Weighted Reed-Solomon Convolutional Codes

Gianira N. Alfarano
Joint work with Diego Napp, Alessandro Neri and Veronica Requena

Zurich
June 7th, 2023

EINDHOVEN UNIVERSITY OF TECHNOLOGY

Contents

Ingredients

- $\mathbb{F}_q$ finite field of q elements, q prime power
- n, k positive integers
- $\mathbb{F}_q[z]$ polynomial ring over $\mathbb{F}_q$

Definition

An $(n, k)_q$ **convolutional code** is a rank k $\mathbb{F}_q[z]$-submodule $\mathcal{C} \subseteq \mathbb{F}_q[z]^n$.

Ingredients

- $\mathbb{F}_q$ finite field of q elements, q prime power
- n, k positive integers
- $\mathbb{F}_q[z]$ polynomial ring over $\mathbb{F}_q$

Definition

An $(n,k)_q$ **convolutional code** is a rank k $\mathbb{F}_q[z]$-submodule $\mathcal{C} \subseteq \mathbb{F}_q[z]^n$.

- $\mathcal{C}$ possesses a **generator matrix** $G(z) \in \mathbb{F}_q[z]^{k\times n}$, such that

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

- the ***i*th row degree** δ_i is the largest degree among the entries in the ith row of $G(z)$.
- the **degree** δ is the highest degree of the $k \times k$ minors of $G(z)$.

Ingredients

- $\mathbb{F}_q$ finite field of q elements, q prime power
- n, k positive integers
- $\mathbb{F}_q[z]$ polynomial ring over $\mathbb{F}_q$

Definition

An $(n, k, \delta)_q$ **convolutional code** is a rank k $\mathbb{F}_q[z]$-submodule $\mathcal{C} \subseteq \mathbb{F}_q[z]^n$.

- $\mathcal{C}$ possesses a **generator matrix** $G(z) \in \mathbb{F}_q[z]^{k \times n}$, such that

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

- the i**th row degree** δ_i is the largest degree among the entries in the ith row of $G(z)$.
- the **degree** δ is the highest degree of the $k \times k$ minors of $G(z)$.

Ingredients

- $\mathbb{F}_q$ finite field of q elements, q prime power
- n, k positive integers
- $\mathbb{F}_q[z]$ polynomial ring over $\mathbb{F}_q$

Definition

An $(n, k, \delta)_q$ **convolutional code** is a rank k $\mathbb{F}_q[z]$-submodule $\mathcal{C} \subseteq \mathbb{F}_q[z]^n$.

- $\mathcal{C}$ possesses a **generator matrix** $G(z) \in \mathbb{F}_q[z]^{k \times n}$, such that

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

- the i**th row degree** δ_i is the largest degree among the entries in the ith row of $G(z)$.
- the **degree** δ is the highest degree of the $k \times k$ minors of $G(z)$.
- $G(z)$ is **reduced** if the sum of its row degrees attains the minimum possible value among the generator matrices (δ is equal to sum of row degrees).
- G(z) is **basic** if its Smith-form is given by $\begin{pmatrix} I_k & 0 \end{pmatrix}$.

Contents

jth Column Distances

Definition

$$d_j^c(\mathcal{C}) := \min\left\{\mathrm{wt}(v_{[0,j]}(z)) = \mathrm{wt}(v_0 + v_1 z + \cdots + v_j z^j) \mid v(z) \in \mathcal{C},\ v_0 \neq 0\right\}$$

Definition

Let

$$G(z) := \sum_{i=0}^{m} G_i z^i.$$

For every $j \in \mathbb{N}_0$ we define the j**-th truncated sliding generator**

$$G_j^c := \begin{bmatrix} G_0 & G_1 & \cdots & G_j \\ & G_0 & \cdots & G_{j-1} \\ & & \ddots & \vdots \\ & & & G_0 \end{bmatrix}$$

MDP Convolutional Codes

- $d_j^c \leq \mathrm{d_{free}}$ for all $j \in \mathbb{N}_0$
- $d_0^c \leq d_1^c \leq d_2^c \leq \dots$
- For every $j \in \mathbb{N}_0$, we have $d_j^c \leq (n-k)(j+1)+1$.
- If $d_j^c = (n-k)(j+1)+1$ for some $j \in \mathbb{N}_0$, then $d_i^c = (n-k)(i+1)+1$ for all $i \leq j$.

