Column rank distances of rank metric convolutional codes

Diego Napp, Raquel Pinto, Filipa Santana
(CIDMA, University of Aveiro)

Joachim Rosenthal
(University of Zurich)

5ICMCTA, August 28-31, 2017, Vihula Manor

Motivation

- Multi-shot network coding $\rightarrow$ rank metric convolutional codes

- Streaming applications $\rightarrow$ column rank distance

Overview

- Convolutional codes
- Rank metric convolutional codes
- Column rank distance
- Strongly-MRD rank metric convolutional codes

Convolutional Codes

Definition

A convolutional code $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]$-submodule of $\mathbb{F}_q^n[D]$ of rank k.

Convolutional Codes

Definition

A convolutional code $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]$-submodule of $\mathbb{F}_q^n[D]$ of rank k.

A matrix $G(D) \in \mathbb{F}_q^{k\times n}[D]$ whose rows form a basis for $\mathcal{C}$ is called an encoder.

$$\mathcal{C} \;=\; \mathrm{Im}_{\mathbb{F}_q[D]} G(D) = \left\{ u(D)G(D) : \; u(D) \in \mathbb{F}_q^k[D] \right\}$$

Convolutional Codes

Definition

A convolutional code $\mathcal{C}$ of rate k/n is an $\mathbb{F}_q[D]$-submodule of $\mathbb{F}_q^n[D]$ of rank k.

A matrix $G(D) \in \mathbb{F}_q^{k\times n}[D]$ whose rows form a basis for $\mathcal{C}$ is called an encoder.

$$\mathcal{C} \;=\; \mathrm{Im}_{\mathbb{F}_q[D]} G(D) = \left\{ u(D)G(D) :\; u(D) \in \mathbb{F}_q^k[D] \right\}$$

Codewords are polynomial vectors

Any other encoder of $\mathcal{C}$ can be obtained by $\tilde{G}(D) = U(D)G(D)$, where $U(D) \in \mathbb{F}_q^{k \times k}[D]$ is unimodular (i.e., it admits an inverse in $\mathbb{F}_q^{k \times k}[D]$).

Any other encoder of $\mathcal{C}$ can be obtained by $\tilde{G}(D) = U(D)G(D)$, where $U(D) \in \mathbb{F}_q^{k\times k}[D]$ is unimodular (i.e., it admits an inverse in $\mathbb{F}_q^{k\times k}[D]$).

An encoder $G(D) \in \mathbb{F}^{k\times n}[D]$ is left prime if

$$G(D) = L(D)\tilde{G}(D),\ L(D) \in \mathbb{F}^{k\times k}[D], \tilde{G}(D) \in \mathbb{F}^{k\times n}[D] \Rightarrow$$

$\Rightarrow L(D)$ unimodular.

If $\mathcal{C}$ admits a left prime encoder then all its encoders are left prime $\rightarrow \mathcal{C}$ is called observable.

Row reduced encoders are the ones that have minimal sum of the row degrees among all encoders of $\mathcal{C}$ $\rightarrow$ degree of $\mathcal{C}$.

If $\mathcal{C}$ has rate k/n and degree δ is said to be an (n, k, δ)-convolutional code.

Rank metric convolutional codes

A *rank metric convolutional code* $\mathcal{C} \subset \mathbb{F}_q^{n\times m}[D]$ is the image of a monomorphism

$$\begin{array}{rcl} \varphi : \mathbb{F}_q[D]^k & \xrightarrow{\gamma} \quad \mathbb{F}_q[D]^{nm} & \xrightarrow{\psi} \mathbb{F}_q[D]^{n\times m} \\ u(D) & \mapsto v(D) = u(D)G(D) \mapsto & V(D) \end{array}$$

where $G(D) \in \mathbb{F}_q^{k\times nm}[D]$ is full row rank and ψ is an isomorphism (e.g.: $V(D) = \psi(v(D))$ s.t. $V_{i,j}(D) = v_{mi+j}(D)$).

Codewords are polynomial matrices

- $G(D)$ is an encoder of $\mathcal{C}$;

- $\mathcal{C}$ is called observable if all its encoders are left prime;

- the degree δ of $\mathcal{C}$ is the minimal sum of the row degrees of all encoders of $\mathcal{C}$.

