-Quantum Cryptography

- Quantum computer breaks cryptography based on number theory
- NP-hard problems in coding theory

Post-Quantum Cryptography

- Quantum computer breaks cryptography based on number theory
- NP-hard problems in coding theory

Hamming Metric

well trusted

Post-Quantum Cryptography

- Quantum computer breaks cryptography based on number theory
- NP-hard problems in coding theory

Hamming Metric	**Rank Metric**
well trusted	smaller sizes

Post-Quantum Cryptography

- Quantum computer breaks cryptography based on number theory
- NP-hard problems in coding theory

Hamming Metric	**Cover Metric**	**Rank Metric**
well trusted	?	smaller sizes

The Cover Metric

Gabidulin, E. M. (1985). Optimal array error-correcting codes. *Probl. Peredach. Inform.*

Roth, R. M. (1991). Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. on Inf. Th.*

The Cover Metric

Gabidulin, E. M. (1985). Optimal array error-correcting codes. *Probl. Peredach. Inform.*

Roth, R. M. (1991). Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. on Inf. Th.*

- Cover: set of rows & columns
  that contains all non-zero entries

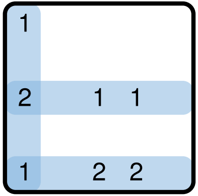
$$\begin{bmatrix} 1 & & & & \\ & & & & \\ 2 & & 1 & 1 & \\ & & & & \\ 1 & & 2 & 2 & \end{bmatrix}$$

The Cover Metric

Gabidulin, E. M. (1985). Optimal array error-correcting codes. *Probl. Peredach. Inform.*

Roth, R. M. (1991). Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. on Inf. Th.*

- Cover: set of rows & columns that contains all non-zero entries

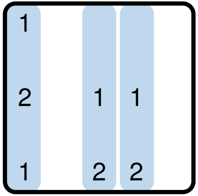


The Cover Metric

Gabidulin, E. M. (1985). Optimal array error-correcting codes. *Probl. Peredach. Inform.*

Roth, R. M. (1991). Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. on Inf. Th.*

- Cover: set of rows & columns that contains all non-zero entries

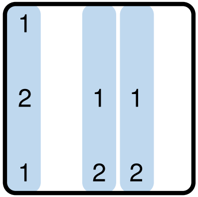


The Cover Metric

Gabidulin, E. M. (1985). Optimal array error-correcting codes. *Probl. Peredach. Inform.*

Roth, R. M. (1991). Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. on Inf. Th.*

- Cover: set of rows & columns that contains all non-zero entries
- Weight: size of minimum cover

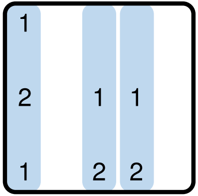


The Cover Metric

Gabidulin, E. M. (1985). Optimal array error-correcting codes. *Probl. Peredach. Inform.*

Roth, R. M. (1991). Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. on Inf. Th.*

- **Cover**: set of rows & columns that contains all non-zero entries
- **Weight**: size of minimum cover
  $\mathrm{wt}_R(A) \leq \mathrm{wt}_C(A) \leq \mathrm{wt}_H(A)$

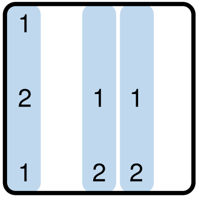


The Cover Metric

Gabidulin, E. M. (1985). Optimal array error-correcting codes. *Probl. Peredach. Inform.*

Roth, R. M. (1991). Maximum-rank array codes and their application to crisscross error correction. *IEEE Trans. on Inf. Th.*

- **Cover**: set of rows & columns that contains all non-zero entries
- **Weight**: size of minimum cover $\mathrm{wt}_R(A) \leq \mathrm{wt}_C(A) \leq \mathrm{wt}_H(A)$
- **Distance**: $\mathrm{d}_C(A, B) = \mathrm{wt}_C(A - B)$



$\mathbb{F}_q$-Linear Matrix Codes

- Generators $G_1, \dots, G_k \in \mathbb{F}_q^{m \times n}$

$$G_1 = \begin{bmatrix} 1 & & \\ & 1 & \\ 1 & & 1 \end{bmatrix} \quad \cdots \quad G_k = \begin{bmatrix} & 2 & \\ & & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