Definition

Let $L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$. An $(n,k,\delta)_q$ convolutional code with column distances $d_j^c, j \in \mathbb{N}_0$ is said to have **maximum distance profile** (MDP) if

$$d_j^c = (n-k)(j+1)+1, \text{ for } j = 1, \dots, L.$$

Characterization of MDP Convolutional Codes

Theorem (Gluesing-Luerssen, Rosenthal, Smarandache, '06)

Let $G(z) = \sum_{i=0}^{m} G_i z^i$ be a basic generator matrix of an (n, k, δ) convolutional code $\mathcal{C}$. The following statements are equivalent:

1. $d_L^c(\mathcal{C}) = (n-k)(L+1)+1$.
2. *every $(L+1)k \times (L+1)k$ full-size minor of G_L^c formed by columns with indices $1 \leq t_1 < \cdots < t_{(L+1)k}$, where $t_{sk+1} > sn$ for $s = 1, \ldots, L$, is nonzero .*

H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. "Strongly MDS convolutional codes.", IEEE Transactions on Information Theory, 2006.

$G(z)$ has the **MDP property** if (2) holds.

Characterization of MDP Convolutional Codes

Theorem (Gluesing-Luerssen, Rosenthal, Smarandache, '06)

Let $G(z) = \sum_{i=0}^{m} G_i z^i$ be a basic generator matrix of an (n, k, δ) convolutional code $\mathcal{C}$. The following statements are equivalent:

1. $d_L^c(\mathcal{C}) = (n-k)(L+1) + 1.$
2. *every $(L+1)k \times (L+1)k$ full-size minor of G_L^c formed by columns with indices $1 \leq t_1 < \cdots < t_{(L+1)k}$, where $t_{sk+1} > sn$ for $s = 1, \ldots, L$, is nonzero .*

H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. "Strongly MDS convolutional codes.", IEEE Transactions on Information Theory, 2006.

$G(z)$ has the **MDP property** if (2) holds.

Remark

- It is not necessary to have $G(z)$ basic in order to show that the code generated by $G(z)$ is MDP.
- If $\delta = km$ and $G(z)$ has the MDP property, then the convolutional code generated by $G(z)$ is noncatastrophic and the code is MDP.

G.N. Alfarano and J. Lieb "On the left primeness of some polynomial matrices with applications to convolutional codes.", Journal of Algebra and its Applications, 2020.

Contents

Generalized Reed-Solomon Codes

Definition

Let $n \leq q$ and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ pairwise distinct elements, $b_1, \ldots, b_n \in \mathbb{F}_q^*$. The code

$$C := \{(b_1 f(\alpha_1), \ldots, b_n f(\alpha_n)) \mid f \in \mathbb{F}_q[x]_{<k}\}$$

is called *Generalized Reed-Solomon (GRS) code* and it is denoted by $\mathcal{GRS}_k(\alpha, b)$, where $\alpha := (\alpha_1, \ldots, \alpha_n)$ and $b = (b_1, \ldots, b_n)$.

$$G := \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ b_1\alpha_1 & b_2\alpha_2 & \cdots & b_n\alpha_n \\ b_1\alpha_1^2 & b_2\alpha_2^2 & \cdots & b_n\alpha_n^2 \\ \vdots & \vdots & & \vdots \\ b_1\alpha_1^{k-1} & b_2\alpha_2^{k-1} & \cdots & b_n\alpha_n^{k-1} \end{pmatrix} = V_k(\alpha)\mathrm{diag}(b)$$

Weighted Reed-Solomon Convolutional Codes

- Let $\alpha := (\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_q^*)^n$, α_i's pairwise distinct
- Let γ be root of an irreducible polynomial of **degree** s in $\mathbb{F}_q[z]$

Weighted Reed-Solomon Convolutional Codes

- Let $\alpha := (\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_q^*)^n$, α_i's pairwise distinct
- Let γ be root of an irreducible polynomial of **degree** s in $\mathbb{F}_q[z]$
- For any $0 \leq r \leq m$, let G_r be the following matrix

$$\begin{pmatrix} \gamma^{\frac{r(r+1)}{2}k-r}\alpha_1^{(r+1)k-1} & \gamma^{\frac{r(r+1)}{2}k-r}\alpha_2^{(r+1)k-1} & \cdots & \gamma^{\frac{r(r+1)}{2}k-r}\alpha_n^{(r+1)k-1} \\ \vdots & \vdots & & \vdots \\ \gamma^{\frac{r(r-1)}{2}k+r}\alpha_1^{rk+1} & \gamma^{\frac{r(r-1)}{2}k+r}\alpha_2^{rk+1} & \cdots & \gamma^{\frac{r(r-1)}{2}k+r}\alpha_n^{rk+1} \\ \gamma^{\frac{r(r-1)}{2}k}\alpha_1^{rk} & \gamma^{\frac{r(r-1)}{2}k}\alpha_2^{rk} & \cdots & \gamma^{\frac{r(r-1)}{2}k}\alpha_n^{rk} \end{pmatrix}$$