- $\mathcal{C}$ is called an $(n \times m, k, \delta)$-rank metric convolutional code.

Particular case ($\delta = 0$)

An $(n \times m, k)$-*linear rank metric code* $\mathcal{C} \subset \mathbb{F}_q^{n\times m}$ is the image of a monomorphism

$$\begin{array}{ccccc} \varphi : \mathbb{F}_q^k & \xrightarrow{\gamma} & \mathbb{F}_q^{nm} & \xrightarrow{\psi} & \mathbb{F}_q^{n\times m} \\ u & \mapsto & v = uG & \mapsto & V \end{array}$$

where $G \in \mathbb{F}_q^{k\times nm}$ is full row rank and ψ is an isomorphism (e.g.: $V = \psi(v)$ s.t. $V_{ij} = v_{mi+j}$).

Rank distance: $d_R(A,B) = rk(A-B)$, $A,B \in \mathbb{F}_q^{m\times n}$.

Distance of $\mathcal{C}$: $d_R(\mathcal{C}) = \min\{d_R(A,B) : A,B \in \mathcal{C}, A \neq B\}$.

Rank distance: $d_R(A,B) = rk(A-B)$, $A,B \in \mathbb{F}_q^{m\times n}$.

Distance of $\mathcal{C}$: $d_R(\mathcal{C}) = \min\{d_R(A,B) : A,B \in \mathcal{C}, A \neq B\}$.

If $m \geq n$: $d_R(\mathcal{C}) \leq n - \lceil \frac{k}{m} \rceil + 1$ (Singleton bound).

If $d_R(\mathcal{C}) = n - \lceil \frac{k}{m} \rceil + 1$, $\mathcal{C}$ is MRD (Maximum Rank Distance).

More known approach

A *linear rank metric code* $\mathcal{C}$ is the image of a monomorphism

$$\begin{array}{rccccc} \varphi : \mathbb{F}_{q^m}^{\tilde{k}} & \xrightarrow{\gamma} & \mathbb{F}_{q^m}^{n} & \xrightarrow{\psi} & \mathbb{F}_{q}^{n\times m} \\ \tilde{u} & \mapsto & \tilde{v} = \tilde{u}\tilde{G} & \mapsto & V \end{array}$$

where $\tilde{G} \in \mathbb{F}_{q^m}^{\tilde{k}\times n}$ is full row rank and ψ is an isomorphism.

More known approach

A *linear rank metric code* $\mathcal{C}$ is the image of a monomorphism

$$\begin{array}{ccccc} \varphi: \mathbb{F}_{q^m}^{\tilde{k}} & \xrightarrow{\gamma} & \mathbb{F}_{q^m}^{n} & \xrightarrow{\psi} & \mathbb{F}_q^{n\times m} \\ \tilde{u} & \mapsto & \tilde{v} = \tilde{u}\tilde{G} & \mapsto & V \end{array}$$

where $\tilde{G} \in \mathbb{F}_{q^m}^{\tilde{k}\times n}$ is full row rank and ψ is an isomorphism.

Note: $\mathbb{F}_{q^m}^{\tilde{k}} \simeq \mathbb{F}_q^{\tilde{k}m}$; $\quad \mathbb{F}_{q^m}^{n} \simeq \mathbb{F}_q^{nm} \rightarrow k = m\tilde{k}$, i.e., $m \mid k$

The previous scheme in coordinates, with $G \in \mathbb{F}^{m\tilde{k} \times mn}$ is

$$\begin{array}{rccccc} \varphi : \mathbb{F}_q^{m\tilde{k}} & \xrightarrow{\gamma} & \mathbb{F}_q^{mn} & \xrightarrow{\psi} & \mathbb{F}_q^{n \times m} \\ u & \mapsto & v = uG & \mapsto & V \end{array}$$

The previous scheme in coordinates, with $G \in \mathbb{F}^{m\tilde{k}\times mn}$ is

$$\begin{array}{rcccc} \varphi : \mathbb{F}_q^{m\tilde{k}} & \xrightarrow{\gamma} & \mathbb{F}_q^{mn} & \xrightarrow{\psi} & \mathbb{F}_q^{n\times m} \\ u & \mapsto & v = uG & \mapsto & V \end{array}$$

$$d_R(\mathcal{C}) \leq n - \lceil \frac{k}{m} \rceil + 1 = n - \tilde{k} + 1$$

Gabidulin code (*Delsarte'73, Gabidulin'85*)

