This is a previous version of the article published in Linear and Multilinear Algebra. 2024. https://doi.org/10.1080/03081087.2023.2300673

On the construction of MRD convolutional codes

Diego Napp *, Raquel Pinto, Filipa Santana and Carlos Vela†

March 2022

Abstract

The problem of building optimal block codes, such as MDS codes, over small fields has been an active area of research that led to several interesting conjectures. In the context of convolutional codes, optimal constructions, such as MDS or MDP, are very rare and all require very large finite fields. In this work, we focus on the problem of constructing optimal convolutional codes with respect to the rank distance, *i.e.*, we study the construction of Maximum Rank Distance (MRD) convolutional codes. Considering convolutional codes within a very general framework, we present concrete novel classes of MRD convolutional codes for a large set of given parameters.

Keywords— Coding theory, polynomial matrices, finite fields, convolutional codes, Rank metric codes

1 Introduction

Maximum Distance Separable (MDS) codes are one of the most fascinating notions in the area of coding theory [14, Chapter 11]. The name comes from the fact that such a class of codes has the maximum possible free Hamming distance for a given set of parameters. In the context of block codes, these parameters are $[n, k]$, the length and dimension of the code. Block codes that achieve free Hamming distance equal to $n - k + 1$ are called MDS codes. Convolutional codes are more involved than block codes and an additional parameter needs to be introduced: the degree of the code. MDS convolutional codes were introduced in [21] and thoroughly studied by many researchers in the last two decades [18, 23]. These codes were mainly investigated in the context of q-ary symmetric channels and hence the Hamming distance was considered. However, the seminal paper of Koetter and Kschischang [12] introduced novel coding concepts for errors and erasures in a random network coding setting. The mathematical foundations of Random Linear Network Coding (RLNC) were presented for the case where the topology of the network is unknown and the nodes perform a random linear combination of the packets received and forward this random combination to adjacent nodes. From a mathematical point of view, one can consider a packet as a row

*University of Alicante, Spain, diego.napp@ua.es

†CIDMA – Center for Research and Development in Mathematics and Applications, Department of Mathematics, University of Aveiro, Portugal

of a matrix with entries in a finite field and then the linear combinations performed in the nodes are row operations on this matrix. At each shot, several packets are sent via the network and this data can be represented with a matrix. In order to be able to correct errors occurring during the transmission, this set of matrices are equipped with a metric to measure the discrepancy between transmitted matrices, namely, the rank distance. The analogues of MDS codes in the context of rank metric codes are called Maximum Rank Distance (MRD) codes. Rank metric codes have been extensively applied to random network coding and Gabidulin or MRD codes are known to be able to protect packets in such a scenario [10]. We call these codes *one-shot codes*, as they use the (network) channel only once.

However, in a context where several uses of the network are needed to transmit the data, one can create dependencies among the transmitted codewords (matrices) of different shots in order to improve the error-correction capability of the code. This idea gave rise to the so-called *multi-shot network coding* [3, 19, 22]. In the multi-shot setting, an extension of the rank metric was proposed to provide a suitable measure for the number of errors that a code can tolerate. This new metric, called *sum rank distance*, was first proposed in [19] and later, in [3, 22], it was shown to be a suitable metric to deal with errors, erasures and deviations.

A very natural way for building multi-shot codes is to use rank metric convolutional codes (see [20] for different approaches). The work in [22] was pioneer in this direction by presenting the first class of unit-memory rank metric convolutional codes. Later, more properties and applications were investigated in [2, 3, 15], showing the potential of such a framework to spread redundancy across the codewords. However, there exist very few algebraic constructions of multi-shot network codes in comparison to the literature on one-shot network rank metric codes. To the best of our knowledge, only one class of maximum rank distance convolutional codes in this setting has been presented in [3, 15] based on the construction derived in [1].

In [16] a more general theoretical framework to rank metric convolutional codes was presented. Let $\mathbb{F}_q$ be a finite field and let $\mathbb{F}_{q^m}$ be an extension field. Linear rank metric codes have been defined in the literature as images of homomorphisms over $\mathbb{F}_{q^m}$. In contrast, the work presented in [16, 17] introduces linear rank metric codes as being images of a homomorphism that is the composition of a monomorphism and an isomorphism over $\mathbb{F}_q$. Extending this notion, the authors defined rank metric convolutional codes as images of a homomorphism that is a composition of a monomorphism and an isomorphism over $\mathbb{F}_q[D]$. One of the advantages of this approach is that it allows one to deal with rank metric codes of any rate and over any finite field.