Weighted Reed-Solomon Convolutional Codes

Remark

- $\mathbb{F}_q(\gamma) \cong \mathbb{F}_{q^s}$

Weighted Reed-Solomon Convolutional Codes

Remark

- $\mathbb{F}_q(\gamma) \cong \mathbb{F}_{q^s}$
- $G_0 \in \mathbb{F}_q^{k \times n}$

Weighted Reed-Solomon Convolutional Codes

Remark

- $\mathbb{F}_q(\gamma) \cong \mathbb{F}_{q^s}$
- $G_0 \in \mathbb{F}_q^{k \times n}$
- $G_i \in \mathbb{F}_{q^s}^{k \times n}$ for every $i = 1, \ldots, m$

Weighted Reed-Solomon Convolutional Codes

Remark

- $\mathbb{F}_q(\gamma) \cong \mathbb{F}_{q^s}$
- $G_0 \in \mathbb{F}_q^{k \times n}$
- $G_i \in \mathbb{F}_{q^s}^{k \times n}$ for every $i = 1, \ldots, m$
- G_i's are all generator matrices of a GRS code

Weighted Reed-Solomon Convolutional Codes

Remark

- $\mathbb{F}_q(\gamma) \cong \mathbb{F}_{q^s}$
- $G_0 \in \mathbb{F}_q^{k \times n}$
- $G_i \in \mathbb{F}_{q^s}^{k \times n}$ for every $i = 1, \ldots, m$
- G_i's are all generator matrices of a GRS code

Definition

A **weighted RS convolutional code** $\mathcal{C}_{k,n}^m(\gamma, \alpha)$ is the code whose generator matrix is $G(z) = \sum_{r=0}^{m} G_r z^r$.

G.N. Alfarano, D. Napp, V. Requena and A. Neri "Weighted Reed-Solomon Convolutional Codes.", Linear and Multilinear Algebra, 2022.

Example: $\mathcal{C}^2_{3,5}$

$k = 3,\ m = 2,\ \delta = 6,\ L = 5.$

$$G_0 = \begin{pmatrix} \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 & \alpha_5^2 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad G_1 = \begin{pmatrix} \gamma^2\alpha_1^5 & \gamma^2\alpha_2^5 & \gamma^2\alpha_3^5 & \gamma^2\alpha_4^5 & \gamma^2\alpha_5^5 \\ \gamma\alpha_1^4 & \gamma\alpha_2^4 & \gamma\alpha_3^4 & \gamma\alpha_4^4 & \gamma\alpha_5^4 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_4^3 & \alpha_5^3 \end{pmatrix}$$

$$G_2 = \begin{pmatrix} \gamma^7\alpha_1^8 & \gamma^7\alpha_2^8 & \gamma^7\alpha_3^8 & \gamma^7\alpha_4^8 & \gamma^7\alpha_5^8 \\ \gamma^5\alpha_1^7 & \gamma^5\alpha_2^7 & \gamma^5\alpha_3^7 & \gamma^5\alpha_4^7 & \gamma^5\alpha_5^7 \\ \gamma^3\alpha_1^6 & \gamma^3\alpha_2^6 & \gamma^3\alpha_3^6 & \gamma^3\alpha_4^6 & \gamma^3\alpha_5^6 \end{pmatrix}$$

Example: $\mathcal{C}^2_{3,5}$

$k = 3,\ m = 2,\ \delta = 6,\ L = 5.$

$$G_0 = \begin{pmatrix} \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \alpha_4^2 & \alpha_5^2 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad G_1 = \begin{pmatrix} \gamma^2\alpha_1^5 & \gamma^2\alpha_2^5 & \gamma^2\alpha_3^5 & \gamma^2\alpha_4^5 & \gamma^2\alpha_5^5 \\ \gamma\alpha_1^4 & \gamma\alpha_2^4 & \gamma\alpha_3^4 & \gamma\alpha_4^4 & \gamma\alpha_5^4 \\ \alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \alpha_4^3 & \alpha_5^3 \end{pmatrix}$$

$$G_2 = \begin{pmatrix} \gamma^7\alpha_1^8 & \gamma^7\alpha_2^8 & \gamma^7\alpha_3^8 & \gamma^7\alpha_4^8 & \gamma^7\alpha_5^8 \\ \gamma^5\alpha_1^7 & \gamma^5\alpha_2^7 & \gamma^5\alpha_3^7 & \gamma^5\alpha_4^7 & \gamma^5\alpha_5^7 \\ \gamma^3\alpha_1^6 & \gamma^3\alpha_2^6 & \gamma^3\alpha_3^6 & \gamma^3\alpha_4^6 & \gamma^3\alpha_5^6 \end{pmatrix}$$

$$G_5^c = \begin{pmatrix} G_0 & G_1 & G_2 & & & \\ & G_0 & G_1 & G_2 & & \\ & & G_0 & G_1 & G_2 & \\ & & & G_0 & G_1 & G_2 \\ & & & & G_0 & G_1 \\ & & & & & G_0 \end{pmatrix}$$

Parameters of $\mathcal{C}^m_{k,n}(\gamma, \alpha)$

Proposition

The code $\mathcal{C}^m_{k,n}(\gamma, \alpha)$ is a $(n, k, km)_{q^s}$ convolutional code.

