Decoding Algorithms for Rank Metric Reed–Muller Codes

Rakhi Pratihar
joint works with Alain Couvreur (Inria & LIX, École Polytechnique)

OpeRa 2026

Bordeaux, February 27, 2026

Université de Rennes

IRMAR

Decoding Problem in Rank Metric

$$\begin{array}{c}\mathbb{L}\\ \Big|\Big| \\ \mathbb{K}\end{array} \quad \mathrm{G} \stackrel{\text{def}}{=} \mathrm{Gal}(\mathbb{L}/\mathbb{K})$$

$\mathbb{L}$ a finite Galois extension over an arbitrary field $\mathbb{K}$ with $[\mathbb{L}\colon \mathbb{K}] = m$.

Decoding Problem in Rank Metric

$$\begin{array}{c}\mathbb{L}\\ \Big|\\ \Big|\\ \mathbb{K}\end{array} \quad \mathrm{G} \stackrel{\text{def}}{=} \mathrm{Gal}(\mathbb{L}/\mathbb{K})$$

$\mathbb{L}$ a finite Galois extension over an arbitrary field $\mathbb{K}$ with $[\mathbb{L}\colon \mathbb{K}] = m$.

The Bounded Distance Decoding Problem in Rank Metric:

Data. A rank metric code $\mathscr{C} \subseteq \mathbb{K}^{m\times n}$, a matrix $Y \in \mathbb{K}^{m\times n}$ and an integer $t \leqslant \lfloor \frac{d-1}{2} \rfloor$,

Goal. Find (if exists) $C \in \mathscr{C}$ such that $d(C, Y) = t$

Decoding Problem in Rank Metric

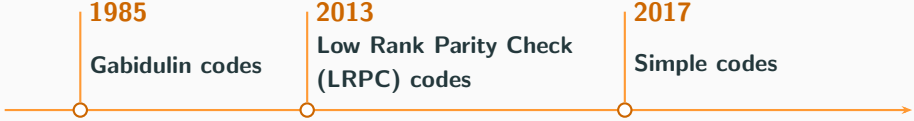
$$\begin{array}{c}\mathbb{L}\\ \Big|\\ \Big|\ \mathrm{G} \stackrel{\text{def}}{=} \mathrm{Gal}(\mathbb{L}/\mathbb{K})\\ \Big|\\ \mathbb{K}\end{array}$$

$\mathbb{L}$ a finite Galois extension over an arbitrary field $\mathbb{K}$ with $[\mathbb{L}\colon \mathbb{K}] = m$.

The Bounded Distance Decoding Problem in Rank Metric:

Data. A rank metric code $\mathscr{C} \subseteq \mathbb{K}^{m\times n}$, a matrix $Y \in \mathbb{K}^{m\times n}$ and an integer $t \leqslant \lfloor \frac{d-1}{2} \rfloor$,

Goal. Find (if exists) $C \in \mathscr{C}$ such that $d(C, Y) = t$



Rank Metric Reed–Muller Codes

$$\begin{array}{c} \mathbb{L} \\ \Big| \Big) \, \mathrm{G} \\ \mathbb{K} \end{array}$$

$\boldsymbol{\theta} = (\theta_1, \ldots, \theta_m)$ a canonical system of generators of $\mathrm{G} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$.

$\boldsymbol{\theta}^{\boldsymbol{i}} = \theta_1^{i_1} \circ \cdots \circ \theta_m^{i_m} \in G$ for $\boldsymbol{i} = (i_1, \cdots, i_m) \in \mathbb{N}^m$, $|\boldsymbol{i}| = i_1 + \ldots + i_m$.

$\boldsymbol{n} := (n_1, \ldots, n_m)$, $\Lambda(\boldsymbol{n}) := [n_1] \times \cdots \times [n_m]$ with $[t] := \{0, 1, \cdots, t-1\}$

A $\boldsymbol{\theta}$-polynomial $P = \sum_{\boldsymbol{i} \in \Lambda(\boldsymbol{n})} a_{\boldsymbol{i}} \boldsymbol{\theta}^{\boldsymbol{i}} \in \mathbb{L}[\mathrm{G}]$: $\deg_{\boldsymbol{\theta}}(P) := \max\{|\boldsymbol{i}| \mid \boldsymbol{i} \in \Lambda(\boldsymbol{n}), a_{\boldsymbol{i}} \neq 0\}$.

Rank Metric Reed–Muller Codes

$$\begin{array}{c}\mathbb{L}\\ \Big|\\ \Big|\mathrm{G}\\ \Big|\\ \mathbb{K}\end{array}$$

$\boldsymbol{\theta} = (\theta_1, \ldots, \theta_m)$ a canonical system of generators of $\mathrm{G} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$.

$\boldsymbol{\theta}^{\boldsymbol{i}} = \theta_1^{i_1} \circ \cdots \circ \theta_m^{i_m} \in G$ for $\boldsymbol{i} = (i_1, \cdots, i_m) \in \mathbb{N}^m$, $|\boldsymbol{i}| = i_1 + \ldots + i_m$.

$\boldsymbol{n} := (n_1, \ldots, n_m)$, $\Lambda(\boldsymbol{n}) := [n_1] \times \cdots \times [n_m]$ with $[t] := \{0, 1, \cdots, t-1\}$

A $\boldsymbol{\theta}$-polynomial $P = \sum_{\boldsymbol{i} \in \Lambda(\boldsymbol{n})} a_{\boldsymbol{i}} \boldsymbol{\theta}^{\boldsymbol{i}} \in \mathbb{L}[\mathrm{G}]$: $\deg_{\boldsymbol{\theta}}(P) := \max\{|\boldsymbol{i}| \mid \boldsymbol{i} \in \Lambda(\boldsymbol{n}), a_{\boldsymbol{i}} \neq 0\}$.