Let $q = 2, m = 3, n = 2, \tilde{k} = 1$ and $\alpha = 1 + \alpha^3$ generator of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$

Gabidulin code (*Delsarte'73, Gabidulin'85*)

Let $q = 2, m = 3, n = 2, \tilde{k} = 1$ and $\alpha = 1 + \alpha^3$ generator of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$

Note: $\mathbb{F}_2^3$ is a vector space over $\mathbb{F}_2$ with basis $(1, \alpha, \alpha^2)$

Gabidulin code (*Delsarte'73, Gabidulin'85*)

Let $q = 2, m = 3, n = 2, \tilde{k} = 1$ and $\alpha = 1 + \alpha^3$ generator of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$

Note: $\mathbb{F}_2^3$ is a vector space over $\mathbb{F}_2$ with basis $(1, \alpha, \alpha^2)$

$\mathcal{C}$ is the image

$$\begin{array}{ccccc} \varphi : \mathbb{F}_{q^m}^{\tilde{k}} & \xrightarrow{\gamma} & \mathbb{F}_{q^m}^{n} & \xrightarrow{\psi} & \mathbb{F}_q^{n \times m} \\ \tilde{u} & \mapsto & \tilde{v} = \tilde{u}\tilde{G} & \mapsto & V \end{array}$$

where $\tilde{G} = [\tilde{g}_1 \;\; \tilde{g}_2] \in \mathbb{F}_{2^3}^{1\times 2}$ is s.t. $\tilde{g}_1$ and $\tilde{g}_2$ are LI over $\mathbb{F}_2$; the rows of V are the coordinates of the columns of $\tilde{v} = [\tilde{v}_1 \; \tilde{v}_2]$ over $(1, \alpha, \alpha^2)$

$$\tilde{u} = u_0 + u_1\alpha + u_2\alpha^2 \in \mathbb{F}_2^3, \quad u_i \in \mathbb{F}_2,$$

$\tilde{G} = [\tilde{g}_1 \ \tilde{g}_2]$ with

$\tilde{g}_1 = g_{01} + g_{11}\alpha + g_{21}\alpha^2, \ \ g_{i1} \in \mathbb{F}_2$ and $\tilde{g}_2 = g_{02} + g_{12}\alpha + g_{22}\alpha^2, \ \ g_{i2} \in \mathbb{F}_2$

$$\tilde{u} = u_0 + u_1\alpha + u_2\alpha^2 \in \mathbb{F}_2^3, \quad u_i \in \mathbb{F}_2,$$

$\tilde{G} = [\tilde{g}_1 \ \tilde{g}_2]$ with

$\tilde{g}_1 = g_{01} + g_{11}\alpha + g_{21}\alpha^2, \ \ g_{i1} \in \mathbb{F}_2$ and $\tilde{g}_2 = g_{02} + g_{12}\alpha + g_{22}\alpha^2, \ \ g_{i2} \in \mathbb{F}_2$

$\tilde{u}\tilde{G} = [\tilde{u}\tilde{g}_1 \ \tilde{u}\tilde{g}_2]$

$$\begin{aligned}
\tilde{u}\tilde{g}_1 &= (u_0 + u_1\alpha + u_2\alpha^2)(g_{01} + g_{11}\alpha + g_{21}\alpha^2) \\
&= (u_0 g_{01}) + (u_1 g_{01} + u_0 g_{11})\alpha + (u_2 g_{01} + u_1 g_{11} + u_0 g_{21})\alpha^2 + \\
&\quad (u_2 g_{11} + u_1 g_{21})\alpha^3 + u_2 g_{21}\alpha^4 \\
&= (u_0 g_{01} + u_1 g_{21}) + (u_0 g_{11} + u_1(g_{01} + g_{21}) + u_2(g_{11} + g_{21}))\alpha + \\
&\quad (u_0 g_{21} + u_1 g_{101} + u_2(g_{01} + g_{21}))\alpha^2
\end{aligned}$$