$\mathbb{F}_q$-Linear Matrix Codes

- Generators $G_1, \ldots, G_k \in \mathbb{F}_q^{m \times n}$
- Code $\mathcal{C} = \langle G_1, \ldots, G_k \rangle$

$$\overset{u_1 G_1}{\begin{bmatrix} 1 & & \\ & 1 & \\ 1 & & 1 \end{bmatrix}} + \cdots + \overset{u_k G_k}{\begin{bmatrix} & 2 & \\ & & 1 \\ 1 & 1 & 2 \end{bmatrix}} = \overset{C \in \mathcal{C}}{\begin{bmatrix} 1 & 2 & \\ & 1 & 1 \\ 2 & 1 & \end{bmatrix}}$$

$\mathbb{F}_q$-Linear Matrix Codes

- Generators $G_1, \ldots, G_k \in \mathbb{F}_q^{m \times n}$
- Code $\mathcal{C} = \langle G_1, \ldots, G_k \rangle$
- Minimum distance $d = \min_{A \in \mathcal{C} \setminus \{0\}} \mathrm{wt}_C(A)$

$$\overset{u_1 G_1}{\begin{bmatrix} 1 & & \\ & 1 & \\ 1 & & 1 \end{bmatrix}} + \cdots + \overset{u_k G_k}{\begin{bmatrix} & 2 & \\ & & 1 \\ 1 & 1 & 2 \end{bmatrix}} = \overset{C \in \mathcal{C}}{\begin{bmatrix} 1 & 2 & \\ & 1 & 1 \\ 2 & 1 & \end{bmatrix}}$$

$\mathbb{F}_q$-Linear Matrix Codes

- Generators $G_1, \ldots, G_k \in \mathbb{F}_q^{m \times n}$
- Code $\mathcal{C} = \langle G_1, \ldots, G_k \rangle$
- Minimum distance
  $d = \min_{A \in \mathcal{C} \setminus \{0\}} \mathrm{wt}_C(A)$

$$\overset{u_1 G_1}{\begin{bmatrix}1 & & \\ & 1 & \\ 1 & & 1\end{bmatrix}} + \cdots + \overset{u_k G_k}{\begin{bmatrix} & 2 & \\ & & 1 \\ 1 & 1 & 2\end{bmatrix}} = \overset{C \in \mathcal{C}}{\begin{bmatrix}1 & 2 & \\ & 1 & 1 \\ 2 & 1 & \end{bmatrix}}$$

Theorem (Random Codes are Optimal)

For $\min\{m, n\} \to \infty$, random linear codes achieve w.h.p. the cover-metric Singleton bound

$$k \leq \max\{m, n\}(\min\{m, n\} - d + 1).$$

Decoding Random Codes in the Cover Metric

Cover-Metric Decoding Problem

Given: random linear code $\mathcal{C} \subset \mathbb{F}_q^{m \times n}$, error weight $t \leq \min\{m, n\}$
and corrupted codeword $Y = C + E \in \mathbb{F}_q^{m \times n}$

Find: codeword $C \in \mathcal{C}$ such that $\mathrm{d}_C(Y, C) = t$.

Decoding Random Codes in the Cover Metric

Cover-Metric Decoding Problem

Given: random linear code $\mathcal{C} \subset \mathbb{F}_q^{m \times n}$, error weight $t \leq \min\{m, n\}$
and corrupted codeword $Y = C + E \in \mathbb{F}_q^{m \times n}$
Find: codeword $C \in \mathcal{C}$ such that $\mathrm{d}_C(Y, C) = t$.

Theorem

The cover-metric decoding problem is NP-hard.

Prange-like Decoding Algorithm

$$Y = C + E$$

$$\begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 1 & 2 \end{bmatrix}$$

Prange-like Decoding Algorithm

$$Y = C + E$$

$$\begin{bmatrix} 1 & 0 & 2 & \color{red}{2} & 1 \\ \color{red}{1} & \color{red}{2} & \color{red}{2} & \color{red}{1} & \color{red}{2} \\ 1 & 0 & 1 & \color{red}{2} & 1 \\ 0 & 2 & 0 & \color{red}{2} & 0 \\ 1 & 0 & 1 & \color{red}{1} & 2 \end{bmatrix}$$