In this work, we continue this thread of research within this general framework and present several results that extend the preliminary ones presented in [16, 17]. We focus on the important class of codes called Maximum Rank Distance (MRD) convolutional codes which are rank metric convolutional codes that are optimal (have the largest possible sum rank distance) for a given set of parameters. This class is the analogue of MDS (convolutional) codes when considering the sum rank metric instead of the Hamming metric. In particular, we present novel and more general algebraic constructions of MRD convolutional codes. Although the framework developed in [17] is very general, the constructions presented were very restricted to a small set of parameters. Here, we present a nontrivial extension of these algebraic constructions that are valid for convolutional codes of higher degree and therefore expanding significantly the set of MRD convolutional codes. As mentioned above, preliminary versions of this work were presented in the conferences [16, 17].

2 Preliminaries

Block MDS codes are codes that have the maximum possible value for the minimum Hamming distance between different codewords for a given length n and dimension k. Convolutional codes require an additional parameter: the degree of the code, denoted by δ. The degree of the code is directly related to the memory of the code, *i.e.*, the amount of information an encoder of the code can store when encoding the information vectors, see [8] for more details. In this work, we focus on the codes that matches with MDS codes in the context of rank metric codes, MRD, and study convolutional codes that achieve the maximum possible *rank* distance between codewords taking into account also the degree δ of the code. We begin this section by recalling some notions and results on matrices over $\mathbb{F}_q[D]$, the ring of polynomials in D with coefficients in $\mathbb{F}_q$, that will be needed when defining the degree δ of a convolutional code in the next section.

Definition 2.1. *A matrix $U(D) \in \mathbb{F}_q[D]^{k\times k}$ is said to be unimodular if it has a polynomial inverse, i.e., if there exists $V(D) \in \mathbb{F}_q[D]^{k\times k}$ such that $U(D)V(D) = V(D)U(D) = I$.*

A matrix $U(D) \in \mathbb{F}_q[D]^{k\times k}$ is unimodular if and only if its determinant belongs to $\mathbb{F}_q\backslash\{0\}$, [7, 11].

Polynomial matrices that differ by left multiplication by unimodular matrices are said to be (left) equivalent. Among equivalent polynomial matrices, we will consider the ones that have least sum of its row degrees. The degree of a row of a polynomial matrix is defined as the maximum degree of the row entries.

Definition 2.2. *Let $A(D) \in \mathbb{F}_q[D]^{k\times n}$.*

1. *The internal degree of $A(D)$ is the maximum degree of all $k \times k$ minors of $A(D)$ and it is represented by $intdeg(A(D))$;*
2. *The external degree of $A(D)$ is the sum of the row degrees of $A(D)$, and it is represented by $extdeg(A(D))$.*

It is clear that the internal degree of a polynomial matrix is smaller or equal than its external degree.

Definition 2.3. *Let $A(D) \in \mathbb{F}_q[D]^{k\times n}$ be a full row rank matrix. $A(D)$ is said to be row reduced if $intdeg(A(D)) = extdeg(A(D))$.*

If $A(D) \in \mathbb{F}_q[D]^{k\times n}$ we denote by $[A]^{hc} \in \mathbb{F}_q^{k\times n}$ the coefficient matrix of the highest-order terms in each row, *i.e.*, the matrix with the i-th row constituted by the coefficients of D^{ν_i}, where ν_i is the row degree of the i-th row of $A(D)$. The following theorem gives an efficient way to check if a matrix is row reduced.

Theorem 2.1. *[11, page 385] Let $A(D) \in \mathbb{F}_q[D]^{k\times n}$ and the corresponding $[A]^{hc} \in \mathbb{F}_q^{k\times n}$. Then $A(D)$ is row reduced if and only if $[A]^{hc}$ is a full row rank matrix.*

The next theorems present some results about row reduced matrices.