$$\tilde{u}\tilde{G} = uG$$

$$= [u_0\ u_1\ u_2] \left[\begin{array}{ccc|ccc} g_{01} & g_{11} & g_{21} & g_{02} & g_{12} & g_{22} \\ g_{21} & g_{01}+g_{21} & g_{11} & g_{22} & g_{02}+g_{22} & g_{12} \\ g_{11} & g_{11}+g_{21} & g_{01}+g_{21} & g_{12} & g_{12}+g_{22} & g_{02}+g_{22} \end{array}\right]$$

$$\tilde{u}\tilde{G} = uG$$

$$= [u_0\ u_1\ u_2] \left[\begin{array}{ccc|ccc} g_{01} & g_{11} & g_{21} & g_{02} & g_{12} & g_{22} \\ g_{21} & g_{01}+g_{21} & g_{11} & g_{22} & g_{02}+g_{22} & g_{12} \\ g_{11} & g_{11}+g_{21} & g_{01}+g_{21} & g_{12} & g_{12}+g_{22} & g_{02}+g_{22} \end{array} \right]$$

$\mathcal{C}$ is the image

$$\begin{array}{ccccc} \varphi : \mathbb{F}_2^3 & \xrightarrow{\gamma} & \mathbb{F}_2^6 & \xrightarrow{\psi} & \mathbb{F}_q^{3\times 2} \\ u & \mapsto & v = uG & \mapsto & V \end{array}$$

where $v = [v_{01}\ v_{11}\ v_{21} \mid v_{02}\ v_{12}\ v_{22}]$ and $V = \left[\begin{array}{c|c} v_{01} & v_{02} \\ v_{11} & v_{12} \\ v_{21} & v_{22} \end{array} \right]^T$

Back to rank metric convolutional codes

Distance: $A(D) = \sum_{i \in \mathbb{N}} A_i D^i, B(D) = \sum_{i \in \mathbb{N}} B_i D^i \in \mathbb{F}^{n \times m}[D]$

Rank weight: $rkwt(A(D)) = \sum_{i \in \mathbb{N}} rk(A_i)$

Sum rank distance: $d_{SR}(A(D) - B(D)) = rkwt(A(D) - B(D))$

Back to rank metric convolutional codes

Distance: $A(D) = \sum_{i \in \mathbb{N}} A_i D^i, B(D) = \sum_{i \in \mathbb{N}} B_i D^i \in \mathbb{F}^{n \times m}[D]$

Rank weight: $rkwt(A(D)) = \sum_{i \in \mathbb{N}} rk(A_i)$

Sum rank distance: $d_{SR}(A(D) - B(D)) = rkwt(A(D) - B(D))$

Sum rank distance of a rank metric convolutional code

$$d_{SR}(\mathcal{C}) = \min_{V(D),U(D) \in C, V(D) \neq U(D)} d_{SR}(V(D), U(D))$$
$$= \min_{0 \neq V(D) \in C} rkwt\big(V(D)\big).$$

Singleton bound

Theorem (Napp,P.,Rosenthal,Vettori,2016)

Let $\mathcal{C}$ be an (n, k, δ)-rank metric convolutional code. Then the sum rank distance of $\mathcal{C}$ is upper bounded by

$$d_{SR}(\mathcal{C}) \leq n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k(\lfloor \frac{\delta}{k} \rfloor + 1) - \delta}{m} \right\rceil + 1.$$

An $(n \times m, k, \delta)$-rank metric convolutional code whose sum rank distance attains the Singleton bound is called Maximum Rank Distance (MRD).

j-th column rank distance of $\mathcal{C}$

Definition

Let $\mathcal{C}$ be an observable $(n \times m, k, \delta)$-rank metric convolutional code.

For $j \in \mathbb{N}$ the j-th column rank distance of $\mathcal{C}$ is given by

$$d_j^{cr} = \min\{rkwt(V(D)_{|[0,j]}) : V(D) \in \mathcal{C} \text{ and } V_0 \neq 0\},$$

where for $V(D) = \sum_{i \in \mathbb{N}} V_i D^i$ we define $V(D)_{|[0,j]} = \sum_{i=0}^{j} V_i D^i$.