- $G_0 = M_0$ full rank hence k is the dimension of the code.
- The degree δ is equal to the sum of the row-degrees km.

Corollary

The generator matrix of $\mathcal{C}^m_{k,n}(\gamma, \alpha)$ is reduced.

Parameters of $\mathcal{C}^m_{k,n}(\gamma,\alpha)$

Proposition

The code $\mathcal{C}^m_{k,n}(\gamma,\alpha)$ is a $(n,k,km)_{q^s}$ convolutional code.

- $G_0 = M_0$ full rank hence k is the dimension of the code.
- The degree δ is equal to the sum of the row-degrees km.

Corollary

The generator matrix of $\mathcal{C}^m_{k,n}(\gamma,\alpha)$ is reduced.

Theorem

$\mathcal{C}^m_{k,n}(\gamma,\alpha)$ is an MDP convolutional code in $\mathbb{F}_{q^s}[z]^n$.

Parameters of $\mathcal{C}_{k,n}^{m}(\gamma, \alpha)$

Proposition

The code $\mathcal{C}_{k,n}^{m}(\gamma, \alpha)$ is a $(n, k, km)_{q^s}$ convolutional code.

- $G_0 = M_0$ full rank hence k is the dimension of the code.
- The degree δ is equal to the sum of the row-degrees km.

Corollary

The generator matrix of $\mathcal{C}_{k,n}^{m}(\gamma, \alpha)$ is reduced.

Theorem

$\mathcal{C}_{k,n}^{m}(\gamma, \alpha)$ is an MDP convolutional code in $\mathbb{F}_{q^s}[z]^n$.

Proof.

Difficult! □

Sketch of the Proof

- Let $Y = (y_i)_i$ be a vector of algebraically independent variables
- Let $G(x, Y, \mathrm{B}, \Lambda)$ be an upper triangular block matrix : every block is a generalized Vandermonde matrix $V(\Lambda, Y)$, where each row is multiplied by a suitable power of an another algebraically independent variable x
- B is a vector whose components are the involved powers of x
- Λ is the vector of the exponents involved in the generalized Vandermonde matrices.

$$G(x, Y, \mathrm{B}, \Lambda) := \begin{pmatrix} A_{0,0} & A_{0,1} & \cdots & A_{0,m} \\ & A_{1,1} & \cdots & A_{1,m} \\ & & \ddots & \vdots \\ & & & A_{m,m} \end{pmatrix}$$

Sketch of the Proof

- Let $Y = (y_i)_i$ be a vector of algebraically independent variables
- Let $G(x, Y, \mathrm{B}, \Lambda)$ be an upper triangular block matrix : every block is a generalized Vandermonde matrix $V(\Lambda, Y)$, where each row is multiplied by a suitable power of an another algebraically independent variable x
- B is a vector whose components are the involved powers of x
- Λ is the vector of the exponents involved in the generalized Vandermonde matrices.

$$G(x, Y, \mathrm{B}, \Lambda) := \begin{pmatrix} A_{0,0} & A_{0,1} & \cdots & A_{0,m} \\ & A_{1,1} & \cdots & A_{1,m} \\ & & \ddots & \vdots \\ & & & A_{m,m} \end{pmatrix}$$

$A_{i,j} = A^{\left(\beta^{(i,j)}, \lambda^{(i,j)}\right)} := \mathrm{diag}\left(x^{\beta^{(i,j)}}\right) V\left(\lambda^{(i,j)}, y^{(j)}\right) \in \mathbb{F}[x, Y]^{k_i \times \ell_j}$, where

$$\mathrm{diag}\left(x^{\beta^{(i,j)}}\right) = \begin{pmatrix} x^{\beta_1^{(i,j)}} & 0 & \cdots & 0 \\ 0 & x^{\beta_2^{(i,j)}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x^{\beta_{k_i}^{(i,j)}} \end{pmatrix}.$$

Sketch of the Proof

- Observe that the determinant of the matrix $G(x, Y, \mathrm{B}, \Lambda)$ is a polynomial $p(x, Y)$.

- We show that the monomial of minimal degree in x of p is a polynomial in Y non identically zero.

- $\det G(x, Y, \mathrm{B}, \Lambda) = p(x, Y) = p_0(Y)x^t + p_1(x, Y)x^{t+1}$.