Rank metric Reed–Muller code of order r and type $\boldsymbol{n}$ [ACLN21]

$$\mathsf{RM}_{\boldsymbol{\theta}}(r, \boldsymbol{n}) \stackrel{\text{def}}{=} \{P \in \mathbb{L}[\mathrm{G}] \mid \deg_{\boldsymbol{\theta}}(P) \leqslant r\} \subseteq \mathbb{L}[\mathrm{G}].$$

[ACLN21] Augot, D., Couvreur, A., Lavauzelle, J. and Neri, A., Rank-metric codes over arbitrary Galois extensions and rank analogues of Reed–Muller codes, SIAM Journal of Applied Algebra and Geometry, 2021

G-Dickson Matrices

G-Dickson matrix of $A \in \mathbb{L}[\mathbf{G}]$

$\mathrm{D}_{\mathrm{G}}(A)$ is the matrix representation of the $\mathbb{L}$–linear map in an ordered basis $\{\mathrm{g}_0, \ldots, \mathrm{g}_{m-1}\}$

$$\begin{array}{ccc} \mathbb{L}[\mathrm{G}] & \longrightarrow & \mathsf{End}_{\mathbb{L}}(\mathbb{L}[\mathrm{G}]) \\ A & \longmapsto & (B \mapsto B \circ A) \end{array} .$$

G-Dickson Matrices

G-Dickson matrix of $A \in \mathbb{L}[\mathrm{G}]$

$\mathrm{D}_{\mathrm{G}}(A)$ is the matrix representation of the $\mathbb{L}$–linear map in an ordered basis $\{\mathrm{g}_0, \ldots, \mathrm{g}_{m-1}\}$

$$\begin{array}{ccc} \mathbb{L}[\mathrm{G}] & \longrightarrow & \mathrm{End}_{\mathbb{L}}(\mathbb{L}[\mathrm{G}]) \\ A & \longmapsto & (B \mapsto B \circ A) \end{array} .$$

$\mathrm{Rk}_{\mathbb{K}}(A) = \mathrm{Rk}_{\mathbb{L}}(D_{\mathrm{G}}(A))$ and $A = \sum_{i=0}^{m-1} a_i \mathrm{g}_i \in \mathbb{L}[\mathrm{G}] \quad \Longrightarrow \quad \mathrm{D}_{\mathrm{G}}(A) \stackrel{\text{def}}{=} \left(\mathrm{g}_j \left(a_{\sigma_j^{-1}(i)} \right) \right)$

where $\sigma_j \in \mathfrak{S}_m$ such that $\sigma_j(i) = k$ if $\mathrm{g}_j \mathrm{g}_i = \mathrm{g}_k$ for $i \in \{0, \ldots, m-1\}$.

G-Dickson Matrices

G-Dickson matrix of $A \in \mathbb{L}[\mathrm{G}]$

$\mathrm{D}_{\mathrm{G}}(A)$ is the matrix representation of the $\mathbb{L}$–linear map in an ordered basis $\{\mathrm{g}_0, \ldots, \mathrm{g}_{m-1}\}$

$$\begin{array}{ccc} \mathbb{L}[\mathrm{G}] & \longrightarrow & \mathrm{End}_{\mathbb{L}}(\mathbb{L}[\mathrm{G}]) \\ A & \longmapsto & (B \mapsto B \circ A) \end{array}.$$

$$\mathrm{Rk}_{\mathbb{K}}(A) = \mathrm{Rk}_{\mathbb{L}}(D_{\mathrm{G}}(A)) \quad \text{and} \quad A = \sum_{i=0}^{m-1} a_i \mathrm{g}_i \in \mathbb{L}[\mathrm{G}] \quad \Longrightarrow \quad \mathrm{D}_{\mathrm{G}}(A) \stackrel{\text{def}}{=} \left(\mathrm{g}_j \left(a_{\sigma_j^{-1}(i)} \right) \right)$$

where $\sigma_j \in \mathfrak{S}_m$ such that $\sigma_j(i) = k$ if $\mathrm{g}_j \mathrm{g}_i = \mathrm{g}_k$ for $i \in \{0, \ldots, m-1\}$.

$$D_{\mathrm{G}}(A) = \begin{pmatrix} a_0 & a_6^q & a_5^{q^2} & a_4^{q^3} & a_3^{q^4} & a_2^{q^5} & a_1^{q^6} \\ a_1 & a_0^q & a_6^{q^2} & a_5^{q^3} & a_4^{q^4} & a_3^{q^5} & a_2^{q^6} \\ a_2 & a_1^q & a_0^{q^2} & a_6^{q^3} & a_5^{q^4} & a_4^{q^5} & a_3^{q^6} \\ a_3 & a_2^q & a_1^{q^2} & a_0^{q^3} & a_6^{q^4} & a_5^{q^5} & a_4^{q^6} \\ a_4 & a_3^q & a_2^{q^2} & a_1^{q^3} & a_0^{q^4} & a_6^{q^5} & a_5^{q^6} \\ a_5 & a_4^q & a_3^{q^2} & a_2^{q^3} & a_1^{q^4} & a_0^{q^5} & a_6^{q^6} \\ a_6 & a_5^q & a_4^{q^2} & a_3^{q^3} & a_2^{q^4} & a_1^{q^5} & a_0^{q^6} \end{pmatrix}$$

$A = a_0 X + a_1 X^q + \cdots + a_6 X^{q^6} \in \mathbb{F}_{q^7}[G]$.

$\mathrm{G} = \mathrm{Gal}(\mathbb{F}_{q^7}/\mathbb{F}_q)$ with the ordered basis $\{\mathrm{g}_j = \theta^j : j = 0, \ldots, 6\}$, θ the Frobenius map.

The Decoding Strategy

$$Y = \sum_{\mathrm{g}\in\mathrm{G}} y_{\mathrm{g}}\mathrm{g}, \quad C = \sum_{\mathrm{g}\in\mathrm{G}} c_{\mathrm{g}}\mathrm{g}, \quad E = \sum_{\mathrm{g}\in\mathrm{G}} e_{\mathrm{g}}\mathrm{g} \quad \text{and} \quad \mathsf{Rk}(E) = t, \quad \mathsf{D}_{\mathrm{G}}(Y) = \mathsf{D}_{\mathrm{G}}(C) + \mathsf{D}_{\mathrm{G}}(E)$$

The Decoding Strategy

$$Y = \sum_{\mathrm{g}\in\mathrm{G}} y_{\mathrm{g}}\mathrm{g}, \quad C = \sum_{\mathrm{g}\in\mathrm{G}} c_{\mathrm{g}}\mathrm{g}, \quad E = \sum_{\mathrm{g}\in\mathrm{G}} e_{\mathrm{g}}\mathrm{g} \quad \text{and} \quad \mathsf{Rk}(E) = t, \quad \mathsf{D}_{\mathrm{G}}(Y) = \mathsf{D}_{\mathrm{G}}(C) + \mathsf{D}_{\mathrm{G}}(E)$$

- $\mathbf{D_G}(E)$ **is partially known**: For any g of $\boldsymbol{\theta}$–degree $> r$, e_{g} is known.