Theorem 2.2. *[11, page 386] Let $A(D) \in \mathbb{F}_q[D]^{k\times n}$ be a full row rank matrix. Then there exists a unimodular matrix $U(D) \in \mathbb{F}_q[D]^{k\times k}$ such that $U(D)A(D)$ is row reduced.*

Theorem 2.3. *[11, Lema 6.3, page 388] Let $A(D), B(D) \in \mathbb{F}_q[D]^{k\times n}$ be two row reduced matrices such that*

$$A(D) = U(D)B(D),$$

for some unimodular matrix $U(D) \in \mathbb{F}_q[D]^{k\times k}$. Then $A(D)$ and $B(D)$ have the same row degrees, up to a permutation of the rows.

It follows then that in a class of equivalent matrices, row reduced matrices are the ones with minimal external degree.

3 Rank metric convolutional codes

In this work, we consider a very general class of rank metric convolutional codes that allows to work with convolutional codes of any rate and over any finite field. For the sake of clarity we first present this general framework in the context of rank metric block codes and then generalize it to the convolutional setting.

3.1 Rank metric block codes

Let $A, B \in \mathbb{F}_q^{n\times m}$. Gabidulin [6] defines *rank distance* between A and B as

$$d_{\text{rank}}(A, B) = \text{rank}(A - B).$$

Any subset $\mathcal{C}$ of $\mathbb{F}_q^{n\times m}$ equipped with this distance is a *rank metric code*.

Although linear rank metric codes in $\mathbb{F}_q^{n\times m}$ are usually constructed as block codes of length n over the extension field $\mathbb{F}_{q^m}$ (see Remark 3.1 below), in this work we consider a more general definition, first introduced in [17]. An $(n \times m, k)$ *linear rank metric code* $\mathcal{C} \subset \mathbb{F}_q^{n\times m}$ of rate $k/nm < 1$ is the image of a monomorphism $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^{n\times m}$ that is a composition $\varphi = \psi \circ \gamma$ of an isomorphism ψ and a monomorphism γ:

$$\begin{array}{rcccl} \varphi : \mathbb{F}_q^k & \xrightarrow{\gamma} & \mathbb{F}_q^{nm} & \xrightarrow{\psi} & \mathbb{F}_q^{n\times m} \\ u & \longmapsto & v = uG & \longmapsto & V = \psi(v), \end{array}$$

where $G \in \mathbb{F}_q^{k\times nm}$ is full row rank. A codeword $V = \psi(v)$ is simply the n consecutive blocks of v with m elements. The n rows of the codeword V can be interpreted as the n packets of length m that are transmitted through the network at one shot.

The rank distance of $\mathcal{C}$, $d_{\text{rank}}(\mathcal{C})$, is defined as

$$d_{\text{rank}}(\mathcal{C}) = \min_{U,V\in\mathcal{C}} d_{\text{rank}}\big(U - V\big) = \min_{V\in\mathcal{C}, V\neq 0} d_{\text{rank}}\big(V\big),$$

or simply the minimum rank distance between two different codewords. In the following, for the sake of simplicity, we will assume that $n \le m$ (but analogous results can be given for the other case). Linear rank metric codes also have a Singleton-like bound which provides a limit for the value of the code distance.

Theorem 3.1. *[17, Theorem 1] The rank distance of an $(n \times m, k)$ linear rank metric code satisfies*

$$d_{\text{rank}}(\mathcal{C}) \le n - \left\lfloor \frac{k-1}{m} \right\rfloor = n - \left\lceil \frac{k}{m} \right\rceil + 1.$$

A block code $\mathcal{C}$ that attains such an upper-bound is called *Maximum Rank Distance* (MRD) code. The first MRD codes over a finite field $\mathbb{F}_q$ were derived by Delsarte and Gabidulin [5, 6]. In the literature these codes are often called (generalized) Gabidulin codes.

Remark 3.1. *As mentioned above, linear rank metric codes are typically defined over the extension field $\mathbb{F}_{q^m}$ using an isomorphism ϕ between $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_q^{n\times m}$. More concretely, a linear rank metric code is typically defined via*

$$\mathcal{C} = \mathrm{Im}_{\mathbb{F}_{q^m}} G = \left\{ uG : u \in \mathbb{F}_{q^m}^k \right\} \subset \mathbb{F}_{q^m}^n,$$

with $G \in \mathbb{F}_{q^m}^{k\times n}$. Then, the rank metric code is $\phi(\mathcal{C})$, where ϕ is an isomorphism between $\mathbb{F}_{q^m}^n$ and $\mathbb{F}_q^{n\times m}$. MRD codes, including Gabidulin codes, and most of the existing rank metric codes are defined within this framework [9, 4]. Note that in this setting the rate is km/nm and the finite field is $\mathbb{F}_{q^m}$ whereas in the more general framework described above the rate is k/mn and is defined over any finite field $\mathbb{F}_q$ and k does not need to be multiple of m.

