Design of MDP Convolutional Codes and Maximally Recoverable Codes Through the Lens of Matrix Completion

Sakshi Dang

Department of Electrical Communication Engineering
Indian Institute of Science
Bengaluru-560012, India

sakshidang10@gmail.com

Joint work with

Julia Lieb, Pedro Soto, and Alex Sprintson

14th International Workshop on Coding Theory and Cryptography
June 8-12, 2026

Overview

- What is Matrix Completion?
- Construction of MDP convolutional codes.
- Construction of Maximally Recoverable codes.

Linear Codes

- $\mathbb{F}_q$: finite field with q elements, $q = p^\gamma$, p prime, $\gamma \geq 1$.

Linear Codes

- $\mathbb{F}_q$: finite field with q elements, $q = p^\gamma$, p prime, $\gamma \geq 1$.
- Linear code $\mathcal{C}$ of length n: a subspace of $\mathbb{F}_q^n$.

Linear Codes

- $\mathbb{F}_q$: finite field with q elements, $q = p^\gamma$, p prime, $\gamma \geq 1$.
- Linear code $\mathcal{C}$ of length n: a subspace of $\mathbb{F}_q^n$.
- $[n, k]_q$- code: linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$.

Linear Codes

- $\mathbb{F}_q$: finite field with q elements, $q = p^\gamma$, p prime, $\gamma \geq 1$.
- Linear code $\mathcal{C}$ of length n: a subspace of $\mathbb{F}_q^n$.
- $[n, k]_q$- code: linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$.
- A $k \times n$ matrix G of rank k is called Generator matrix of $\mathcal{C}$ if

$$\mathcal{C} = \{uG : (u_1, \ldots, u_k) \in \mathbb{F}_q^k\}.$$

Linear Codes

- $\mathbb{F}_q$: finite field with q elements, $q = p^\gamma$, p prime, $\gamma \geq 1$.
- Linear code $\mathcal{C}$ of length n: a subspace of $\mathbb{F}_q^n$.
- $[n, k]_q$- code: linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$.
- A $k \times n$ matrix G of rank k is called Generator matrix of $\mathcal{C}$ if

$$\mathcal{C} = \{uG : (u_1, \ldots, u_k) \in \mathbb{F}_q^k\}.$$

- The minimum distance $d(\mathcal{C})$ of a $[n, k]_q$-code $\mathcal{C}$ is defined by

$$d(\mathcal{C}) := \min_{\boldsymbol{c} \in \mathcal{C},\ \boldsymbol{c} \neq 0} |\{i \in [n] : c_i \neq 0\}|.$$

Linear Codes

- $\mathbb{F}_q$: finite field with q elements, $q = p^\gamma$, p prime, $\gamma \geq 1$.
- Linear code $\mathcal{C}$ of length n: a subspace of $\mathbb{F}_q^n$.
- $[n, k]_q$- code: linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$.
- A $k \times n$ matrix G of rank k is called Generator matrix of $\mathcal{C}$ if

$$\mathcal{C} = \{uG : (u_1, \ldots, u_k) \in \mathbb{F}_q^k\}.$$

- The minimum distance $d(\mathcal{C})$ of a $[n, k]_q$-code $\mathcal{C}$ is defined by

$$d(\mathcal{C}) := \min_{\boldsymbol{c} \in \mathcal{C},\ \boldsymbol{c} \neq 0} |\{i \in [n] : c_i \neq 0\}|.$$

- Singleton Bound: $d(\mathcal{C}) \leq n - k + 1$.

Linear Codes

- $\mathbb{F}_q$: finite field with q elements, $q = p^\gamma$, p prime, $\gamma \geq 1$.
- Linear code $\mathcal{C}$ of length n: a subspace of $\mathbb{F}_q^n$.
- $[n, k]_q$- code: linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$.
- A $k \times n$ matrix G of rank k is called Generator matrix of $\mathcal{C}$ if

$$\mathcal{C} = \{uG : (u_1, \ldots, u_k) \in \mathbb{F}_q^k\}.$$

- The minimum distance $d(\mathcal{C})$ of a $[n, k]_q$-code $\mathcal{C}$ is defined by

$$d(\mathcal{C}) := \min_{\boldsymbol{c} \in \mathcal{C},\ \boldsymbol{c} \neq 0} |\{i \in [n] : c_i \neq 0\}|.$$

- Singleton Bound: $d(\mathcal{C}) \leq n - k + 1$.
- $\mathcal{C}$ is called Maximum Distance Separable (MDS) if $d(\mathcal{C}) = n - k + 1$.