The Decoding Strategy

$$Y = \sum_{\mathrm{g}\in\mathrm{G}} y_{\mathrm{g}}\mathrm{g}, \quad C = \sum_{\mathrm{g}\in\mathrm{G}} c_{\mathrm{g}}\mathrm{g}, \quad E = \sum_{\mathrm{g}\in\mathrm{G}} e_{\mathrm{g}}\mathrm{g} \quad \text{and} \quad \mathsf{Rk}(E) = t, \quad \mathsf{D}_{\mathrm{G}}(Y) = \mathsf{D}_{\mathrm{G}}(C) + \mathsf{D}_{\mathrm{G}}(E)$$

- $\mathbf{D_G}(E)$ **is partially known**: For any g of $\boldsymbol{\theta}$–degree $> r$, e_{g} is known.
- The strategy is to find submatrices of the G-Dickson matrix $\mathsf{D}_{\mathrm{G}}(E)$ that contain only one unknown entry denoted as x such that the row containing x can be written as a linear combination of the rest of the rows.

$$\begin{pmatrix} (*) & \dots & x \\ (*) & \dots & (*) \\ & \ddots & \\ (*) & \dots & (*) \end{pmatrix}.$$

A First Example: Decoding Gabidulin Codes

The Gabidulin code $\mathcal{G}_{m,k} \subseteq \mathbb{F}_{q^7}[\theta]$: $m = 7$, $k = 3$, $d = 5$.

A First Example: Decoding Gabidulin Codes

The Gabidulin code $\mathcal{G}_{m,k} \subseteq \mathbb{F}_{q^7}[\theta]$: $m = 7$, $k = 3$, $d = 5$.

- Sent $\quad C = c_0 X + c_1 X^q + c_2 X^{q^2} \qquad \deg_q(C) < 3$
- Received $Y = C + E, \qquad$ where $\qquad \mathsf{Rank}(E) = \lfloor \frac{d-1}{2} \rfloor = 2.$

$$\mathsf{D}_{\mathrm{G}}(Y) = \underbrace{\begin{pmatrix} c_0 & 0 & 0 & 0 & 0 & c_2^{q^5} & c_1^{q^6} \\ c_1 & c_0^q & 0 & 0 & 0 & 0 & c_2^{q^6} \\ c_2 & c_1^q & c_0^{q^2} & 0 & 0 & 0 & 0 \\ 0 & c_2^q & c_1^{q^2} & c_0^{q^3} & 0 & 0 & 0 \\ 0 & 0 & c_2^{q^2} & c_1^{q^3} & c_0^{q^4} & 0 & 0 \\ 0 & 0 & 0 & c_2^{q^3} & c_1^{q^4} & c_0^{q^5} & 0 \\ 0 & 0 & 0 & 0 & c_2^{q^4} & c_1^{q^5} & c_0^{q^6} \end{pmatrix}}_{\mathsf{D}_{\mathrm{G}}(C)} + \underbrace{\begin{pmatrix} e_0 & e_6^q & e_5^{q^2} & e_4^{q^3} & e_3^{q^4} & e_2^{q^5} & e_1^{q^6} \\ e_1 & e_0^q & e_6^{q^2} & e_5^{q^3} & e_4^{q^4} & e_3^{q^5} & e_2^{q^6} \\ e_2 & e_1^q & e_0^{q^2} & e_6^{q^3} & e_5^{q^4} & e_4^{q^5} & e_3^{q^6} \\ e_3 & e_2^q & e_1^{q^2} & e_0^{q^3} & e_6^{q^4} & e_5^{q^5} & e_4^{q^6} \\ e_4 & e_3^q & e_2^{q^2} & e_1^{q^3} & e_0^{q^4} & e_6^{q^5} & e_5^{q^6} \\ e_5 & e_4^q & e_3^{q^2} & e_2^{q^3} & e_1^{q^4} & e_0^{q^5} & e_6^{q^6} \\ e_6 & e_5^q & e_4^{q^2} & e_3^{q^3} & e_2^{q^4} & e_1^{q^5} & e_0^{q^6} \end{pmatrix}}_{\mathsf{D}_{\mathrm{G}}(E)}.$$

The Known and the Unknown Coefficients of E

We know Y and hence, also $D_{\mathrm{G}}(Y)$.

The coefficients e_i for $3 \leqslant i \leqslant 6$ of $E = \sum_{i=0}^{6} e_i X^{q^i}$ are known (in green).

$$\underbrace{\begin{pmatrix} e_0 & e_6^q & e_5^{q^2} & e_4^{q^3} & e_3^{q^4} & e_2^{q^5} & e_1^{q^6} \\ e_1 & e_0^q & e_6^{q^2} & e_5^{q^3} & e_4^{q^4} & e_3^{q^5} & e_2^{q^6} \\ e_2 & e_1^q & e_0^{q^2} & e_6^{q^3} & e_5^{q^4} & e_4^{q^5} & e_3^{q^6} \\ e_3 & e_2^q & e_1^{q^2} & e_0^{q^3} & e_6^{q^4} & e_5^{q^5} & e_4^{q^6} \\ e_4 & e_3^q & e_2^{q^2} & e_1^{q^3} & e_0^{q^4} & e_6^{q^5} & e_5^{q^6} \\ e_5 & e_4^q & e_3^{q^2} & e_2^{q^3} & e_1^{q^4} & e_0^{q^5} & e_6^{q^6} \\ e_6 & e_5^q & e_4^{q^2} & e_3^{q^3} & e_2^{q^4} & e_1^{q^5} & e_0^{q^6} \end{pmatrix}}_{\mathrm{D_G}(E)}.$$

Next we recover the unknown coefficients e_2, e_1, e_0.

Recovering e_2

If $\mathbf{G}$ is cyclic

For an element $E = \sum_{\mathrm{g} \in \mathrm{G}} e_{\mathrm{g}} \mathrm{g} \in \mathbb{L}[\mathrm{G}]$ of rank t, any $t \times t$ submatrix consists of consecutive rows and columns of $\mathrm{D}_{\mathrm{G}}(E)$ is invertible.