3.2 A general framework for rank metric convolutional codes

Again, rank metric convolutional codes are typically defined over $\mathbb{F}_{q^m}[D]$ (see [1, 2, 3, 15, 22]) as finitely generated $\mathbb{F}_{q^m}[D]$-submodules of $\mathbb{F}_{q^m}[D]^n$ described by

$$\mathcal{C} = \mathrm{Im}_{\mathbb{F}_{q^m}[D]} G = \left\{ u(D)G(D) : u(D) \in \mathbb{F}_{q^m}[D]^k \right\} \subset \mathbb{F}_{q^m}[D]^n,$$

or equivalently by $\phi(\mathcal{C})$, where ϕ is a fixed isomorphism between $\mathbb{F}_{q^m}[D]^n$ and $\mathbb{F}_q[D]^{n\times m}$.

However, in this paper, we follow the more general approach first introduced in [16, 17] and define a *rank metric convolutional code* $\mathcal{C} \subset \mathbb{F}_q[D]^{n\times m}$ as the image of an homomorphism $\varphi : \mathbb{F}_q[D]^k \to \mathbb{F}_q[D]^{n\times m}$, such that $\varphi = \psi \circ \gamma$ is a composition of a monomorphism γ and an isomorphism ψ:

$$\begin{aligned} \varphi : \mathbb{F}_q[D]^k &\xrightarrow{\gamma} \mathbb{F}_q[D]^{nm} \xrightarrow{\psi} \mathbb{F}_q[D]^{n\times m} \\ u(D) &\mapsto v(D) = u(D)G(D) \mapsto V(D), \end{aligned} \tag{1}$$

where $G(D) \in \mathbb{F}_q^{k\times nm}$ is a full row rank polynomial matrix, called *encoder* of $\mathcal{C}$. For simplicity, we will consider that the isomorphism ψ is such that $V_{i,j}(D) = v_{mi+j}(D)$, *i.e.*, the rows of $V(D)$ are the n consecutive blocks of $v(D)$, each one with m elements.

Two encoders of $\mathcal{C}$ differ by left multiplication by a unimodular matrix and therefore $\mathcal{C}$ always admits row reduced encoders.

The degree δ of a rank metric convolutional code $\mathcal{C}$ is the sum of the row degrees of a row reduced encoder of $\mathcal{C}$, *i.e.*, the minimum value of the sum of the row degrees of its encoders. A rank metric convolutional code $\mathcal{C}$ is said to be *delay-free* if it has an encoder $G(D)$ with constant term $G(0)$ having full row rank. Note that since any other encoder of $\mathcal{C}$, $\tilde{G}(D)$, is such that $\tilde{G}(D) = U(D)G(D)$ for some unimodular matrix $U(D)$, it follows that all encoders of $\mathcal{C}$ have constant term full row rank.

A rank metric convolutional code $\mathcal{C}$ of degree δ, defined as in (1), is called an $(n \times m, k, \delta)$-rank metric convolutional code.

When dealing with rank metric codes, a different measure of distance must be considered. The *rank weight* of a polynomial matrix $A(D) = \sum_{i\in\mathbb{N}} A_i D^i \in \mathbb{F}_q[D]^{n\times m}$, is given by

$$\mathrm{rwt}\big(A(D)\big) = \sum_{i\in\mathbb{N}} \mathrm{rank}(A_i).$$

If $B(D) = \sum_{i\in\mathbb{N}} B_i D^i \in \mathbb{F}_q[D]^{n\times m}$, the *sum rank distance* between $A(D)$ and $B(D)$ is defined as

$$\begin{aligned} d_{\mathrm{SR}}\big(A(D), B(D)\big) &= \mathrm{rwt}\big(A(D) - B(D)\big) \\ &= \sum_{i\in\mathbb{N}} \mathrm{rank}(A_i - B_i). \end{aligned}$$

Lemma 3.1. *[16, Lemma 2] The sum rank distance d_{SR} is a distance in $\mathbb{F}_q[D]^{n\times m}$.*

The *sum rank distance* of a rank metric convolutional code $\mathcal{C}$ is defined as