What is Matrix Completion?

Given a matrix with fixed position of zeros and remaining entries as variables (denoted by x).

x	x	0	0	x	x
0	0	x	x	x	x
x	x	x	x	0	0

What is Matrix Completion?

Given a matrix with fixed position of zeros and remaining entries as variables (denoted by X).

x	x	0	0	x	x
0	0	x	x	x	x
x	x	x	x	0	0

Goal: Find values/solution for these variable entries (X) such that the matrix becomes a Generator matrix for the particular code under discussion.

Example

Complete the matrix given below such that it becomes a generator matrix for an MDS code.

x	x	0	0	x	x
0	0	x	x	x	x
x	x	x	x	0	0

Determine the values of x that satisfy the MDS condition[1].

[1] Shachar Lovett, MDS matrices over small fields: A proof of the GM- MDS conjecture, in: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pp 194–199, 2018.

Example

Complete the matrix given below such that it becomes a generator matrix for an MDS code.

x	x	0	0	x	x
0	0	x	x	x	x
x	x	x	x	0	0

Determine the values of x that satisfy the MDS condition[1].

- Every $k \times k$ minor is nonzero,
- Matrix does not contain an all zero submatrix of size $a \times b$, such that $a + b \geq k + 1$.

[1] Shachar Lovett, MDS matrices over small fields: A proof of the GM- MDS conjecture, in: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pp 194–199, 2018.

Example

Complete the matrix given below such that it becomes a generator matrix for an MDS code.

x	x	0	0	x	x
0	0	x	x	x	x
x	x	x	x	0	0

Determine the values of x that satisfy the MDS condition[1].

- Every 3×3 minor is nonzero,
- The matrix should not have a zero submatrix of the following sizes: 1×3, 1×4, 2×2, 2×3, 2×4, 3×1, 3×2, 3×3, 3×4.

[1] Shachar Lovett, MDS matrices over small fields: A proof of the GM- MDS conjecture, in: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pp 194–199, 2018.

Example

Complete the matrix given below such that it becomes a generator matrix for an MDS code.

x	x	0	0	x	x
0	0	x	x	x	x
x	x	x	x	0	0

Determine the values of x that satisfy the MDS condition[1].

Solution: Over $\mathbb{F}_3$:

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

[1] Shachar Lovett, MDS matrices over small fields: A proof of the GM- MDS conjecture, in: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pp 194–199, 2018.

Matrix completion problem

Goal: Construct a matrix that meets specific rank conditions on its minors while adhering to structural constraints, such as predefined row support patterns.

Matrix completion problem

Goal: Construct a matrix that meets specific rank conditions on its minors while adhering to structural constraints, such as predefined row support patterns.

Definition

Let $M = (m_{i,j})$ be a $K \times N$ matrix with entries $m_{i,j}$ considered as variables. Define $\mathbb{F}_q[M] := \mathbb{F}_q[m_{1,1}, \ldots, m_{K,N}]$ and consider a set of polynomials $f_\ell(M) \in \mathbb{F}_q[M]$ for $\ell = 1, \ldots, s$.

*A **solution** to the **matrix completion problem** is a set of values for $m_{i,j} \in \mathbb{F}_q$ satisfying the following conditions:*

- *$f_\ell(M) = 0$ for $\ell = 1, \ldots, s$.*
- *all **non-trivial full-size minors**, i.e., the $K \times K$ minors of M that are not nilpotent in the ring $\mathbb{F}_q[M]/\langle f_1(M), \ldots, f_s(M)\rangle$, are non-zero at the values chosen for $m_{i,j}$.*

Construction of MDP convolutional codes

Convolutional codes

- Convolutional code of length n over $\mathbb{F}_q$: An $\mathbb{F}_q[z]$-submodule $\mathcal{C}$ of $\mathbb{F}_q[z]^n$.

