On Linear Field Size Access-Optimal MDS Convertible Codes

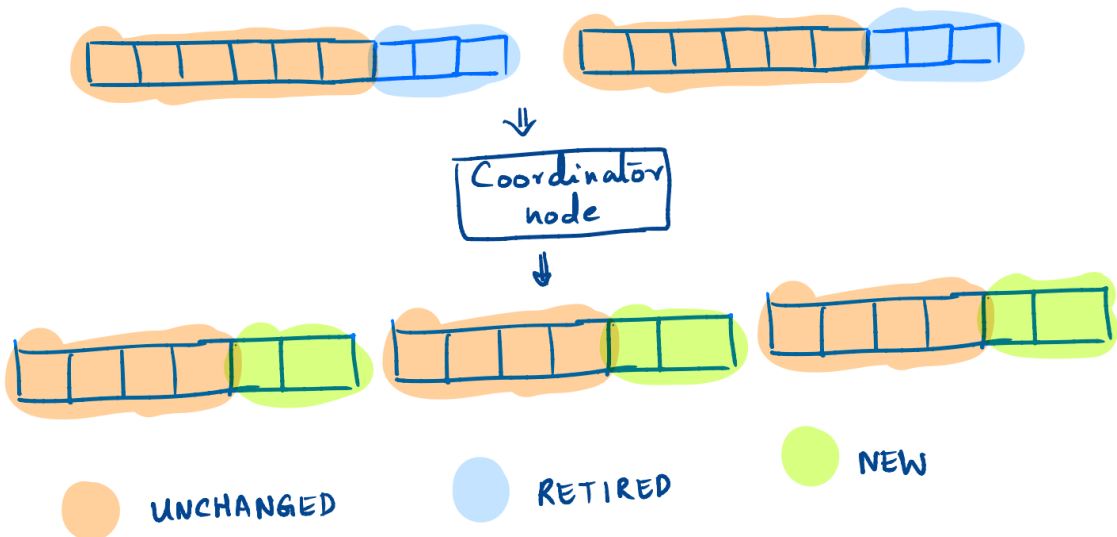
M. Nikhil Krishnan [†] Myna Vajha [‡] Vinayak Ramkumar[◇]
G. Yeswanth Sai [†] Xiangliang Kong [*]

[†] IIT Palakkad, [‡]IIT Hyderabad, [◇]TU Munich, [*]Tel Aviv University

IEEE ISIT 2025, June 25

Convertible Codes: Framework

- Convertible codes a framework introduced by Maturana and Rashmi [TIT 2022] to study the code conversion.
- Goal: To be able to effectively change from any $[n^I = k^I + r^I, k^I]$ initial code to a $[n^F = k^F + r^F, k^F]$ final code.
  - For $M = \text{lcm}(k^I, k^F)$, $\lambda^I = \frac{M}{k^I}$ initial codewords get converted to $\lambda^F = \frac{M}{k^F}$ final codewords. Number of message symbols across initial and final codewords is M.



$$k^I = 6, k^F = 4, M = 12, \lambda^I = 2, \lambda^F = 3, r^I = 3, r^F = 2$$

- Two parameter regimes:
  - merge regime: $k^F = \lambda^I k^I$
  - split regime: $k^I = \lambda^F k^F$

MDS Convertible Codes: Access cost

- MDS convertible codes are convertible codes where the initial and final codes are Maximum Distance Separable (MDS) codes.
- Access cost: number of symbols read from initial codewords to construct the final codewords plus the number of symbols written.
- We will focus on merge regime where $k^F = \lambda k^I$.
  - default approach: download λk^I symbols to construct the parity symbols of the final code.
  - Tight lower bound on access cost (Maturana and Rashmi, TIT 22)

$$\text{access cost} \geq \begin{cases} \lambda r^F + r^F & r^F \leq \min(r^I, k^I) \\ \lambda k^I + r^F & \text{otherwise} \end{cases}$$