Sketch of the Proof

- Observe that the determinant of the matrix $G(x, Y, \mathrm{B}, \Lambda)$ is a polynomial $p(x, Y)$.
- We show that the monomial of minimal degree in x of p is a polynomial in Y non identically zero.
- $\det G(x, Y, \mathrm{B}, \Lambda) = p(x, Y) = p_0(Y)x^t + p_1(x, Y)x^{t+1}$.

In our construction:

- All the minors we have to check have the shape of $G(\gamma, \alpha, \mathrm{B}, \Lambda)$
- $\det G(\gamma, \alpha, \mathrm{B}, \Lambda) = p(\gamma, \alpha) = p_0(\alpha)\gamma^t + p_1(\gamma, \alpha)\gamma^{t+1}$:
- $p_0(\alpha)$ is given by the product of some determinants of Vandermonde matrices
- γ is such that it is not a zero of $\det G(\gamma, \alpha, \mathrm{B}, \Lambda)$

Example

$$G(x, Y, \mathrm{B}, \Lambda) = \begin{pmatrix} A_{0,0} & A_{0,1} & A_{0,2} \\ & A_{1,1} & A_{1,2} \\ & & A_{2,2} \end{pmatrix} =$$

$$\left(\begin{array}{cc|cccc|cccccc}
y_1^2 & y_2^2 & x^2z_1^6 & x^2z_2^6 & x^2z_3^6 & x^2z_4^6 & x^9w_1^{11} & x^9w_2^{11} & x^9w_3^{11} & x^9w_4^{11} & x^9w_5^{11} & x^9w_6^{11} \\
y_1 & y_2 & xz_1^5 & xz_2^5 & xz_3^5 & xz_4^5 & x^7w_1^{10} & x^7w_2^{10} & x^7w_3^{10} & x^7w_4^{10} & x^7w_5^{10} & x^7w_6^{10} \\
1 & 1 & z_1^4 & z_2^4 & z_3^4 & z_4^4 & x^5w_1^9 & x^5w_2^9 & x^5w_3^9 & x^5w_4^9 & x^5w_5^9 & x^5w_6^9 \\
\hline
 & & z_1^3 & z_2^3 & z_3^3 & z_4^3 & x^3w_1^8 & x^3w_2^8 & x^3w_3^8 & x^3w_4^8 & x^3w_5^8 & x^3w_6^8 \\
 & & z_1^2 & z_2^2 & z_3^2 & z_4^2 & x^2w_1^7 & x^2w_2^7 & x^2w_3^7 & x^2w_4^7 & x^2w_5^7 & x^2w_6^7 \\
 & & z_1 & z_2 & z_3 & z_4 & xw_1^6 & xw_2^6 & xw_3^6 & xw_4^6 & xw_5^6 & xw_6^6 \\
 & & 1 & 1 & 1 & 1 & w_1^5 & w_2^5 & w_3^5 & w_4^5 & w_5^5 & w_6^5 \\
\hline
 & & & & & & w_1^4 & w_2^4 & w_3^4 & w_4^4 & w_5^4 & w_6^4 \\
 & & & & & & w_1^3 & w_2^3 & w_3^3 & w_4^3 & w_5^3 & w_6^3 \\
 & & & & & & w_1^2 & w_2^2 & w_3^2 & w_4^2 & w_5^2 & w_6^2 \\
 & & & & & & w_1 & w_2 & w_3 & w_4 & w_5 & w_6 \\
 & & & & & & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right).$$

Example

$$\begin{pmatrix}
y_1^2 & y_2^2 & x^2z_1^6 & x^2z_2^6 & x^2z_3^6 & x^2z_4^6 & x^9w_1^{11} & x^9w_2^{11} & x^9w_3^{11} & x^9w_4^{11} & x^9w_5^{11} & x^9w_6^{11} \\
y_1 & y_2 & xz_1^5 & xz_2^5 & xz_3^5 & xz_4^5 & x^7w_1^{10} & x^7w_2^{10} & x^7w_3^{10} & x^7w_4^{10} & x^7w_5^{10} & x^7w_6^{10} \\
1 & 1 & z_1^4 & z_2^4 & z_3^4 & z_4^4 & x^5w_1^9 & x^5w_2^9 & x^5w_3^9 & x^5w_4^9 & x^5w_5^9 & x^5w_6^9 \\
 & & z_1^3 & z_2^3 & z_3^3 & z_4^3 & x^3w_1^8 & x^3w_2^8 & x^3w_3^8 & x^3w_4^8 & x^3w_5^8 & x^3w_6^8 \\
 & & z_1^2 & z_2^2 & z_3^2 & z_4^2 & x^2w_1^7 & x^2w_2^7 & x^2w_3^7 & x^2w_4^7 & x^2w_5^7 & x^2w_6^7 \\
 & & z_1 & z_2 & z_3 & z_4 & xw_1^6 & xw_2^6 & xw_3^6 & xw_4^6 & xw_5^6 & xw_6^6 \\
 & & 1 & 1 & 1 & 1 & w_1^5 & w_2^5 & w_3^5 & w_4^5 & w_5^5 & w_6^5 \\
 & & & & & & w_1^4 & w_2^4 & w_3^4 & w_4^4 & w_5^4 & w_6^4 \\
 & & & & & & w_1^3 & w_2^3 & w_3^3 & w_4^3 & w_5^3 & w_6^3 \\
 & & & & & & w_1^2 & w_2^2 & w_3^2 & w_4^2 & w_5^2 & w_6^2 \\
 & & & & & & w_1 & w_2 & w_3 & w_4 & w_5 & w_6 \\
 & & & & & & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