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

As $\mathcal{C}$ is linear, $V(D) - U(D) \in \mathcal{C}$ for any $V(D), U(D) \in \mathcal{C}$, and therefore it follows that

$$d_{\mathrm{SR}}(\mathcal{C}) = \min_{0\neq V(D)\in\mathcal{C}} \mathrm{rwt}\big(V(D)\big).$$

The next theorem establishes an upper-bound on the sum rank distance of a rank metric convolutional code. Analogously, as for the free Hamming distance of a convolutional code [8], this bound is referred to as the generalized Singleton bound for rank metric convolutional codes. For simplicity, we will assume that $n \leq m$, but similar results can be given for the case in which $n > m$.

Theorem 3.2. *[16, Theorem 3] Let $\mathcal{C}$ be an $(n \times m, k, \delta)$ rank metric convolutional code. Then, the sum rank distance of $\mathcal{C}$ is upper bounded by*

$$d_{\mathrm{SR}}(\mathcal{C}) \leq n\left(\left\lfloor\frac{\delta}{k}\right\rfloor + 1\right) - \left\lceil\frac{k(\lfloor\frac{\delta}{k}\rfloor + 1) - \delta}{m}\right\rceil + 1. \tag{2}$$

An $(n\times m, k, \delta)$ rank metric convolutional code whose sum rank distance attains the generalized Singleton bound is called *Maximum Rank Distance* (MRD) convolutional code. The row reduced encoders of MRD convolutional codes have a well-established set of row degrees as stated in the following lemma.

Corollary 3.1. *[16, Corollary 4]. Let $\mathcal{C}$ be an $(n \times m, k, \delta)$ rank metric convolutional code and $G(D) \in \mathbb{F}_q[D]^{k\times n}$ be a row reduced encoder of $\mathcal{C}$. Then $G(D)$ has $k\left(\lfloor\frac{\delta}{k}\rfloor + 1\right) - \delta$ rows of degree $\lfloor\frac{\delta}{k}\rfloor$ and $\delta - k\lfloor\frac{\delta}{k}\rfloor$ rows of degree $\lfloor\frac{\delta}{k}\rfloor + 1$.*

It is not known the existence of MRD $(n \times m, k, \delta)$ convolutional codes for every choice of parameters $n, m, k, \delta \in \mathbb{N}$. Napp, Pinto, Rosenthal and Vettori [17] proposed the first construction of $(n \times m, k, \delta)$ MRD convolutional codes for $m \geq \delta + k$. For the sake of clarity and completeness, we recall these constructions and present the proof that they are indeed MRD codes.

Theorem 3.3. *[17, Theorem 6] Let n, m, k, δ be integers such that $k < nm$, $n > m$, $\delta < m - k$ and $A \in \mathbb{F}_q^{m\times m}$ be a matrix with irreducible characteristic polynomial and a full row rank matrix $X \in \mathbb{F}_q^{n\times m}$. Let*

$$G(D) = \sum_{i=0}^{\lfloor \frac{\delta}{k} \rfloor + 1} G_i D^i \in \mathbb{F}_q[D]^{k\times mm}, \tag{3}$$

with

$$G_i = \begin{bmatrix} \psi^{-1}(XA^{ki}) \\ \psi^{-1}(XA^{ki+1}) \\ \vdots \\ \psi^{-1}(XA^{ki+k-1}) \end{bmatrix}, \ 0 \leq i \leq \left\lfloor \frac{\delta}{k} \right\rfloor$$

and

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

then $G(D)$ is an encoder of an MRD $(n \times m, k, \delta)$ convolutional code.

Remark 3.2. *Since $A \in \mathbb{F}_q^{m\times m}$ is a matrix with irreducible characteristic polynomial, then the matrices A^i, $0 \leq i < m$, are linearly independent over $\mathbb{F}_q$ and*

$$\mathbb{F}_q[A] = \{\sum_{i=0}^{m-1} u_i A^i \ : \ i = 0, 1, \ldots, m-1\} \simeq \mathbb{F}_q^m$$

is a field [13]. Thus, any nontrivial linear combination of A^i, $0 \leq i < m$ is a full rank matrix.