  - Assume $r^F \leq \min(r^I, k^I)$ the non-trivial case

MDS Convertible Codes: An Example

- Let $G^I = [I_{k^I} \ P^I], G^F = [I_{k^F} \ P^F]$ be generator matrices of initial and final codes respectively. P^I, P^F are of sizes $k^I \times r^I$ and $\lambda k^I \times r^F$ respectively.
- Example: $k^I = 3, k^F = 6$ and $r^I = r^F = 2$

$$P^I = \begin{bmatrix} 1 & 1 \\ \theta_1 & \theta_2 \\ \theta_1^2 & \theta_2^2 \end{bmatrix}, P^F = \begin{bmatrix} 1 & 1 \\ \theta_1 & \theta_2 \\ \theta_1^2 & \theta_2^2 \\ \theta_1^3 & \theta_2^3 \\ \theta_1^4 & \theta_2^4 \\ \theta_1^5 & \theta_2^5 \end{bmatrix}$$

  - Let p_1^1, p_2^1 and p_1^2, p_2^2 be the parities from two initial codewords.

$$p_1^F = p_1^1 + \theta_1^3 p_1^2$$
$$p_2^F = p_2^1 + \theta_2^3 p_2^2$$

  - Can do conversion in this case by accessing $\lambda r^F = 4 < \lambda k^I = 6$ symbols

Access Optimality from Block-Reconstructable Property

$$P^F = \begin{bmatrix} P^{F,1} \\ P^{F,2} \\ \vdots \\ P_{F,\lambda} \end{bmatrix} \text{ where } P^{F,\ell} \text{ is } k^I \times r^F \text{ matrix.}$$

- P^F is said to be r^F-block reconstructable from P^I if for each $\ell \in [\lambda]$ there exists r^F columns of P^I that span the columns of $P^{F,\ell}$.
- MDS convertible code is access-optimal if P^F is r^F-block reconstructable from P^I
  - r^F final parities can be constructed by accessing exactly λr^I parity symbols.

Per-Symbol Access Optimality

- Recovery of each final parity symbol uses exactly λ initial parities with each parity belonging to an initial codeword.
- P^F is said to be parallel-block reconstructable from P^I if for each $\ell \in [\lambda]$ there exist r^F columns of P^I that are exactly equal to or scaling of columns seen in $P^{F,\ell}$.

parallel-block reconstructable $\rightarrow$ block-reconstructable

- Helps non-central conversion setting where the new node downloads the required data to reconstruct the corresponding final parity.

Literature

- Access optimal code constructions
  - merge regime: lower bounds and matching constructions for all parameters with large field size (Maturana and Rashmi, ITCS 2020), low field size constructions based on Hankel arrays (Maturana and Rashmi, TIT 2022), low field size construction for $r = 3$(ISIT 2024), low-field size polynomial based construction for all parameters (Kong, TIT 2024)
  - split regime and general parameters: lower bounds and matching constructions for all parameters (Maturana, Mukka and Rashmi (ISIT 2020))
- Bandwidth optimal code-conversion: data transmitted in the network during conversion
  - This cost can be smaller than access cost if code symbol is a vector (can transmit parts of it.)
  - merge regime: bounds and matching constructions (Maturana and Rashmi, TIT 2023)
- LRC convertible codes (Maturana and Rashmi, ISIT 2023, Kong TIT 2024)
- Secure Convertible codes (Zhang and Rashmi, ISIT 2025)

Our Contribution

- Two constructions of per-symbol optimal access codes for $\lambda \leq r$
  - Multiplicative sub group based construction
  - Additive sub group based construction
- Access optimal code based on modified-polynomial construction for all parameters with field size $q \geq k^F + r^l$.

Earlier Approaches To Code Construction

1. Vandermonde construction

$$P^I = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_{r^I} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{k^I-1} & \theta_2^{k^I-1} & \cdots & \theta_{r^I}^{k^I-1} \end{bmatrix}, P^F = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_{r^I} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{\lambda k^I-1} & \theta_2^{\lambda k^I-1} & \cdots & \theta_{r^I}^{\lambda k^I-1} \end{bmatrix}$$

   - Need q to be large ($O(2^{(n^F)^3})$) to guarantee that P^F and P^I are super-regular
   - Clear to see parallel-block reconstructable property

2. Hankel matrix based convertible codes
   - Super-regular property guaranteed for sub-matrices of Hankel matrices.
   - Can be constructed with linear field size
   - Constructions limited to parameters $r^F \leq r^I - \lambda + 1$ with linear field size for fixed number of parities