Recovering e_2

If G is cyclic

For an element $E = \sum_{\mathrm{g} \in \mathrm{G}} e_{\mathrm{g}} \mathrm{g} \in \mathbb{L}[\mathrm{G}]$ of rank t, any $t \times t$ submatrix consists of consecutive rows and columns of $\mathsf{D}_{\mathrm{G}}(E)$ is invertible.

$$\begin{pmatrix}
e_0 & e_6^q & e_5^{q^2} & e_4^{q^3} & e_3^{q^4} & e_2^{q^5} & e_1^{q^6} \\
e_1 & e_0^q & e_6^{q^2} & e_5^{q^3} & e_4^{q^4} & e_3^{q^5} & e_2^{q^6} \\
e_2 & e_1^q & e_0^{q^2} & e_6^{q^3} & e_5^{q^4} & e_4^{q^5} & e_3^{q^6} \\
e_3 & e_2^q & e_1^{q^2} & e_0^{q^3} & e_6^{q^4} & e_5^{q^5} & e_4^{q^6} \\
e_4 & e_3^q & e_2^{q^2} & e_1^{q^3} & e_0^{q^4} & e_6^{q^5} & e_5^{q^6} \\
e_5 & e_4^q & e_3^{q^2} & e_2^{q^3} & e_1^{q^4} & e_0^{q^5} & e_6^{q^6} \\
e_6 & e_5^q & e_4^{q^2} & e_3^{q^3} & e_2^{q^4} & e_1^{q^5} & e_0^{q^6}
\end{pmatrix}$$

Since $\mathrm{Rk}(D_{\mathrm{G}}(E)) = 2$

$$\det \begin{bmatrix} e_4 & e_3^q & e_2^{q^2} \\ e_5 & e_4^q & e_3^{q^2} \\ e_6 & e_5^q & e_4^{q^2} \end{bmatrix} = 0$$

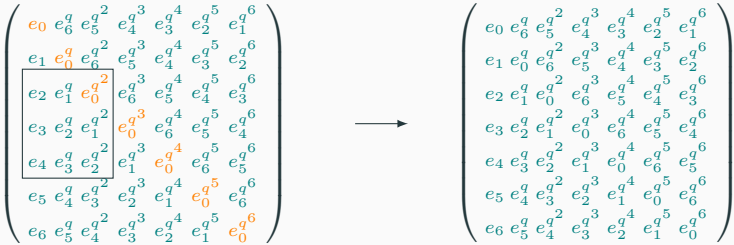
We found e_2!

Now we look for e_1

$$\begin{pmatrix}
e_0 & e_6^q & e_5^{q^2} & e_4^{q^3} & e_3^{q^4} & e_2^{q^5} & e_1^{q^6} \\
e_1 & e_0^q & e_6^{q^2} & e_5^{q^3} & e_4^{q^4} & e_3^{q^5} & e_2^{q^6} \\
e_2 & e_1^q & e_0^{q^2} & e_6^{q^3} & e_5^{q^4} & e_4^{q^5} & e_3^{q^6} \\
e_3 & e_2^q & e_1^{q^2} & e_0^{q^3} & e_6^{q^4} & e_5^{q^5} & e_4^{q^6} \\
e_4 & e_3^q & e_2^{q^2} & e_1^{q^3} & e_0^{q^4} & e_6^{q^5} & e_5^{q^6} \\
e_5 & e_4^q & e_3^{q^2} & e_2^{q^3} & e_1^{q^4} & e_0^{q^5} & e_6^{q^6} \\
e_6 & e_5^q & e_4^{q^2} & e_3^{q^3} & e_2^{q^4} & e_1^{q^5} & e_0^{q^6}
\end{pmatrix}$$

We get e_1!

Finding e_0



Here we get e_0 and $\mathrm{D}_{\mathrm{G}}(E)$!

Next example: $\mathbf{RM}_{\boldsymbol{\theta}}(r, \boldsymbol{n})$: $r = 1$, $\boldsymbol{n} = (3, 3)$, $d = 6$

- Sent: $C = c_0^0\theta_1^0\theta_2^0 + c_1^0\theta_1^1\theta_2^0 + c_0^1\theta_1^0\theta_2^1$
- Received: $Y = C + E$, where $E = \sum_{i,j=0}^{2} e_i^j \theta_1^i \theta_2^j$ with $\mathsf{Rank}(E) = 2 = \lfloor \frac{d-1}{2} \rfloor$.

Next example: $\mathbf{RM}_{\boldsymbol{\theta}}(r, \boldsymbol{n})$: $r = 1$, $\boldsymbol{n} = (3, 3)$, $d = 6$

- Sent: $C = c_0^0\theta_1^0\theta_2^0 + c_1^0\theta_1^1\theta_2^0 + c_0^1\theta_1^0\theta_2^1$
- Received: $Y = C + E$, where $E = \sum_{i,j=0}^{2} e_i^j \theta_1^i \theta_2^j$ with $\mathrm{Rank}(E) = 2 = \lfloor \frac{d-1}{2} \rfloor$.
- **The reverse lexicographic ordering on** G: $\mathrm{g}_0 = \theta_1^0\,\theta_2^0$, $\mathrm{g}_1 = \theta_1^1\,\theta_2^0$, $\mathrm{g}_2 = \theta_1^2\,\theta_2^0$, $\mathrm{g}_3 = \theta_1^0\,\theta_2^1$, $\mathrm{g}_4 = \theta_1^1\,\theta_2^1$, $\mathrm{g}_5 = \theta_1^2\,\theta_2^1$, $\mathrm{g}_6 = \theta_1^0\,\theta_2^2$, $\mathrm{g}_7 = \theta_1^1\,\theta_2^2$, $\mathrm{g}_8 = \theta_1^2\,\theta_2^2$.

Next example: $\mathbf{RM}_{\boldsymbol{\theta}}(r, \boldsymbol{n})$: $r = 1$, $\boldsymbol{n} = (3, 3)$, $d = 6$

- Sent: $C = c_0^0 \theta_1^0 \theta_2^0 + c_1^0 \theta_1^1 \theta_2^0 + c_0^1 \theta_1^0 \theta_2^1$
- Received: $Y = C + E$, where $E = \sum_{i,j=0}^{2} e_i^j \theta_1^i \theta_2^j$ with $\mathrm{Rank}(E) = 2 = \lfloor \frac{d-1}{2} \rfloor$.
- **The reverse lexicographic ordering on** G: $\mathrm{g}_0 = \theta_1^0\,\theta_2^0$, $\mathrm{g}_1 = \theta_1^1\,\theta_2^0$, $\mathrm{g}_2 = \theta_1^2\,\theta_2^0$, $\mathrm{g}_3 = \theta_1^0\,\theta_2^1$, $\mathrm{g}_4 = \theta_1^1\,\theta_2^1$, $\mathrm{g}_5 = \theta_1^2\,\theta_2^1$, $\mathrm{g}_6 = \theta_1^0\,\theta_2^2$, $\mathrm{g}_7 = \theta_1^1\,\theta_2^2$, $\mathrm{g}_8 = \theta_1^2\,\theta_2^2$.