Prange-like Decoding Algorithm

$$\begin{array}{ccc} Y = C + E & & \hat{C} \in \mathcal{C} \\ \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 1 & 2 \end{bmatrix} & \xrightarrow{\text{re-encode}} & \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 1 & 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 2 \end{bmatrix} \end{array}$$

Prange-like Decoding Algorithm

$$Y = C + E \qquad \xrightarrow{\text{re-encode}} \qquad \hat{C} \in \mathcal{C}$$

$$\begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 1 & 2 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 1 & 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 2 \end{bmatrix}$$

Prange-like Decoding Algorithm

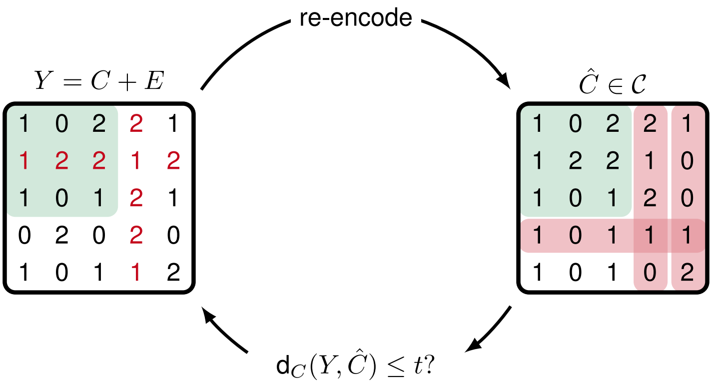
re-encode

$$Y = C + E \qquad \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 1 & 2 \end{bmatrix}$$

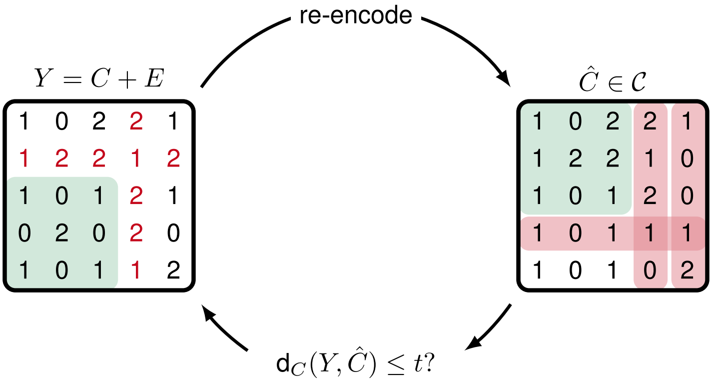
$$\hat{C} \in \mathcal{C} \qquad \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 1 & 0 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 2 \end{bmatrix}$$

$\mathsf{d}_C(Y, \hat{C}) \leq t?$

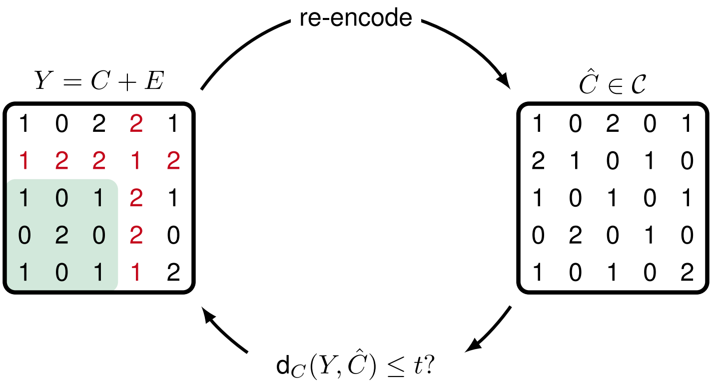
Prange-like Decoding Algorithm



Prange-like Decoding Algorithm



Prange-like Decoding Algorithm



Prange-like Decoding Algorithm

$$Y = C + E \qquad \begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 1 & 2 \end{bmatrix} \xrightarrow{\text{re-encode}} \begin{bmatrix} 1 & 0 & 2 & 0 & 1 \\ 2 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 2 \end{bmatrix} \qquad \hat{C} \in \mathcal{C}$$

$\mathsf{d}_C(Y, \hat{C}) \leq t?$

Prange-like Decoding Algorithm

re-encode

$Y = C + E$

$$\begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 1 & 2 \end{bmatrix}$$