Remark 3.3. *Theorem 3.3 is valid for any field $\mathbb{F}_q$ since it depends on the existence of a matrix with an irreducible characteristic polynomial of a certain degree. There exist irreducible polynomials of every degree over any finite field and the correspondent companion matrices can be considered as the A in the theorem. Note however that the parameters n, k, δ and m are restricted.*

4 Constructions of MRD convolutional codes

Although the constructions presented above are MRD convolutional codes over finite fields relatively small number of elements (compare for instance with [3, Theorem 4] or [1, Section 4]) they are intrinsically restricted to very small parameters and there is no obvious way to extend them to larger set of parameters. In this section, we will present novel constructions of MRD convolutional codes that overcome these limitations. The idea we present in this work, in order to increase the degree of these codes, is to build new encoders similar to the ones presented above, but carefully adding new terms of higher degree to come up with new polynomial matrices (encoders) of larger degrees.

These new terms are obtained from coefficients of terms with lower degree reversing the rows order, in such a way that the resulting codes are again MRD convolutional codes.

Recall that n, m and k are integers such that $n \leq m$, $k < nm$. We divide this section into two separate parts where we address the cases in which $k \mid m$ and $k \nmid m$.

4.1 Construction for the case $k \mid m$

The constructions presented in [16] allowed to obtain $(n \times m, k, \delta)$ MRD convolutional codes, with $\delta \leq m - k$. In this section, we will present a nontrivial generalization of this construction in order to allow much larger degrees. In particular, we build a concrete class of $(n \times m, k, \delta)$ MRD convolutional codes for $\delta \leq 2m - k$ where $k \mid m$.

Let us consider $\delta = m - k$. Note that $k \mid \delta$ since $k \mid m$. Define the polynomial matrix

$$G(D) = \sum_{i=0}^{2\frac{\delta}{k}+1} G_i D^i \in \mathbb{F}_q[D]^{k \times nm}, \tag{4}$$

with

$$G_i = \begin{bmatrix} \psi^{-1}(XA^{ki}) \\ \psi^{-1}(XA^{ki+1}) \\ \vdots \\ \psi^{-1}(XA^{ki+k-1}) \end{bmatrix}, \ 0 \leq i \leq \frac{\delta}{k},$$

where $A \in \mathbb{F}_q^{m \times m}$ is a matrix with irreducible characteristic polynomial and $X \in \mathbb{F}_q^{n \times m}$ a full row rank matrix, and

$$G_i = \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_{2\frac{\delta}{k}+1-i},$$

for $\frac{\delta}{k} + 1 \leq i \leq 2\frac{\delta}{k} + 1$ and where the matrix $\begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix}$ is the one with ones on the main reversed diagonal and zeros everywhere else.

Let $\mathcal{C}$ be the rank metric convolutional code with encoder $G(D)$. The next lemma shows that $\mathcal{C}$ has degree $2\delta + k$.

Lemma 4.1. *Let m, n, k and δ be integers with $n \leq m$, $k < nm$, $\delta = m - k$ and such that $k \mid m$. Let $A \in \mathbb{F}_q^{m \times m}$ be a matrix with irreducible characteristic polynomial and $X \in \mathbb{F}_q^{n \times m}$ a full row rank matrix. Let $\mathcal{C}$ be the rank metric convolutional code with encoder $G(D)$ as defined in (4). Then $\mathcal{C}$ is an $(n \times m, k, 2\delta + k)$ rank metric convolutional code.*

Proof. Note that

$$[G]^{hc} = G_{2\frac{\delta}{k}+1} = \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_0.$$

Since G_0 has full row rank (by a similar reasoning as in Theorem 3.3), then $[G]^{hc} = G_{2\frac{\delta}{k}+1}$ is also a full row rank matrix. This means that $G(D)$ is row reduced. Thus the degree of $\mathcal{C}$ is equal to the external degree of $G(D)$ which is $k\left(2\frac{\delta}{k} + 1\right) = 2\delta + k$. □

The next theorem shows that $\mathcal{C}$ is an $(n \times m, k, 2\delta + k)$ MRD convolutional code.