1	3	4	3	10	10	5	9	6	5	10
3	4	3	10	10	5	9	6	5	10	
4	3	10	10	5	9	6	5	10		
3	10	10	5	9	6	5	10			
10	10	5	9	6	5	10				
10	5	9	6	5	10					
5	9	6	5	10						
9	6	5	10							
6	5	10								
5	10									
10										

$k^I = 5,\ \lambda = 2,\ r^F = 2,\ r^I = 4$
Hankel array of size $n^F - 1 = 11$

Our Approach

- P^I and P^F are Cauchy matrices.
- Cauchy matrix $C(X, Y)$ where $X = \{x_1, \cdots, x_k\}$, $Y = \{y_1, \cdots, y_r\}$:

$$C(X,Y) = \begin{bmatrix} \frac{1}{x_1 - y_1} & \frac{1}{x_1 - y_2} & \cdots & \frac{1}{x_1 - y_r} \\ \frac{1}{x_2 - y_1} & \frac{1}{x_2 - y_2} & \cdots & \frac{1}{x_2 - y_r} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{x_k - y_1} & \frac{1}{x_k - y_2} & \cdots & \frac{1}{x_k - y_r} \end{bmatrix}$$

- Cauchy matrices are super-regular.
- Goal: Design X, Y and X_1 of cardinalities k^F, r^I, k^I such that:

$$P^F = C(X, Y) \text{ is parallel-block reconstructable from } P^I = C(X_1, Y)$$

- Enough to look at $r^F = r^I = r$.
- For $r^F \leq r^I$, we do not convert $(r^I - r^F)$ nodes

Sub-Group Based Construction: Using Multiplicative Sub-Group of $\mathbb{F}_q^*$

- Let $\mathbb{F}_q$ be such that $r \mid (q-1)$ and $\nu = \frac{q-1}{r}$, $k' \leq \nu - 1$
- Let α be the primitive element of F_q and $\gamma = \alpha^\nu$.

$$Y = \{\gamma, \gamma^2, \cdots, \gamma^r = 1\}, \quad X_1 = \{\alpha, \alpha^2, \cdots, \alpha^{k'}\}, \quad X_\ell = \gamma^{\ell-1} X_1, X = \cup_{\ell=1}^{\lambda} X_\ell$$

- $X_1, \cdots, X_\lambda, Y$ are disjoint if $\lambda \leq r$
- $P^F = C(X, Y)$ is parallel-block reconstructable from $P' = C(X_1, Y)$

$$\begin{aligned} P^{F,\ell}(i,j) &= \frac{1}{\gamma^{\ell-1}\alpha^i - \gamma^j} = \frac{\gamma^{-(\ell-1)}}{\alpha^i - \gamma^{j-\ell+1}} \\ &= \gamma^{-(\ell-1)} P'(i,j') \end{aligned}$$

where $j' \in [r]$ such that $\gamma^{j'} = \gamma^{j-\ell+1}$.

- j-th column of $P^{F,\ell}$ is scaling of j'-th column of P'

Sub-Group Based Construction: Using Multiplicative Sub-Group of $\mathbb{F}_q^*$

- Modification 1: $\lambda \leq (r-1)$
  - Let $\mathbb{F}_q$ be such that $(r-1) \mid (q-1)$ and $\nu = \frac{q-1}{r-1}$, $k^l \leq \nu - 1$, $\gamma = \alpha^\nu$.

$$Y = \{0, \gamma, \cdots, \gamma^{r-1} = 1\}$$

  - $P^F = C(X, Y)$ is parallel-block reconstructable from $P^l = C(X_1, Y)$
    - ★ $P^{F,\ell}(i,1) = \frac{1}{\gamma^{\ell-1}\alpha^i} = \gamma^{-(\ell-1)} P^l(i,1)$
- Modification 2: $\lambda \leq (r-2)$
  - Append an all-one column to Cauchy matrix is still super-regular matrix (Roth and G. Seroussi, TIT 85)
  - $\mathbb{F}_q$ be such that $(r-2) \mid (q-1)$ and $\nu = \frac{q-1}{r-2}$, $k^l \leq \nu - 1$, $\gamma = \alpha^\nu$.