$D_{\mathrm{G}}(E) =$

e_0^0	$\mathrm{g}_1(e_2^0)$	$\mathrm{g}_2(e_1^0)$	$\mathrm{g}_3(e_0^2)$	$\mathrm{g}_4(e_2^2)$	$\mathrm{g}_5(e_1^2)$	$\mathrm{g}_6(e_0^1)$	$\mathrm{g}_7(e_2^1)$	$\mathrm{g}_8(e_1^1)$
e_1^0	$\mathrm{g}_1(e_0^0)$	$\mathrm{g}_2(e_2^0)$	$\mathrm{g}_3(e_1^2)$	$\mathrm{g}_4(e_0^2)$	$\mathrm{g}_5(e_2^2)$	$\mathrm{g}_6(e_1^1)$	$\mathrm{g}_7(e_0^1)$	$\mathrm{g}_8(e_2^1)$
e_2^0	$\mathrm{g}_1(e_1^0)$	$\mathrm{g}_2(e_0^0)$	$\mathrm{g}_3(e_2^2)$	$\mathrm{g}_4(e_1^2)$	$\mathrm{g}_5(e_0^2)$	$\mathrm{g}_6(e_2^1)$	$\mathrm{g}_7(e_1^1)$	$\mathrm{g}_8(e_0^1)$
e_0^1	$\mathrm{g}_1(e_2^1)$	$\mathrm{g}_2(e_1^1)$	$\mathrm{g}_3(e_0^0)$	$\mathrm{g}_4(e_2^0)$	$\mathrm{g}_5(e_1^0)$	$\mathrm{g}_6(e_0^2)$	$\mathrm{g}_7(e_2^2)$	$\mathrm{g}_8(e_1^2)$
e_1^1	$\mathrm{g}_1(e_0^1)$	$\mathrm{g}_2(e_2^1)$	$\mathrm{g}_3(e_1^0)$	$\mathrm{g}_4(e_0^0)$	$\mathrm{g}_5(e_2^0)$	$\mathrm{g}_6(e_1^2)$	$\mathrm{g}_7(e_0^2)$	$\mathrm{g}_8(e_2^2)$
e_2^1	$\mathrm{g}_1(e_1^1)$	$\mathrm{g}_2(e_0^1)$	$\mathrm{g}_3(e_2^0)$	$\mathrm{g}_4(e_1^0)$	$\mathrm{g}_5(e_0^0)$	$\mathrm{g}_6(e_2^2)$	$\mathrm{g}_7(e_1^2)$	$\mathrm{g}_8(e_0^2)$
e_0^2	$\mathrm{g}_1(e_2^2)$	$\mathrm{g}_2(e_1^2)$	$\mathrm{g}_3(e_0^1)$	$\mathrm{g}_4(e_2^1)$	$\mathrm{g}_5(e_1^1)$	$\mathrm{g}_6(e_0^0)$	$\mathrm{g}_7(e_2^0)$	$\mathrm{g}_8(e_1^0)$
e_1^2	$\mathrm{g}_1(e_0^2)$	$\mathrm{g}_2(e_2^2)$	$\mathrm{g}_3(e_1^1)$	$\mathrm{g}_4(e_0^1)$	$\mathrm{g}_5(e_2^1)$	$\mathrm{g}_6(e_1^0)$	$\mathrm{g}_7(e_0^0)$	$\mathrm{g}_8(e_2^0)$
e_2^2	$\mathrm{g}_1(e_1^2)$	$\mathrm{g}_2(e_0^2)$	$\mathrm{g}_3(e_2^1)$	$\mathrm{g}_4(e_1^1)$	$\mathrm{g}_5(e_0^1)$	$\mathrm{g}_6(e_2^0)$	$\mathrm{g}_7(e_1^0)$	$\mathrm{g}_8(e_0^0)$

Can we mimic the minor cancellation method?

$$\begin{pmatrix}
f_0^0 & \mathrm{g}_1(f_2^0) & \mathrm{g}_2(f_1^0) & \mathrm{g}_3(f_0^2) & \mathrm{g}_4(f_2^2) & \mathrm{g}_5(f_1^2) & \mathrm{g}_6(f_0^1) & \mathrm{g}_7(f_2^1) & \mathrm{g}_8(f_1^1) \\
f_1^0 & \mathrm{g}_1(f_0^0) & \mathrm{g}_2(f_2^0) & \mathrm{g}_3(f_1^2) & \mathrm{g}_4(f_0^2) & \mathrm{g}_5(f_2^2) & \mathrm{g}_6(f_1^1) & \mathrm{g}_7(f_0^1) & \mathrm{g}_8(f_2^1) \\
f_2^0 & \mathrm{g}_1(f_1^0) & \mathrm{g}_2(f_0^0) & \mathrm{g}_3(f_2^2) & \mathrm{g}_4(f_1^2) & \mathrm{g}_5(f_0^2) & \mathrm{g}_6(f_2^1) & \mathrm{g}_7(f_1^1) & \mathrm{g}_8(f_0^1) \\
f_0^1 & \mathrm{g}_1(f_2^1) & \mathrm{g}_2(f_1^1) & \mathrm{g}_3(f_0^0) & \mathrm{g}_4(f_2^0) & \mathrm{g}_5(f_1^0) & \mathrm{g}_6(f_0^2) & \mathrm{g}_7(f_2^2) & \mathrm{g}_8(f_1^2) \\
f_1^1 & \mathrm{g}_1(f_0^1) & \mathrm{g}_2(f_2^1) & \mathrm{g}_3(f_1^0) & \mathrm{g}_4(f_0^0) & \mathrm{g}_5(f_2^0) & \mathrm{g}_6(f_1^2) & \mathrm{g}_7(f_0^2) & \mathrm{g}_8(f_2^2) \\
f_2^1 & \mathrm{g}_1(f_1^1) & \mathrm{g}_2(f_0^1) & \mathrm{g}_3(f_2^0) & \mathrm{g}_4(f_1^0) & \mathrm{g}_5(f_0^0) & \mathrm{g}_6(f_2^2) & \mathrm{g}_7(f_1^2) & \mathrm{g}_8(f_0^2) \\
f_0^2 & \mathrm{g}_1(f_2^2) & \mathrm{g}_2(f_1^2) & \mathrm{g}_3(f_0^1) & \mathrm{g}_4(f_2^1) & \mathrm{g}_5(f_1^1) & \mathrm{g}_6(f_0^0) & \mathrm{g}_7(f_2^0) & \mathrm{g}_8(f_1^0) \\
f_1^2 & \mathrm{g}_1(f_0^2) & \mathrm{g}_2(f_2^2) & \mathrm{g}_3(f_1^1) & \mathrm{g}_4(f_0^1) & \mathrm{g}_5(f_2^1) & \mathrm{g}_6(f_1^0) & \mathrm{g}_7(f_0^0) & \mathrm{g}_8(f_2^0) \\
f_2^2 & \mathrm{g}_1(f_1^2) & \mathrm{g}_2(f_0^2) & \mathrm{g}_3(f_2^1) & \mathrm{g}_4(f_1^1) & \mathrm{g}_5(f_0^1) & \mathrm{g}_6(f_2^0) & \mathrm{g}_7(f_1^0) & \mathrm{g}_8(f_0^0)
\end{pmatrix}$$