Convolutional codes

- Convolutional code of length n over $\mathbb{F}_q$: An $\mathbb{F}_q[z]$-submodule $\mathcal{C}$ of $\mathbb{F}_q[z]^n$.
- Generator matrix of $\mathcal{C}$: A matrix $G(z) \in \mathbb{F}_q[z]^{k \times n}$ of rank k such that

$$\mathcal{C} = \{c(z) = m(z)G(z) \in \mathbb{F}_q[z]^n \mid m(z) \in \mathbb{F}_q[z]^k\}.$$

Convolutional codes

- Convolutional code of length n over $\mathbb{F}_q$: An $\mathbb{F}_q[z]$-submodule $\mathcal{C}$ of $\mathbb{F}_q[z]^n$.
- Generator matrix of $\mathcal{C}$: A matrix $G(z) \in \mathbb{F}_q[z]^{k \times n}$ of rank k such that

$$\mathcal{C} = \{c(z) = m(z)G(z) \in \mathbb{F}_q[z]^n \mid m(z) \in \mathbb{F}_q[z]^k\}.$$

- Degree of $\mathcal{C}$, $\delta := \max\{\deg(\Delta(z)) : \Delta(z) \text{ is a } k \times k \text{ minor of } G(z)\}$.

Convolutional codes

- Convolutional code of length n over $\mathbb{F}_q$: An $\mathbb{F}_q[z]$-submodule $\mathcal{C}$ of $\mathbb{F}_q[z]^n$.
- Generator matrix of $\mathcal{C}$: A matrix $G(z) \in \mathbb{F}_q[z]^{k \times n}$ of rank k such that

$$\mathcal{C} = \{c(z) = m(z)G(z) \in \mathbb{F}_q[z]^n \mid m(z) \in \mathbb{F}_q[z]^k\}.$$

- Degree of $\mathcal{C}$, $\delta := \max\{\deg(\Delta(z)) : \Delta(z) \text{ is a } k \times k \text{ minor of } G(z)\}$.
- For $j \geq 0$, the j-th column distance of $\mathcal{C}$ is

$$d_j^c(\mathcal{C}) := \min\left\{ \sum_{t=0}^{j} \mathrm{wt}_H(c_t) : \quad c(z) = \sum_{t \geq 0} c_t z^t \in \mathcal{C} \text{ and } c_0 \neq 0 \right\}.$$

Convolutional codes

- Convolutional code of length n over $\mathbb{F}_q$: An $\mathbb{F}_q[z]$-submodule $\mathcal{C}$ of $\mathbb{F}_q[z]^n$.
- Generator matrix of $\mathcal{C}$: A matrix $G(z) \in \mathbb{F}_q[z]^{k \times n}$ of rank k such that

$$\mathcal{C} = \{c(z) = m(z)G(z) \in \mathbb{F}_q[z]^n \mid m(z) \in \mathbb{F}_q[z]^k\}.$$

- Degree of $\mathcal{C}$, $\delta := \max\{\deg(\Delta(z)) : \Delta(z) \text{ is a } k \times k \text{ minor of } G(z)\}$.
- For $j \geq 0$, the j-th column distance of $\mathcal{C}$ is

$$d_j^c(\mathcal{C}) := \min\left\{ \sum_{t=0}^{j} \mathrm{wt}_H(c_t) : \quad c(z) = \sum_{t\geq 0} c_t z^t \in \mathcal{C} \text{ and } c_0 \neq 0 \right\}.$$

- Generalized singleton bound: For $j \geq 0$

$$d_j^c(\mathcal{C}) \leq (n-k)(j+1) + 1.$$

Convolutional codes

- Convolutional code of length n over $\mathbb{F}_q$: An $\mathbb{F}_q[z]$-submodule $\mathcal{C}$ of $\mathbb{F}_q[z]^n$.
- Generator matrix of $\mathcal{C}$: A matrix $G(z) \in \mathbb{F}_q[z]^{k \times n}$ of rank k such that

$$\mathcal{C} = \{c(z) = m(z)G(z) \in \mathbb{F}_q[z]^n \mid m(z) \in \mathbb{F}_q[z]^k\}.$$

- Degree of $\mathcal{C}$, $\delta := \max\{\deg(\Delta(z)) : \Delta(z) \text{ is a } k \times k \text{ minor of } G(z)\}$.
- For $j \geq 0$, the j-th column distance of $\mathcal{C}$ is

$$d_j^c(\mathcal{C}) := \min\left\{\sum_{t=0}^{j} \mathrm{wt}_H(c_t) : \quad c(z) = \sum_{t\geq 0} c_t z^t \in \mathcal{C} \text{ and } c_0 \neq 0\right\}.$$