j-th column rank distance of $\mathcal{C}$

Theorem

Let $\mathcal{C}$ be an observable $(n \times m, k, \delta)$-rank metric convolutional code. Then the j-th column rank distance of $\mathcal{C}$ is upper bounded by

$$d_j^{cr} \leq j\left(n - \left\lfloor \frac{k}{m} \right\rfloor\right) + n - \left\lfloor \frac{k-1}{m} \right\rfloor$$

j-th column rank distance of $\mathcal{C}$

Theorem

Let $\mathcal{C}$ be an observable $(n \times m, k, \delta)$-rank metric convolutional code. Then the j-th column rank distance of $\mathcal{C}$ is upper bounded by

$$d_j^{cr} \leq j\left(n - \left\lfloor \frac{k}{m} \right\rfloor\right) + n - \left\lfloor \frac{k-1}{m} \right\rfloor$$

$$d_0^{cr} \leq d_1^{cr} \leq d_2^{cr} \leq \cdots \leq \lim_{j \to \infty} d_j^{cr} = d_{SR}$$

Theorem

Let $\mathcal{C}$ be an MRD observable $(n \times m, k, \delta)$-rank metric convolutional code with column rank distances $d_j^{cr}, j \in \mathbb{N}_0$, and sum rank distance $d_{sumrank}$.
Let $M = min\{j \in \mathbb{N}_0, d_j^{cr} = d_{sumrank}\}$. Then,

$$M = \left\lceil \frac{n\left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta - k\left\lfloor \frac{\delta}{k} \right\rfloor}{m} \right\rfloor}{n - \left\lfloor \frac{k}{m} \right\rfloor} \right\rceil$$

Definition

An observable $(n \times m, k, \delta)$-rank metric convolutional code with column rank distances $d_j^{cr}, j \in \mathbb{N}_0$, is called strongly-MRD if

$$d_M^{cr} = n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k(\lfloor \frac{\delta}{k} \rfloor + 1) - \delta}{m} \right\rceil + 1$$

for

$$M = \left\lceil \frac{n\left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta - k\left\lfloor \frac{\delta}{k} \right\rfloor}{m} \right\rfloor}{n - \left\lfloor \frac{k}{m} \right\rfloor} \right\rceil$$

Definition

An observable $(n \times m, k, \delta)$-rank metric convolutional code with column rank distances $d_j^{cr}, j \in \mathbb{N}_0$, is called strongly-MRD if

$$d_M^{cr} = n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k(\lfloor \frac{\delta}{k} \rfloor + 1) - \delta}{m} \right\rceil + 1$$

for

$$M = \left\lceil \frac{n \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta - k \lfloor \frac{\delta}{k} \rfloor}{m} \right\rfloor}{n - \left\lfloor \frac{k}{m} \right\rfloor} \right\rceil$$

Remark: Strongly-MRD $\Rightarrow$ MRD.

Open problem: Do they exist strongly - MRD rank metric convolutional codes for all parameters n, m, k, δ?

Open problem: Do they exist strongly - MRD rank metric convolutional codes for all parameters n, m, k, δ?

Yes, if $m \geq \delta + k$. In this case:

$$M = \left\lfloor \frac{\delta}{k} \right\rfloor \text{ and } d_j^{cr} = (j+1)n, \; j = 0, \ldots, \left\lfloor \frac{\delta}{k} \right\rfloor$$

$$\text{Singleton bound: } \left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) n = d_M^{cr}$$

Constructions ($m \geq \delta + k$)

$A \in \mathbb{F}_q^{m \times m}$ with irreducible characteristic polynomial $\chi(\lambda)$,

$$\mathbb{F}_q[A] = \left\{ \sum_{i=0}^{m-1} \alpha_i A^i : \alpha_1 \in \mathbb{F}_q, i = 0, \dots, m-1 \right\}$$

is a field.

Constructions ($m \geq \delta + k$)

$A \in \mathbb{F}_q^{m \times m}$ with irreducible characteristic polynomial $\chi(\lambda)$,

$$\mathbb{F}_q[A] = \left\{ \sum_{i=0}^{m-1} \alpha_i A^i : \alpha_1 \in \mathbb{F}_q, i = 0, \ldots, m-1 \right\}$$

is a field.