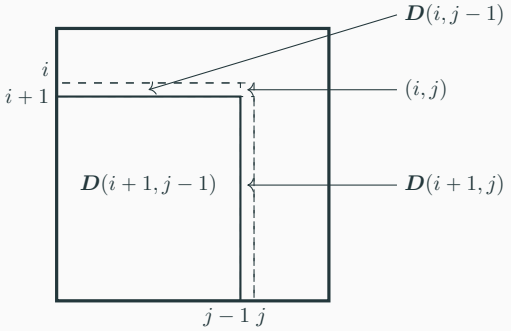
Recovering the unknowns by minor cancellation of Dickson matrix does not work.

Reason: For a rank t G-Dickson matrix over arbitrary Abelian groups, the submatrices consist of t consecutive rows and columns may not be linearly invertible.

Recovering θ-polynomial via Majority Voting

Voting for $e_{\mathbf{far}}$

Let $\boldsymbol{D} \in \mathbb{L}^{N \times N}$ be a matrix. $\boldsymbol{D}(i,j) \stackrel{\text{def}}{=} \{\boldsymbol{D}_{i',j'} \ : \ i \leqslant i' \leqslant N-1 \text{ and } 0 \leqslant j' \leqslant j\}$.

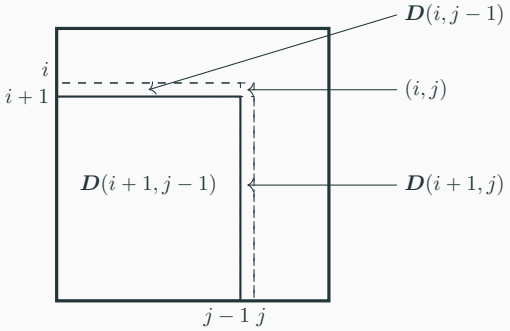


For a position (i,j), if

- $\boldsymbol{D}_{i,j}$ is a conjugate of e_{far};
- $\boldsymbol{D}(i+1,j)$, $\boldsymbol{D}(i,j-1)$ and $\boldsymbol{D}(i+1,j-1)$ have the same rank,

Voting for $e_{\mathbf{far}}$

Let $\boldsymbol{D} \in \mathbb{L}^{N \times N}$ be a matrix. $\boldsymbol{D}(i,j) \stackrel{\text{def}}{=} \{\boldsymbol{D}_{i',j'} \ : \ i \leqslant i' \leqslant N-1 \text{ and } 0 \leqslant j' \leqslant j\}$.



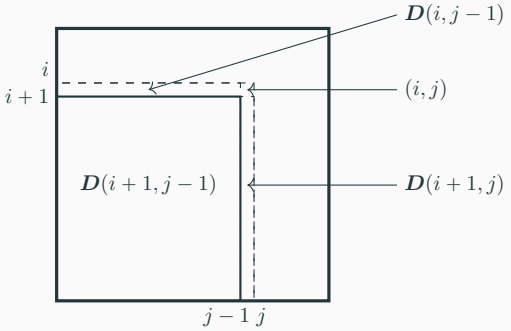
For a position (i,j), if

- $\boldsymbol{D}_{i,j}$ is a conjugate of e_{far};
- $\boldsymbol{D}(i+1,j)$, $\boldsymbol{D}(i,j-1)$ and $\boldsymbol{D}(i+1,j-1)$ have the same rank,

we compute the unique value $d'_{i,j}$ for $\boldsymbol{D}_{i,j}$ such that $\mathsf{Rk}\boldsymbol{D}(i,j) = \mathsf{Rk}\boldsymbol{D}(i+1,j-1)$.

Voting for $e_{\mathbf{far}}$

Let $\boldsymbol{D} \in \mathbb{L}^{N\times N}$ be a matrix. $\boldsymbol{D}(i,j) \stackrel{\text{def}}{=} \{\boldsymbol{D}_{i',j'} \ : \ i \leqslant i' \leqslant N-1 \text{ and } 0 \leqslant j' \leqslant j\}$.



For a position (i,j), if

- $\boldsymbol{D}_{i,j}$ is a conjugate of e_{far};
- $\boldsymbol{D}(i+1,j)$, $\boldsymbol{D}(i,j-1)$ and $\boldsymbol{D}(i+1,j-1)$ have the same rank,

we compute the unique value $d'_{i,j}$ for $\boldsymbol{D}_{i,j}$ such that $\mathsf{Rk}\boldsymbol{D}(i,j) = \mathsf{Rk}\boldsymbol{D}(i+1,j-1)$.

Voting for $e_{\mathbf{far}}$. We compute $\mathsf{g}_j^{-1}(d'_{i,j})$ which is a *predicted value* for e_{far}.

Majority votes for the true value of the unknown

When e_{far} is the farthest unknown in the decoding process

- the number of conjugates of e_{far} appearing on the diagonal Δ_{far} is at least d.

Majority votes for the true value of the unknown

When e_{far} is the farthest unknown in the decoding process

- the number of conjugates of e_{far} appearing on the diagonal Δ_{far} is at least d.
- any entry of $\boldsymbol{D}_{\mathrm{G}}(E)$ lying below the diagonal Δ_{far} is known.

Majority votes for the true value of the unknown

When e_{far} is the farthest unknown in the decoding process

- the number of conjugates of e_{far} appearing on the diagonal Δ_{far} is at least d.
- any entry of $\boldsymbol{D}_{\mathrm{G}}(E)$ lying below the diagonal Δ_{far} is known.

Two situations may occur:

- either the prediction for e_{far} was true;
- or the prediction was false, which implies the corresponding position (i, j) is a pivot position $(= \mathsf{Rk}(D_{\mathrm{G}}(E)) \leqslant \lfloor \frac{d-1}{2} \rfloor)$.