Example

$$
\begin{pmatrix}
y_1^2 & y_2^2 & x^2 z_1^6 & x^2 z_2^6 & x^2 z_3^6 & x^2 z_4^6 & x^9 w_1^{11} & x^9 w_2^{11} & x^9 w_3^{11} & x^9 w_4^{11} & x^9 w_5^{11} & x^9 w_6^{11} \\
y_1 & y_2 & x z_1^5 & x z_2^5 & x z_3^5 & x z_4^5 & x^7 w_1^{10} & x^7 w_2^{10} & x^7 w_3^{10} & x^7 w_4^{10} & x^7 w_5^{10} & x^7 w_6^{10} \\
1 & 1 & z_1^4 & z_2^4 & z_3^4 & z_4^4 & x^5 w_1^9 & x^5 w_2^9 & x^5 w_3^9 & x^5 w_4^9 & x^5 w_5^9 & x^5 w_6^9 \\
 & & z_1^3 & z_2^3 & z_3^3 & z_4^3 & x^3 w_1^8 & x^3 w_2^8 & x^3 w_3^8 & x^3 w_4^8 & x^3 w_5^8 & x^3 w_6^8 \\
 & & z_1^2 & z_2^2 & z_3^2 & z_4^2 & x^2 w_1^7 & x^2 w_2^7 & x^2 w_3^7 & x^2 w_4^7 & x^2 w_5^7 & x^2 w_6^7 \\
 & & z_1 & z_2 & z_3 & z_4 & x w_1^6 & x w_2^6 & x w_3^6 & x w_4^6 & x w_5^6 & x w_6^6 \\
 & & 1 & 1 & 1 & 1 & w_1^5 & w_2^5 & w_3^5 & w_4^5 & w_5^5 & w_6^5 \\
 & & & & & & w_1^4 & w_2^4 & w_3^4 & w_4^4 & w_5^4 & w_6^4 \\
 & & & & & & w_1^3 & w_2^3 & w_3^3 & w_4^3 & w_5^3 & w_6^3 \\
 & & & & & & w_1^2 & w_2^2 & w_3^2 & w_4^2 & w_5^2 & w_6^2 \\
 & & & & & & w_1 & w_2 & w_3 & w_4 & w_5 & w_6 \\
 & & & & & & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
$$

$$
y_1 y_2 z_1 z_2 z_3 z_4 (y_1 - y_2) \prod_{1 \le i < j \le 4} (z_i - z_j) \prod_{1 \le i < j \le 6} (w_i - w_j).
$$

Example

$$
\begin{pmatrix}
y_1^2 & y_2^2 & x^2 z_1^6 & x^2 z_2^6 & x^2 z_3^6 & x^2 z_4^6 & x^9 w_1^{11} & x^9 w_2^{11} & x^9 w_3^{11} & x^9 w_4^{11} & x^9 w_5^{11} & x^9 w_6^{11} \\
y_1 & y_2 & x z_1^5 & x z_2^5 & x z_3^5 & x z_4^5 & x^7 w_1^{10} & x^7 w_2^{10} & x^7 w_3^{10} & x^7 w_4^{10} & x^7 w_5^{10} & x^7 w_6^{10} \\
1 & 1 & z_1^4 & z_2^4 & z_3^4 & z_4^4 & x^5 w_1^9 & x^5 w_2^9 & x^5 w_3^9 & x^5 w_4^9 & x^5 w_5^9 & x^5 w_6^9 \\
 & & z_1^3 & z_2^3 & z_3^3 & z_4^3 & x^3 w_1^8 & x^3 w_2^8 & x^3 w_3^8 & x^3 w_4^8 & x^3 w_5^8 & x^3 w_6^8 \\
 & & z_1^2 & z_2^2 & z_3^2 & z_4^2 & x^2 w_1^7 & x^2 w_2^7 & x^2 w_3^7 & x^2 w_4^7 & x^2 w_5^7 & x^2 w_6^7 \\
 & & z_1 & z_2 & z_3 & z_4 & x w_1^6 & x w_2^6 & x w_3^6 & x w_4^6 & x w_5^6 & x w_6^6 \\
 & & 1 & 1 & 1 & 1 & w_1^5 & w_2^5 & w_3^5 & w_4^5 & w_5^5 & w_6^5 \\
 & & & & & & w_1^4 & w_2^4 & w_3^4 & w_4^4 & w_5^4 & w_6^4 \\
 & & & & & & w_1^3 & w_2^3 & w_3^3 & w_4^3 & w_5^3 & w_6^3 \\
 & & & & & & w_1^2 & w_2^2 & w_3^2 & w_4^2 & w_5^2 & w_6^2 \\
 & & & & & & w_1 & w_2 & w_3 & w_4 & w_5 & w_6 \\
 & & & & & & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
$$