- Generalized singleton bound: For $j \geq 0$

$$d_j^c(\mathcal{C}) \leq (n-k)(j+1)+1.$$

- $\mathcal{C}$ is called maximum distance profile (MDP) if

$$d_L^c(\mathcal{C}) = (n-k)(L+1)+1, \qquad \text{where } L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor.$$

Characterization of MDP Convolutional codes

Let $\mathcal{C}$ be (n, k, δ)-convolutional code with $G(z) = \sum_{i \geq 0} G_i z^i$ and $G_i \in \mathbb{F}_q^{k \times n}$.

Characterization of MDP Convolutional codes

Let $\mathcal{C}$ be (n, k, δ)-convolutional code with $G(z) = \sum_{i \geq 0} G_i z^i$ and $G_i \in \mathbb{F}_q^{k \times n}$.

For $j \geq 0$, define j^{th}-Sliding generator matrix G_j^c by

$$G_j^c := \begin{pmatrix} G_0 & G_1 & \cdots & G_j \\ \mathbf{0} & G_0 & \cdots & G_{j-1} \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{0} & G_0 \end{pmatrix} \in \mathbb{F}_q^{(j+1)k \times (j+1)n}.$$

Characterization of MDP Convolutional codes

Let $\mathcal{C}$ be (n, k, δ)-convolutional code with $G(z) = \sum_{i \geq 0} G_i z^i$ and $G_i \in \mathbb{F}_q^{k \times n}$.

For $j \geq 0$, define j^{th}-Sliding generator matrix G_j^c by

$$G_j^c := \begin{pmatrix} G_0 & G_1 & \cdots & G_j \\ \mathbf{0} & G_0 & \cdots & G_{j-1} \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{0} & G_0 \end{pmatrix} \in \mathbb{F}_q^{(j+1)k \times (j+1)n}.$$

Nontrivial minor[2]: $(j+1)k \times (j+1)k$ minor of G_j^c formed by columns with indices $t_1 < \cdots < t_{(j+1)k}$, where $t_{sk+1} > sn$, for $s = 0, 1, 2, \ldots, j$.

[2] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache, Strongly MDS convolutional codes, *IEEE Trans. Inf. Theory*, **52** (2006), 584–598.

Characterization of MDP Convolutional codes

Let $\mathcal{C}$ be (n, k, δ)-convolutional code with $G(z) = \sum_{i \geq 0} G_i z^i$ and $G_i \in \mathbb{F}_q^{k \times n}$.

For $j \geq 0$, define j^{th}-Sliding generator matrix G_j^c by

$$G_j^c := \begin{pmatrix} G_0 & G_1 & \cdots & G_j \\ \mathbf{0} & G_0 & \cdots & G_{j-1} \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \cdots & \mathbf{0} & G_0 \end{pmatrix} \in \mathbb{F}_q^{(j+1)k \times (j+1)n}.$$

Nontrivial minor[2]: $(j+1)k \times (j+1)k$ minor of G_j^c formed by columns with indices $t_1 < \cdots < t_{(j+1)k}$, where $t_{sk+1} > sn$, for $s = 0, 1, 2, \ldots, j$.

Theorem (Gluesing-Luerssen, Rosenthal, Smarandache, 2006)

For $0 \leq j \leq L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$. *The following statements are equivalent:*

(a) $d_j^c(\mathcal{C}) = (n-k)(j+1) + 1.$

(b) *Every nontrivial minor of* G_j^c *is nonzero.*

This shows that the code is MDP if every nontrivial minor of G_L^c *is nonzero.*

[2] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache, Strongly MDS convolutional codes, *IEEE Trans. Inf. Theory*, **52** (2006), 584–598.

Partial unit-memory MDP convolutional codes

Let $\mathcal{C}$ be a convolutional code with generator matrix $G(z) = G_0 + G_1 z$.

- $\mathcal{C}$ is called partial unit-memory if $\mathrm{rank}(G_1) < k$. Moreover, a partial unit-memory convolutional code is MDP if and only if all $2k \times 2k$ nontrivial minors of G_1^c are nonzero where

$$G_1^c := \begin{bmatrix} G_0 & G_1 \\ \mathbf{0} & G_0 \end{bmatrix} \in \mathbb{F}_q^{2k \times 2n}$$

Partial unit-memory MDP convolutional codes

Let $\mathcal{C}$ be a convolutional code with generator matrix $G(z) = G_0 + G_1 z$.