$$Y = \{0, \gamma, \cdots, \gamma^{r-2} = 1\},$$

  - $P^F = \left[\begin{array}{cc} \underline{1} & C(X, Y) \end{array}\right]$ is parallel-block reconstructable from $P^l = \left[\begin{array}{cc} \underline{1} & C(X_1, Y) \end{array}\right]$

Sub-Group Based Construction: Using Multiplicative Sub-Group of $\mathbb{F}_q^*$

- $r^I = r^F = 4, k^I = 5, \lambda = 2 \implies k^F = 10, n^F = 14$
- Let $q = 13$ (meets the MDS conjecture $q = n^F - 1$)

$$Y = \{2^6 = 11, 2^{12} = 1, 0\}, X_1 = \{2, 2^2, 2^3, 2^4, 2^5\},$$
$$X_2 = \{2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}\}$$

- If $\lambda = r - 2$ and $(r-2) \mid (q-1)$ for $q = (k^I + 1)(r-2) + 1 = n^F - 1$, then MDS conjecture is met.

$$P^I = \begin{bmatrix} 1 & 9 & 7 & 1 \\ 9 & 8 & 10 & 1 \\ 2 & 3 & 5 & 1 \\ 7 & 10 & 9 & 1 \\ 8 & 2 & 11 & 1 \\ 4 & 12 & 6 & 1 \\ 5 & 4 & 3 & 1 \\ 10 & 11 & 8 & 1 \\ 3 & 6 & 4 & 1 \\ 11 & 5 & 2 & 1 \end{bmatrix}$$

Sub-Group Based Construction: Additive Sub-Group of $\mathbb{F}_q$

- Let $q = p^m$ then $\mathbb{F}_q$ is isomorphic to $\{f(x) \in \mathbb{F}_p[x] \mid \deg(f(x)) < m\}$
- $r = p^u$ i.e., $r \mid q$ and $\nu = \frac{q}{r} = p^{m-u}$

$$\begin{aligned} Y &= \{f(x) \in \mathbb{F}_p[x] \mid \deg(f(x)) < u\} = \{y_1(x), \cdots, y_r(x)\} \\ X_1 &= \{f_1(x), \cdots, f_k(x)\} \\ &\subseteq \{x^u f(x) \mid f(x) \in \mathbb{F}_p[x], \deg(f(x)) < m-u-1\} \\ X_\ell &= y_\ell(x) + X_1 \end{aligned}$$

- $P^F = C(X, Y)$ is parallel-block reconstructable from $P^I = C(X_1, Y)$

$$\begin{aligned} P^{F,\ell}(i,j) &= \frac{1}{y_\ell(x) + f_i(x) - y_j(x)} = \frac{1}{f_i(x) - y_{j'}(x)} \\ &= P^I(i,j') \end{aligned}$$

  where $j' \in [r]$ such that $y_{j'}(x) = y_j(x) - y_\ell(x)$.
  - j-th column of $P^{F,\ell}$ is same as j'-th column of P^I
- Can similarly modify to add all one column.

Modified-Polynomial Construction

- Polynomial based construction (Kong, TIT 24)
  - Assumes initial code and final codes to be Reed Solomon (RS) codes defined through evaluation sets $X_1 \cup Y$ and $X \cup Y$ respectively
  - If X_ℓ is of form $X_\ell = \gamma X_1$ then as long as X_is and Y are disjoint, the resultant convertible code is access optimal
- Modified polynomial code
  - We provide an assignment for sets X_ℓ, Y such that any finite field $\mathbb{F}_q$ with $q \geq k^F + r^l$ is enough for code construction.

Conclusions and Open Questions

- Provide two constructions of per-symbol access optimal MDS convertible codes for $\lambda \leq r$ based on multiplicative and additive sub-groups of a finite field.
  - The modification 2 results in convertible codes that achieve the MDS conjecture of $q = n^F - 1$ when $(r-2) \mid (q-1)$
- Simple modification to polynomial code to reduce the field size requirement to $q \geq k^F + r^I$.
  - Can we make this meet MDS conjecture ?