Contents

Field Size Consideration

Let $G := \sum_{r=0}^{m} G_r z^r$, where G_r is

$$\begin{pmatrix} \gamma^{\frac{r(r+1)}{2}k-r}\alpha_1^{(r+1)k-1} & \gamma^{\frac{r(r+1)}{2}k-r}\alpha_2^{(r+1)k-1} & \cdots & \gamma^{\frac{r(r+1)}{2}k-r}\alpha_n^{(r+1)k-1} \\ \vdots & \vdots & & \vdots \\ \gamma^{\frac{r(r-1)}{2}k+r}\alpha_1^{rk+1} & \gamma^{\frac{r(r-1)}{2}k+r}\alpha_2^{rk+1} & \cdots & \gamma^{\frac{r(r-1)}{2}k+r}\alpha_n^{rk+1} \\ \gamma^{\frac{r(r-1)}{2}k}\alpha_1^{rk} & \gamma^{\frac{r(r-1)}{2}k}\alpha_2^{rk} & \cdots & \gamma^{\frac{r(r-1)}{2}k}\alpha_n^{rk} \end{pmatrix}$$

Field Size Consideration

Let $G := \sum_{r=0}^{m} G_r z^r$, where G_r is

$$\begin{pmatrix} \gamma^{\frac{r(r+1)}{2}k-r}\alpha_1^{(r+1)k-1} & \gamma^{\frac{r(r+1)}{2}k-r}\alpha_2^{(r+1)k-1} & \cdots & \gamma^{\frac{r(r+1)}{2}k-r}\alpha_n^{(r+1)k-1} \\ \vdots & \vdots & & \vdots \\ \gamma^{\frac{r(r-1)}{2}k+r}\alpha_1^{rk+1} & \gamma^{\frac{r(r-1)}{2}k+r}\alpha_2^{rk+1} & \cdots & \gamma^{\frac{r(r-1)}{2}k+r}\alpha_n^{rk+1} \\ \gamma^{\frac{r(r-1)}{2}k}\alpha_1^{rk} & \gamma^{\frac{r(r-1)}{2}k}\alpha_2^{rk} & \cdots & \gamma^{\frac{r(r-1)}{2}k}\alpha_n^{rk} \end{pmatrix}$$

Replace γ with an indeterminate x and consider $G_L^c(x)$

$$\mathcal{P}(k,n,m,\alpha) := \{q(x) \in \mathbb{F}_q[x] \mid q(x) \text{ is a full size minor of } G_L^c \text{ formed as stated (2) }\}.$$

Remark

Then $\mathcal{C}_{k,n}^m(\gamma,\alpha)$ is MDP if and only if $q(\gamma) \neq 0$ for every $q(x) \in \mathcal{P}(k,n,m,\alpha)$.

Field Size Consideration

Let $G := \sum_{r=0}^{m} G_r z^r$, where G_r is

$$\begin{pmatrix} \gamma^{\frac{r(r+1)}{2}k-r}\alpha_1^{(r+1)k-1} & \gamma^{\frac{r(r+1)}{2}k-r}\alpha_2^{(r+1)k-1} & \cdots & \gamma^{\frac{r(r+1)}{2}k-r}\alpha_n^{(r+1)k-1} \\ \vdots & \vdots & & \vdots \\ \gamma^{\frac{r(r-1)}{2}k+r}\alpha_1^{rk+1} & \gamma^{\frac{r(r-1)}{2}k+r}\alpha_2^{rk+1} & \cdots & \gamma^{\frac{r(r-1)}{2}k+r}\alpha_n^{rk+1} \\ \gamma^{\frac{r(r-1)}{2}k}\alpha_1^{rk} & \gamma^{\frac{r(r-1)}{2}k}\alpha_2^{rk} & \cdots & \gamma^{\frac{r(r-1)}{2}k}\alpha_n^{rk} \end{pmatrix}$$

Replace γ with an indeterminate x and consider $G_L^c(x)$

$$\mathcal{P}(k,n,m,\alpha) := \{q(x) \in \mathbb{F}_q[x] \mid q(x) \text{ is a full size minor of } G_L^c \text{ formed as stated (2) }\}.$$

Remark

Then $\mathcal{C}_{k,n}^m(\gamma,\alpha)$ is MDP if and only if $q(\gamma) \neq 0$ for every $q(x) \in \mathcal{P}(k,n,m,\alpha)$.