- $\mathcal{C}$ is called partial unit-memory if $\mathrm{rank}(G_1) < k$. Moreover, a partial unit-memory convolutional code is MDP if and only if all $2k \times 2k$ nontrivial minors of G_1^c are nonzero where

$$G_1^c := \begin{bmatrix} G_0 & G_1 \\ \mathbf{0} & G_0 \end{bmatrix} \in \mathbb{F}_q^{2k \times 2n}$$

- Fix $G_0 \in \mathbb{F}_q^{k \times n}$ to be any MDS matrix and let $G_1 = (X \ \mathbf{0}_{k \times k})$, where X is a $k \times (n-k)$ matrix whose entries are variables over $\mathbb{F}_q$.
- Let $I \cup J$ denote the columns of G_1^c chosen in the minor. Then

$$M_{I,J}(X) = \left[\begin{array}{c|c|c} (G_0)_I & X' & \mathbf{0} \\ \hline \mathbf{0} & \multicolumn{2}{c}{(G_0)_J} \end{array}\right]$$

where $0 \leq |I| \leq k \leq |J| \leq n$ and $|I \cup J| = 2k$.

New construction of MDP Convolutional codes

We consider $L = 1$ and $k > n-k$, then $\delta = n-k$. Define $X \in \mathbb{F}_{q^d}^{k\times(n-k)}$ given by

$$X = \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \alpha^2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha^{n-k} \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

where $\alpha \in \mathbb{F}_{q^d}$ has minimal polynomial over $\mathbb{F}_q$ of degree d.

New construction of MDP Convolutional codes

We consider $L = 1$ and $k > n-k$, then $\delta = n-k$. Define $X \in \mathbb{F}_{q^d}^{k\times(n-k)}$ given by

$$X = \begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \alpha^2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha^{n-k} \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

where $\alpha \in \mathbb{F}_{q^d}$ has minimal polynomial over $\mathbb{F}_q$ of degree d.

Theorem (–, Lieb, Makkonen, Soto, Sprintson, 2025)

Let $k > n-k = \delta$ and $d = \left\lceil \frac{\delta^2-1}{4} \right\rceil + 1$. Let $G_0 \in \mathbb{F}_q^{k\times n}$ be a superregular (e.g. Cauchy) matrix and $G_1 = (X\ \mathbf{0}_{k\times k}) \in \mathbb{F}_{q^d}^{k\times n}$ with X defined above. Then, all nontrivial minors of

$$G_1^c = \begin{pmatrix} G_0 & G_1 \\ \mathbf{0} & G_0 \end{pmatrix}$$

are nonzero, i.e., we get an (n,k,δ)-MDP code over $\mathbb{F}_{q^d}$.

Improvements in special cases

Let $k \geq n/2$. Consider a generator matrix $G(z) = G_0 + G_1 z$ for a convolutional code where G_0 is a $k \times n$ Vandermonde matrix over $\mathbb{F}_q$ and $G_1 = (X\ \mathbf{0})$ where

$$X = \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & & & \vdots \\ \beta_1 & \ddots & & \vdots \\ \beta_2 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ \beta_{n-k} & \cdots & \beta_2 & \beta_1 \end{bmatrix},$$

is a $k \times (n-k)$ matrix for some $\beta_1, \ldots, \beta_{n-k} \in \mathbb{F}_{q^{n-k}}$.

MDP convolutional codes with $\delta = 2,\ 3$

Theorem (–, Lieb, Makkonen, Soto, Sprintson, 2026)

Let $n - k = \delta$ and $G_0 \in \mathbb{F}_q^{k \times n}$ be a Vandermonde matrix and let $G_1 = [X\ 0_{k \times k}]$ with X as defined above.

- *If $\delta = 2$, choose $\beta_1, \beta_2 \in \mathbb{F}_{q^2}$ to be linearly independent over $\mathbb{F}_q$.*
- *If $\delta = 3$, let $\beta_1 = z$, $\beta_2 = z^2$, $\beta_3 = 1$ where $z \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ such that the minimal polynomial of z has constant coefficient unequal to -1.*

Then, all nontrivial minors of G_1^c are nonzero, i.e., we get an (n, k, δ) MDP convolutional code over $\mathbb{F}_{q^\delta}$.