$X \in \mathbb{F}^{n \times m}$ full row rank

$$G_0 = \begin{bmatrix} \psi^{-1}(XI) \\ \psi^{-1}(XA) \\ \vdots \\ \psi^{-1}(XA^{k-1}) \end{bmatrix}, \; G_1 = \begin{bmatrix} \psi^{-1}(XA^{k}) \\ \psi^{-1}(XA^{k+1}) \\ \vdots \\ \psi^{-1}(XA^{2k-1}) \end{bmatrix}, \ldots,$$

$$G_{\lfloor \frac{\delta}{k} \rfloor} = \begin{bmatrix} \psi^{-1}(XA^{\lfloor \frac{\delta}{k} \rfloor k}) \\ \psi^{-1}(XA^{\lfloor \frac{\delta}{k} \rfloor k+1}) \\ \vdots \\ \psi^{-1}(XA^{(\lfloor \frac{\delta}{k} \rfloor +1)k-1}) \end{bmatrix}, G_{\lfloor \frac{\delta}{k} \rfloor +1} = \begin{bmatrix} \psi^{-1}(XA^{\lfloor \frac{\delta}{k} \rfloor k}) \\ \vdots \\ \psi^{-1}(XA^{(\lfloor \frac{\delta}{k} \rfloor +1)k-1}) \\ 0 \end{bmatrix}$$

Theorem

The $(n \times m, k, \delta)$-rank metric convolutional code $\mathcal{C}$ with encoder

$$G(D) = G_0 + G_1 D + \cdots + G_{\lfloor \frac{\delta}{k} \rfloor}, \text{ if } k|\delta, \quad \text{and}$$

$$G(D) = G_0 + G_1 D + \cdots + G_{\lfloor \frac{\delta}{k} \rfloor} + G_{\lfloor \frac{\delta}{k} \rfloor + 1}, \text{ otherwise}$$

is strongly-MRD when $m \geq \delta$.

Example

Let $n = 3$, $m = 4$, $k = 2$, $\delta = 2$, the companion matrix A of the irreducible polynomial $\chi(\lambda) = \lambda^4 + \lambda + 1 \in \mathbb{F}_2[\lambda]$ and the full row rank matrix $X = \begin{bmatrix} I_3 & 0_{3\times 1} \end{bmatrix}$, i.e.,

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \in \mathbb{F}_2^{4\times 4}, \qquad X = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \in \mathbb{F}_2^{3\times 4}.$$

$$\mathbb{F}_2[A] = \{u_0 I + u_1 A + u_2 A^2 + u_3 A^3 : u_i \in \mathbb{F}_2\} \text{ is a field}$$

$$XA = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \ XA^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}, \ XA^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

$$G_0 = \begin{bmatrix} \psi^{-1}(XI) \\ \psi^{-1}(XA) \end{bmatrix} = \left[\begin{array}{cccc|cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$G_1 = \begin{bmatrix} \psi^{-1}(XA^2) \\ \psi^{-1}(XA^3) \end{bmatrix} = \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right].$$

The convolutional code with encoder $G(D) = G_0 + G_1 D$ has degree 2.

Consider $u(D) = [u_0 \;\; u_1] + [u_2 \;\; u_3]D + \cdots \in \mathbb{F}_2[D]^2$, with $[u_0 \;\; u_1] \neq 0$.

The first two coefficients of the codeword $V(D) = \varphi\big(u(D)\big)$ are

$$V_0 = X(u_0 I + u_1 A) \text{ and } V_1 = X(u_2 I + u_3 A + u_0 A^2 + u_1 A^3).$$

$rk(V_0) = rk(V_1) = 3 \;\Rightarrow\; d_0^{cr} = 3$ and $d_1^{cr} = 6$, which means that $\mathcal{C}$ is strongly-MRD.

Consider $u(D) = [u_0 \;\; u_1] + [u_2 \;\; u_3]D + \cdots \in \mathbb{F}_2[D]^2$, with $[u_0 \;\; u_1] \neq 0$.

The first two coefficients of the codeword $V(D) = \varphi\big(u(D)\big)$ are

$$V_0 = X(u_0 I + u_1 A) \text{ and } V_1 = X(u_2 I + u_3 A + u_0 A^2 + u_1 A^3).$$

$rk(V_0) = rk(V_1) = 3 \;\Rightarrow\; d_0^{cr} = 3$ and $d_1^{cr} = 6$, which means that $\mathcal{C}$ is strongly-MRD.

Thank you for your attention!