- Let $\nu(q(x)) := \max\{\ell \in \mathbb{N} \mid x^\ell \text{ divides } q(x)\}$
- $D(k,n,m,\alpha) := \max\{\deg q(x) - \nu(q(x)) \mid 0 \neq q(x) \in \mathcal{P}(k,n,m,\alpha)\}$.

Field Size Consideration

Theorem

For any integer $s > D(k, n, m, \alpha)$, $\mathcal{C}^m_{k,n}(\gamma, \alpha)$ *is an MDP convolutional code in* $\mathbb{F}_{q^s}[z]^n$.

Remark

We need to estimate D to determine the field size of our code.

Theorem

For every k, n, m *integers with* $0 < k < n$, *there exists an* $(n, k, km)_{q^s}$ *MDP convolutional code where* $q^s = \mathcal{O}(n^{\frac{(km)^3}{3t}})$, *and* $t = \min\{k, n-k\}$.

Comparison with Known Constructions

$[n, k, \delta]$ L, m, μ, r	ANP	GRS	MAK*	AN*	HST†	L†	$\mathcal{C}^m_{k,n}$	GRS‡
[2, 1, 1] 2, 1, 1, 3	2^8	43	2^5	3	3	55	3	–
[2, 1, 2] 4, 2, 2, 5	2^{32}	434692	2^7	7	11	1261	27	2^3
[3, 2, 2] 3, 1, 2, 8	2^{512}	$5^8 7^8 2^{12} + 1$	2^{11}	31	233	1981	256	2^6
[3, 1, 2] 3, 2, 1, 8	2^{512}	$5^8 7^8 2^{12} + 1$	2^{11}	31	233	3961	16	2^6
[3, 2, 1] 1, 1, 1, 4	2^{32}	$2^4 3^4 + 1$	–	5	5	3	4	2^2
[4, 2, 2] 2, 1, 1, 7	2^{128}	$\sim 10^{12}$	–	17	77	5545	125	2^5
[4, 1, 3] 4, 3, 1, 15	$2^{2^{17}}$	$\sim 7 \cdot 10^{61}$	–	–	1338936	232561	3125	2^{13}
[5, 2, 2] 1, 1, 1, 7	2^{2^9}	$\sim 10^{12}$	–	17	77	35	49	32
[6, 2, 2] 1, 1, 1, 9	$2^{2^{11}}$	$\sim 7 \cdot 10^{20}$	–	59	751	71	49	128
[6, 2, 2] 1, 2, 1, 9	$2^{2^{11}}$	$\sim 7 \cdot 10^{20}$	–	59	751	71	49	128
[7, 2, 2] 1, 1, 1, 11	$2^{2^{13}}$	$\sim 10^{32}$	–	–	8525	126	64	512
[7, 3, 3] 1, 1, 1, 10	$2^{2^{12}}$	$\sim 10^{26}$	–	127	2495	532	512	256

- *: result found by computer search
- †: not constructive
- ‡: based on a conjecture
- – : there are no constructions for such parameters

Contents

Summarizing

- We defined a new family of convolutional codes
- We showed that they are MDP exploiting a more general point of view
- We compare the obtained field size with the existing constructions

Remarks and Future Research

- Recently, for memory 1 combining Vandermonde and Moore matrices a construction of MDP convolutional codes has been obtained.

G. Luo, X. Cao; M.F. Ezerman, S. Ling "A Construction of Maximum Distance Profile Convolutional Codes With Small Alphabet Sizes.", IEEE Transactions on Information Theory, 2023.

- Recently it has been shown that in order to construct an MDP convolutional code we need a field size

$$q \geq \Omega_L(n^{L-1}).$$

Z. Chen "A lower bound on the field size of convolutional codes with a maximum distance profile and an improved construction.", preprint, 2023.

Remarks and Future Research

- Recently, for memory 1 combining Vandermonde and Moore matrices a construction of MDP convolutional codes has been obtained.

G. Luo, X. Cao; M.F. Ezerman, S. Ling "A Construction of Maximum Distance Profile Convolutional Codes With Small Alphabet Sizes.", IEEE Transactions on Information Theory, 2023.

- Recently it has been shown that in order to construct an MDP convolutional code we need a field size

$$q \geq \Omega_L(n^{L-1}).$$

Z. Chen "A lower bound on the field size of convolutional codes with a maximum distance profile and an improved construction.", preprint, 2023.

- Check if this family of codes is closed under duality

- Use the algebraic structure to develop a decoding algorithm

Thank You!