Comparison with exisitng literature

Let $\mathcal{C}$ be (n, k, δ) MDP convolutional code with generator matrix $G(z) = G_0 + G_1 z$. Note that $\delta = \min\{k, n-k\}$.

Constructions	Field Size
Weighted Reed-Solomon codes[3]	$2^{\log_2(n)\frac{11}{24}(\frac{\delta^3}{k}+\delta k)} \approx n^{\delta^2}$
Construction by Chen[4]	n^{δ}
Construction by Luo et.al.[5]	$(n+k)^{\delta}$
Cauchy Matrix construction	$q^{\frac{\delta^2}{4}} \approx (n+k)^{\frac{\delta^2}{4}}$
Vandermonde's construction	$q^{\delta} \approx n^{\delta}$

Main advantage: Sparsity, structure and reduced complexity

[3] G. Alfarano, D. Napp, A. Neri, V. Requena, Weighted reed–solomon convolutional codes, *Linear and Multilinear Algebra*, **72(5)**, 841–874, 2024.

[4] Z. Chen, A lower bound on the field size of convolutional codes with a maximum distance profile and an improved construction, *IEEE Trans. Inf. Theory*, **70(6)**, 4064–4073, 2023.

[5] G. Luo, X. Cao, M. Ezerman, S. Ling, A construction of maximum distance profile convolutional codes with small alphabet sizes, *IEEE Trans. Inf. Theory*, **69(5)**, 2983-2990, 2023.

Construction of Maximally Recoverable codes

Locally Recoverable Codes (LRCs)

- Each symbol can be recovered using a small repair group.

Locally Recoverable Codes (LRCs)

- Each symbol can be recovered using a small repair group.
- Unequal locality:
  - Different repair groups may have different parameters.

Locally Recoverable Codes (LRCs)

- Each symbol can be recovered using a small repair group.
- Unequal locality:
  - Different repair groups may have different parameters.
- Important in distributed storage systems.

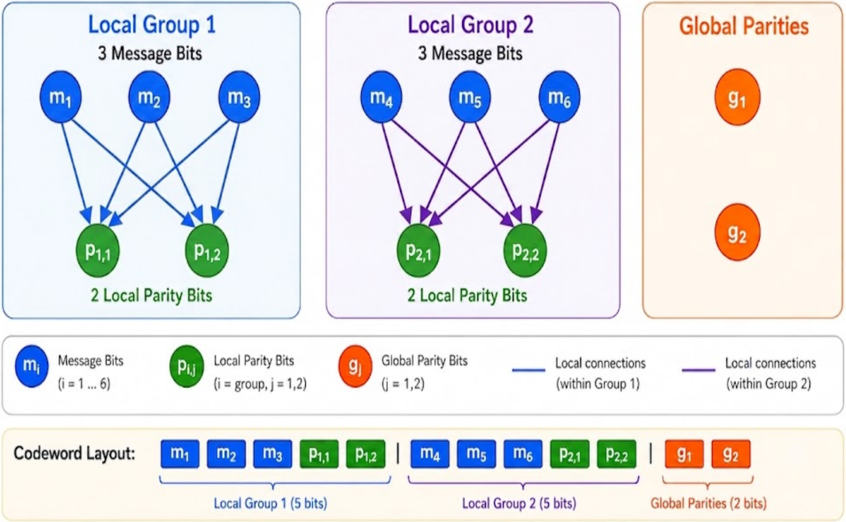
Locally Recoverable Codes (LRCs)

- Each symbol can be recovered using a small repair group.
- Unequal locality:
  - Different repair groups may have different parameters.
- Important in distributed storage systems.

Definition

Let $\mathcal{C}$ be a non-degenerate linear block code of length L. We say that a codeword symbol c_j for $j \in \{1, \ldots, L\}$ has **locality** k_j if there exists a **repair group** $R_j \subset \{1, \ldots, L\}$ such that $j \in R_j$ and $\mathcal{C}|_{R_j}$ forms a $[|R_j|, k_j, \delta_j]$-code; if $\delta_j > 1$ for all j, then we call it a **Locally Recoverable Code with Unequal Locality**.