Majority votes for the true value of the unknown

When e_{far} is the farthest unknown in the decoding process

- the number of conjugates of e_{far} appearing on the diagonal Δ_{far} is at least d.
- any entry of $\boldsymbol{D}_{\mathrm{G}}(E)$ lying below the diagonal Δ_{far} is known.

Two situations may occur:

- either the prediction for e_{far} was true;
- or the prediction was false, which implies the corresponding position (i, j) is a pivot position $(= \mathsf{Rk}(D_{\mathrm{G}}(E)) \leqslant \lfloor \frac{d-1}{2} \rfloor)$.

There cannot be "too many" wrong predictions

Let T be the number of true predictions for e_{far} and F be the number of false ones, then

$$T > F.$$

Complexity

Theorem [Couvreur, P., 2025]

- Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of degree N with Galois group G with a system of generators $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_m)$.
- Let $\mathbf{n} = (n_1, \ldots, n_m)$ denotes the sequence of orders of θ_i's in G.
- Suppose $r \leqslant \sum_{i=1}^{m}(n_i - 1)$ and d denote the minimum distance of the code $\mathsf{RM}_{\boldsymbol{\theta}}(r, \mathbf{n})$.

If we are given a primitive element x of $\mathbb{L}/\mathbb{K}$, then the majority voting algorithm corrects any error pattern of weight $t \leqslant \frac{d-1}{2}$ in $\widetilde{\mathcal{O}}(N^4)$, more precisely, $\mathcal{O}(tN^3 \log(N) \log\log(N) + kN^3)$ operations in $\mathbb{K}$.

Couvreur, A., and Pratihar, R., Decoding Rank Metric Reed–Muller Codes, IEEE Transactions on Information Theory, 2025.

Complexity

Theorem [Couvreur, P., 2025]

- Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of degree N with Galois group G with a system of generators $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_m)$.
- Let $\mathbf{n} = (n_1, \ldots, n_m)$ denotes the sequence of orders of θ_i's in G.
- Suppose $r \leqslant \sum_{i=1}^{m}(n_i - 1)$ and d denote the minimum distance of the code $\mathsf{RM}_{\boldsymbol{\theta}}(r, \mathbf{n})$.

If we are given a primitive element x of $\mathbb{L}/\mathbb{K}$, then the majority voting algorithm corrects any error pattern of weight $t \leqslant \frac{d-1}{2}$ in $\widetilde{\mathcal{O}}(N^4)$, more precisely, $\mathcal{O}(tN^3 \log(N) \log\log(N) + kN^3)$ operations in $\mathbb{K}$.

Couvreur, A., and Pratihar, R., Decoding Rank Metric Reed–Muller Codes, IEEE Transactions on Information Theory, 2025.

Høholdt, T., and Pellikaan, R., On the Decoding of Algebraic-Geometric Codes, IEEE Transactions on Information Theory, 2002.

Recursive Decoding of Binary Rank Metric RM Codes, i.e., $\mathrm{G} \cong (\mathbb{Z}/2\mathbb{Z})^m$

Binary RM codes in rank metric

A binary rank metric Reed–Muller code of length $N = 2^m$ over $\mathbb{L}/\mathbb{K}$ of order r and type m:

$$\mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r, m) \stackrel{\text{def}}{=} \left\{ f \in \mathbb{L}[\mathrm{G}] \ : \ f = \sum_{\mathrm{g} \in \mathrm{G},\ \mathrm{w_H(g)} \leqslant r} f_{\mathrm{g}} \mathrm{g} \right\},$$

$\mathrm{w_H(g)}$ is the Hamming weight of the g seen as a vector in $(\mathbb{Z}/2\mathbb{Z})^m$.

Recursive Decoding of Binary Rank Metric RM Codes, i.e., $\mathrm{G} \cong (\mathbb{Z}/2\mathbb{Z})^m$

Binary RM codes in rank metric

A binary rank metric Reed–Muller code of length $N = 2^m$ over $\mathbb{L}/\mathbb{K}$ of order r and type m:

$$\mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r, m) \stackrel{\text{def}}{=} \left\{ f \in \mathbb{L}[\mathrm{G}] \ : \ f = \sum_{\mathrm{g} \in \mathrm{G},\ \mathrm{w_H}(\mathrm{g}) \leqslant r} f_{\mathrm{g}} \mathrm{g} \right\},$$

$\mathrm{w_H}(\mathrm{g})$ is the Hamming weight of the g seen as a vector in $(\mathbb{Z}/2\mathbb{Z})^m$.

A decoding algorithm with improved complexity in

Couvreur, A., and Pratihar, R., Recursive decoding of binary rank Reed-Muller codes and Plotkin construction for matrix codes, arXiv: 2510.19095.

Recursive Decoding of Binary Rank Metric RM Codes, i.e., $\mathrm{G} \cong (\mathbb{Z}/2\mathbb{Z})^m$

Binary RM codes in rank metric

A binary rank metric Reed–Muller code of length $N = 2^m$ over $\mathbb{L}/\mathbb{K}$ of order r and type m:

$$\mathrm{RM}_{\mathbb{L}/\mathbb{K}}(r, m) \stackrel{\text{def}}{=} \left\{ f \in \mathbb{L}[\mathrm{G}] \ : \ f = \sum_{\mathrm{g} \in \mathrm{G},\ \mathrm{w_H}(\mathrm{g}) \leqslant r} f_{\mathrm{g}} \mathrm{g} \right\},$$

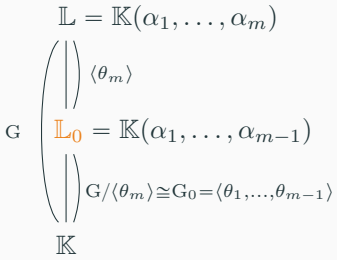
$\mathrm{w_H}(\mathrm{g})$ is the Hamming weight of the g seen as a vector in $(\mathbb{Z}/2\mathbb{Z})^m$.

A decoding algorithm with improved complexity in

Couvreur, A., and Pratihar, R., Recursive decoding of binary rank Reed-Muller codes and Plotkin construction for matrix codes, arXiv: 2510.19095.

Thank You!

The Recursive Structure of Binary Rank Metric Reed–Muller Codes

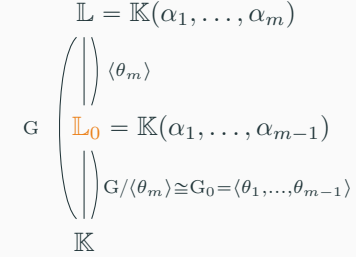


$\mathrm{G} = \mathsf{Gal}(\mathbb{L}/\mathbb{K}) \cong (\mathbb{Z}/2\mathbb{Z})^m = \langle \theta_1, \ldots, \theta_m \rangle$

The minimal polynomial of α_i :

- $X^2 - a_i, \quad a_i \in \mathbb{K}$ when $\mathrm{Char}\,\mathbb{K} \neq 2$
  (the Kummer case),
- $X^2 + X + a_i, \quad a_i \in \mathbb{K}$ when $\mathrm{Char}\,\mathbb{K} = 2$
  (the Artin–Schreier case).