$\hat{C} \in \mathcal{C}$

$$\begin{bmatrix} 1 & 0 & 2 & 0 & 1 \\ 2 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 2 \end{bmatrix}$$

$\mathrm{d}_C(Y, \hat{C}) \leq t?$

success

Prange-like Decoding Algorithm

re-encode

$Y = C + E$

$$\begin{bmatrix} 1 & 0 & 2 & 2 & 1 \\ 1 & 2 & 2 & 1 & 2 \\ 1 & 0 & 1 & 2 & 1 \\ 0 & 2 & 0 & 2 & 0 \\ 1 & 0 & 1 & 1 & 2 \end{bmatrix}$$

Complexity?

$\hat{C} \in \mathcal{C}$

$$\begin{bmatrix} 1 & 0 & 2 & 0 & 1 \\ 2 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 2 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 2 \end{bmatrix}$$

$\mathsf{d}_C(Y, \hat{C}) \leq t?$

$\downarrow$

success

Overview of Analysis

Decoding Complexity

Overview of Analysis

- Cost $=$ number of iterations $\times$ cost of iteration

Decoding Complexity

Overview of Analysis

- Cost $=$ number of iterations $\times$ cost of iteration
- Worst-case instance: $n = m$

Decoding Complexity

Overview of Analysis

- Cost $=$ number of iterations $\times$ cost of iteration
- Worst-case instance: $n = m$
- Optimal choice: information symbols in block

Decoding Complexity

Overview of Analysis

- Cost $=$ number of iterations $\times$ cost of iteration
- Worst-case instance: $n = m$
- Optimal choice: information symbols in block
- Complexity exponential in $\sqrt{\text{symbols}}$

Conclusion

Hamming Metric	Cover Metric	Rank Metric
well trusted	?	smaller sizes

Conclusion

Hamming Metric	Cover Metric	Rank Metric
well trusted	mixed results	smaller sizes

Conclusion

Hamming Metric	**Cover Metric**	**Rank Metric**
well trusted	mixed results	smaller sizes
GV	GV $=$ Singleton	GV

Conclusion

Hamming Metric	Cover Metric	Rank Metric
well trusted	mixed results	smaller sizes
GV	GV = Singleton	GV
NP-hard	NP-hard	NP-hard

Conclusion

Hamming Metric	Cover Metric	Rank Metric
well trusted	mixed results	smaller sizes
GV	GV $=$ Singleton	GV
NP-hard	NP-hard	NP-hard
symbols	$\sqrt{\text{symbols}}$	symbols

Conclusion

Hamming Metric	Cover Metric	Rank Metric
well trusted	mixed results	smaller sizes
GV	GV $=$ Singleton	GV
NP-hard	NP-hard	NP-hard
symbols	$\sqrt{\text{symbols}}$	symbols

Thank you! Questions?

Generic Decoding in the Cover Metric is NP-Hard

$$\underset{r \in \mathbb{F}_q^n}{\boxed{1\ \ 0\ \ 0\ \ 1\ \ 1}} = \underset{c \in \langle g_1, \dots, g_k \rangle}{\boxed{1\ \ 0\ \ 1\ \ 0\ \ 1}} + \underset{\mathrm{wt}_H(e) = t}{\boxed{\ \ \ \ \ \ \ \ 1\ \ 1\ \ \ \ }}$$

$$\underset{R \in \mathbb{F}_q^{(t+1)\times n}}{\boxed{\begin{matrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{matrix}}} = \underset{C \in \langle G_1, \dots, G_k \rangle}{\boxed{\begin{matrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{matrix}}} + \underset{\mathrm{wt}_C(E) = t}{\boxed{\begin{matrix} & & & 1 & 1 & \\ & & & 1 & 1 & \\ & & & 1 & 1 & \end{matrix}}}$$

Random Errors in the Cover Metric

General Error Model

An error E of cover weight t is created by choosing E uniformly at random from $\{A \in \mathbb{F}_q^{m \times n} \mid \mathrm{wt}_C(A) = t\}$.

For large m and n, the minimum-size cover of a matrix is unique with high probability

simplifying approximation

Simple Error Model

- Pick t rows and columns uniformly at random
- Fill picked lines with random entries form $\mathbb{F}_q$
- If $\mathrm{wt}_C(E) < t$, the process is repeated