Example



Local Group 1
3 Message Bits
m_1 m_2 m_3
$p_{1,1}$ $p_{1,2}$
2 Local Parity Bits
Local Group 2
3 Message Bits
m_4 m_5 m_6
$p_{2,1}$ $p_{2,2}$
2 Local Parity Bits
Global Parities
g_1
g_2
m_i Message Bits (i = 1 ... 6)
$p_{i,j}$ Local Parity Bits (i = group, j = 1,2)
g_j Global Parity Bits (j = 1,2)
Local connections (within Group 1)
Local connections (within Group 2)
Codeword Layout:
m_1 m_2 m_3 $p_{1,1}$ $p_{1,2}$ | m_4 m_5 m_6 $p_{2,1}$ $p_{2,2}$ | g_1 g_2
Local Group 1 (5 bits)
Local Group 2 (5 bits)
Global Parities (2 bits)

Maximally Recoverable LRCs

Maximally Recoverable (MR):

- Recover every erasure pattern allowed by locality constraints.

Maximally Recoverable LRCs

Maximally Recoverable (MR):

- Recover every erasure pattern allowed by locality constraints.

Definition

For $\ell, h, n_i, k_i \in \mathbb{N}$ with $n_i \geq k_i$ for $i = 0, \ldots, \ell - 1$, let $\mathcal{C} \subseteq \mathbb{F}_q^N$ be an $\mathbb{F}_q$-linear code of length $N = n_0 + \cdots + n_{\ell-1} + h$ and dimension $K = k_0 + \cdots + k_{\ell-1}$. Set $\mathcal{G}_i := \{1 + \sum_{t=0}^{i-1} n_t, \ldots, \sum_{t=0}^{i} n_t\}$ for $i = 0, \ldots, \ell - 1$. Note that these sets form a partition of $\{1, \ldots, N - h\}$ and $|\mathcal{G}_i| = n_i$. We say that $\mathcal{C}$ is **MR-LRC with UL** if

1. $\dim(\mathcal{C}|_{\mathcal{G}_i}) \leq k_i$, i.e., each codeword symbol indexed by $\mathcal{G}_i$ has locality k_i;
2. for each **admissible** puncturing S, i.e., for each puncturing where exactly $n_i - k_i$ coordinates in $\mathcal{G}_i$ are deleted, the punctured code $\mathcal{C}|_S$ is an $[h + K, K]$-MDS code.

The sets $\mathcal{G}_i$ are called **local repair groups** and the last h coordinates of a codeword are called the **global parities**.

MR-LRCs with Unequal Locality

Parameters:

$$N = \sum_{i=0}^{\ell-1} n_i + h, \qquad K = \sum_{i=0}^{\ell-1} k_i$$

- Repair groups G_i of size n_i
- Locality k_i
- h global parity symbols

Requirement:

- Every admissible puncturing yields an $[K+h, K]$ MDS code.

Generator Matrix Construction for MR-LRCs

Consider

$$G = \begin{bmatrix} G_0 & 0 & \cdots & 0 & P_0 \\ 0 & G_1 & \cdots & 0 & P_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & G_{\ell-1} & P_{\ell-1} \end{bmatrix}$$

- G_i are Cauchy matrices over base field.
- P_i contain extension field elements.

Generator Matrix Construction for MR-LRCs

Consider

$$G = \begin{bmatrix} G_0 & 0 & \cdots & 0 & P_0 \\ 0 & G_1 & \cdots & 0 & P_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & G_{\ell-1} & P_{\ell-1} \end{bmatrix}$$

- G_i are Cauchy matrices over base field.
- P_i contain extension field elements.

Choose:

$$P_i = \begin{bmatrix} \mathrm{Diag}(1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(h-1)i}) \\ 0 \end{bmatrix}$$

Generator Matrix Construction for MR-LRCs

Consider

$$G = \begin{bmatrix} G_0 & 0 & \cdots & 0 & P_0 \\ 0 & G_1 & \cdots & 0 & P_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & G_{\ell-1} & P_{\ell-1} \end{bmatrix}$$

- G_i are Cauchy matrices over base field.
- P_i contain extension field elements.

Choose:

$$P_i = \begin{bmatrix} \mathrm{Diag}(1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(h-1)i}) \\ 0 \end{bmatrix}$$

Key observation:

- Sparse and structured construction.
- Every determinant becomes a polynomial in α.
- Control the degree spread to ensure non-vanishing.