The Recursive Structure of Binary Rank Metric Reed–Muller Codes



$\mathrm{G} = \mathsf{Gal}(\mathbb{L}/\mathbb{K}) \cong (\mathbb{Z}/2\mathbb{Z})^m = \langle \theta_1, \ldots, \theta_m \rangle$

The minimal polynomial of α_i :

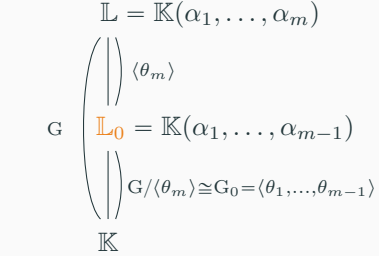
- $X^2 - a_i, \quad a_i \in \mathbb{K}$ when $\mathrm{Char}\,\mathbb{K} \neq 2$ (the Kummer case),
- $X^2 + X + a_i, \quad a_i \in \mathbb{K}$ when $\mathrm{Char}\,\mathbb{K} = 2$ (the Artin–Schreier case).

Proposition [The recursive structure in the Kummer case]

$$\mathsf{RM}_{\mathbb{L}/\mathbb{K}}(r,m) = \left\{ \begin{pmatrix} \boldsymbol{A}_0 + \boldsymbol{B}_0 & a_m(\boldsymbol{A}_1 - \boldsymbol{B}_1) \\ \boldsymbol{A}_1 + \boldsymbol{B}_1 & \boldsymbol{A}_0 - \boldsymbol{B}_0 \end{pmatrix} \; : \; \begin{array}{l} \boldsymbol{A}_i \in \mathsf{RM}_{\mathbb{L}_0/\mathbb{K}}(r, m-1), \\ \boldsymbol{B}_i \in \mathsf{RM}_{\mathbb{L}_0/\mathbb{K}}(r-1, m-1) \end{array} \right\},$$

where $a_m \stackrel{\mathsf{def}}{=} \alpha_m^2 \in \mathbb{K}$.

The Recursive Structure of Binary Rank Metric Reed–Muller Codes



$\mathrm{G} = \mathsf{Gal}(\mathbb{L}/\mathbb{K}) \cong (\mathbb{Z}/2\mathbb{Z})^m = \langle \theta_1, \ldots, \theta_m \rangle$

The minimal polynomial of α_i :

- $X^2 - a_i, \quad a_i \in \mathbb{K}$ when $\mathrm{Char}\,\mathbb{K} \neq 2$ (the Kummer case),
- $X^2 + X + a_i, \quad a_i \in \mathbb{K}$ when $\mathrm{Char}\,\mathbb{K} = 2$ (the Artin–Schreier case).

Proposition [The recursive structure in the Artin–Schreier case]

$$\mathsf{RM}_{\mathbb{L}/\mathbb{K}}(r,m) = \left\{ \begin{pmatrix} \boldsymbol{A}_0 + \boldsymbol{B}_0 & a_m(\boldsymbol{A}_1 + \boldsymbol{B}_1) + \boldsymbol{B}_0 \\ \boldsymbol{A}_1 + \boldsymbol{B}_1 & \boldsymbol{A}_0 + \boldsymbol{A}_1 + \boldsymbol{B}_0 \end{pmatrix} : \begin{array}{l} \boldsymbol{A}_i \in \mathsf{RM}_{\mathbb{L}_0/\mathbb{K}}(r, m-1), \\ \boldsymbol{B}_i \in \mathsf{RM}_{\mathbb{L}_0/\mathbb{K}}(r-1, m-1) \end{array} \right\},$$

where $a_m \stackrel{\mathsf{def}}{=} \alpha_m^2 + \alpha_m \in \mathbb{K}$.

$$\boldsymbol{Y} = \underbrace{\begin{pmatrix} \boldsymbol{A}_0 + \boldsymbol{B}_0 & a_m(\boldsymbol{A}_1 - \boldsymbol{B}_1) \\ \boldsymbol{A}_1 + \boldsymbol{B}_1 & \boldsymbol{A}_0 - \boldsymbol{B}_0 \end{pmatrix}}_{\boldsymbol{C} \in \mathsf{RM}_{\mathbb{L}/\mathbb{K}}(r,m)} + \underbrace{\begin{pmatrix} \boldsymbol{E}_{00} & \boldsymbol{E}_{01} \\ \boldsymbol{E}_{10} & \boldsymbol{E}_{11} \end{pmatrix}}_{\boldsymbol{E} \in \mathbb{K}^{2^m \times 2^m}}, \quad \mathsf{Rk}(\boldsymbol{E}) = t \leqslant 2^{m-r-1} - 1$$

Step 1: Folding $\boldsymbol{Y}$

To get rid of the $\boldsymbol{A}_i$'s without increasing the error rank.

$$\begin{pmatrix} \frac{1}{\alpha_m}\mathbf{I} & \mathbf{I} \end{pmatrix} \boldsymbol{Y} \begin{pmatrix} \mathbf{I} \\ -\frac{1}{\alpha_m}\mathbf{I} \end{pmatrix} = \frac{2}{\alpha_m}\boldsymbol{B}_0 + 2\boldsymbol{B}_1 + \frac{1}{\alpha_m}\boldsymbol{E}_{00} - \frac{1}{\alpha_m}\boldsymbol{E}_{01} + \boldsymbol{E}_{10} - \frac{1}{\alpha_m}\boldsymbol{E}_{11},$$

$$\begin{pmatrix} -\frac{1}{\alpha_m}\boldsymbol{I} & \boldsymbol{I} \end{pmatrix} \boldsymbol{Y} \begin{pmatrix} \boldsymbol{I} \\ \frac{1}{\alpha_m}\boldsymbol{I} \end{pmatrix} = 2\boldsymbol{B}_1 - \frac{2}{\alpha_m}\boldsymbol{B}_0 - \frac{1}{\alpha_m}\boldsymbol{E}_{00} - \frac{1}{\alpha_m}\boldsymbol{E}_{01} + \boldsymbol{E}_{10} + \frac{1}{\alpha_m}\boldsymbol{E}_{11}.$$