Main Result

Theorem ($-$, Lieb, Soto, Sprintson, 2026)

Let $h \leq \min\{k_i,\ 0 \leq i \leq \ell - 1\}$ and let $G_i \in \mathbb{F}_q^{k_i \times n_i}$, for $i = 0, \ldots, \ell - 1$, be Cauchy matrices and

$$P_i := \begin{bmatrix} \mathrm{Diag}(\alpha^0, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(h-1)i}) \\ \mathbf{0}_{(k_i - h) \times h} \end{bmatrix} \tag{1}$$

for some primitive element $\alpha \in \mathbb{F}_{q^d}$. If $h = 1$ and $d \geq 1$, or if $h > 1$ and

$$d \geq (\ell - 1) \cdot \left\lfloor \frac{h}{2} \right\rfloor \cdot \left\lceil \frac{h}{2} \right\rceil + 1 =: D,$$

then the corresponding code is MR-LRC with UL over $\mathbb{F}_{q^d}$.

Advantages of the Construction

- Sparse generator matrices

Advantages of the Construction

- Sparse generator matrices
- Most entries lie in a smaller subfield

Advantages of the Construction

- Sparse generator matrices
- Most entries lie in a smaller subfield
- Efficient updates
  - If some message symbol needs to be updated, one only has to update the corresponding local group and exactly one global parity symbol.

Advantages of the Construction

- Sparse generator matrices
- Most entries lie in a smaller subfield
- Efficient updates
  - If some message symbol needs to be updated, one only has to update the corresponding local group and exactly one global parity symbol.
- Lower encoding complexity

Advantages of the Construction

- Sparse generator matrices
- Most entries lie in a smaller subfield
- Efficient updates
  - If some message symbol needs to be updated, one only has to update the corresponding local group and exactly one global parity symbol.
- Lower encoding complexity

Theorem (–, Lieb, Soto, Sprintson, 2026)

The encoding complexity for our construction is $O\left(\sum_{i=0}^{\ell-1} n_i \log^2 n_i\right)$.

Similarities and Differences

Similarities and Differences

Similarities

- The generator matrix for MRC Construction for $\ell = 2$ can be seen as the generator matrix for MDP code with $G(z) = G_0 + G_1 z$.
- Built using Cauchy matrices over base field and diagonal structures over extension field elements.
- Comparable encoding complexity

Similarities and Differences

Similarities

- The generator matrix for MRC Construction for $\ell = 2$ can be seen as the generator matrix for MDP code with $G(z) = G_0 + G_1 z$.
- Built using Cauchy matrices over base field and diagonal structures over extension field elements.
- Comparable encoding complexity

Differences

- Completely different codes and independent constructions
- Different algorithms for decoding (ongoing work)

Similarities and Differences

Similarities

- The generator matrix for MRC Construction for $\ell = 2$ can be seen as the generator matrix for MDP code with $G(z) = G_0 + G_1 z$.
- Built using Cauchy matrices over base field and diagonal structures over extension field elements.
- Comparable encoding complexity

Differences

- Completely different codes and independent constructions
- Different algorithms for decoding (ongoing work)

What's next?

Understanding if convolutional codes can be viewed as locally recoverable codes using hierarchical locality.

References

[1] Sakshi Dang, Julia Lieb, Pedro Soto, and Alex Sprintson, Design of MDP Convolutional Codes and Maximally Recoverable Codes Through the Lens of Matrix Completion, arXiv:2604.21544.

[2] Sakshi Dang, Julia Lieb, Okko Makkonen, Pedro Soto and Alex Sprintson A Matrix Completion Approach for the Construction of MDP Convolutional Codes, *2025 IEEE Information Theory Workshop*, 710–715, https://doi.org/10.1109/ITW62417.2025.11240400.

References

[1] Sakshi Dang, Julia Lieb, Pedro Soto, and Alex Sprintson, Design of MDP Convolutional Codes and Maximally Recoverable Codes Through the Lens of Matrix Completion, arXiv:2604.21544.

[2] Sakshi Dang, Julia Lieb, Okko Makkonen, Pedro Soto and Alex Sprintson A Matrix Completion Approach for the Construction of MDP Convolutional Codes, *2025 IEEE Information Theory Workshop*, 710–715, https://doi.org/10.1109/ITW62417.2025.11240400.

Thank You!