Theorem 4.1. *Let $m, n, k, \delta, A, X, G(D)$ and $\mathcal{C}$ be as defined in Lemma 4.1. Then $\mathcal{C}$ is an $(n \times m, k, 2\delta + k)$ MRD convolutional code.*

Proof. From Theorem 3.2 it follows that we need to show that

$$d_{\mathrm{SR}}(\mathcal{C}) = 2n\left(\frac{\delta}{k} + 1\right).$$

To this end, we will show that $\operatorname{rwt}(V(D)) \geq 2n\left(\frac{\delta}{k}+1\right)$ for any nonzero $V(D) \in \mathcal{C}$. Let $u(D) = \sum_{i=0}^{\ell} u_i D^i \in \mathbb{F}_q[D]^k$, with $u_\ell \neq 0$, be a nonzero vector $v(D) = u(D)G(D) \in \mathbb{F}_q[D]^{nm}$ and $V(D) = \psi(v(D)) = \sum_{i \in \mathbb{N}_0} V_i D^i \in \mathcal{C}$. We can assume, without loss of generality, that $u_0 \neq 0$. Let us represent $u_i = \begin{bmatrix} u_i^0 & u_i^1 & \cdots & u_i^{k-1} \end{bmatrix}$, $i \in \mathbb{N}_0$.

The first $\frac{\delta}{k} + 1$ coefficients of $v(D)$ are of the form

$$v_i = \sum_{j=0}^{i} u_{i-j} G_j, \quad 0 \leq i \leq \frac{\delta}{k}$$

and the correspondent $\dfrac{\delta}{k} + 1$ coefficients of $V(D)$ are

$$V_i = X B_i, \quad 0 \leq i \leq \frac{\delta}{k},$$

where

$$B_i = \sum_{j=0}^{i} (u_{i-j}^0 A^{ki} + u_{i-j}^1 A^{kj+1} + \cdots + u_{i-i}^{k-1} A^{kj-k+1})$$

which is a nontrivial linear combination of $I, A, \ldots, A^{\delta+k-1}$ since $u_0^s \neq 0$ for some $s \in \{0, 1, \ldots, k-1\}$. This means that B_i, $i = 0, 1, \ldots, \frac{\delta}{k}$ have full row rank and consequently also the first $\frac{\delta}{k} + 1$ coefficients of $V(D)$ have full row rank, and consequently

$$\sum_{i=0}^{\frac{\delta}{k}} \operatorname{rank}(V_i) = n\left(\frac{\delta}{k} + 1\right).$$

The next $\frac{\delta}{k} + 1$ vector coefficients of $v(D)$ are defined as

$$\begin{aligned}
v_{\frac{\delta}{k}+i} &= \sum_{j=0}^{\frac{\delta}{k}+i} u_{\frac{\delta}{k}+i-j} G_j \\
&= \sum_{j=0}^{\frac{\delta}{k}-i} u_{\frac{\delta}{k}+i-j} G_j + \sum_{j=\frac{\delta}{k}-i+1}^{\frac{\delta}{k}} u_{\frac{\delta}{k}+i-j} G_j + \sum_{j=\frac{\delta}{k}-i+1}^{\frac{\delta}{k}} u_{j+i-\frac{\delta}{k}-1} \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_j \\
&= \sum_{j=0}^{\frac{\delta}{k}-i} u_{\frac{\delta}{k}+i-j} G_j + \sum_{j=0}^{i-1} u_{i+j} G_{\frac{\delta}{k}-j} + \sum_{j=0}^{i-1} u_{i-j+1} \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_{\frac{\delta}{k}-j} \\
&= \sum_{j=0}^{\frac{\delta}{k}-i} u_{\frac{\delta}{k}+i-j} G_j + \sum_{j=0}^{i-1} (u_{i+j} + \hat{u}_{i-j+1}) G_{\frac{\delta}{k}-j},
\end{aligned}$$

where $\hat{u}_{i-j+1} = u_{i-j+1} \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} = \begin{bmatrix} u_{i-j+1}^{k-1} & u_{i-j+1}^{k-2} & \cdots & u_{i-j+1}^{0} \end{bmatrix}$, $j = 0, 1, \ldots, i-1$ and $i = 1, \ldots, \frac{\delta}{k} + 1$. Thus,

$$V_{\frac{\delta}{k}+i} = XB_{\frac{\delta}{k}+i}, \tag{5}$$

where

$$\begin{aligned} B_{\frac{\delta}{k}+i} = & \sum_{j=0}^{\frac{\delta}{k}-i} \left(u^0_{\frac{\delta}{k}+i-j} A^{kj} + u^1_{\frac{\delta}{k}+i-j} A^{kj+1} + \cdots + u^{k-1}_{\frac{\delta}{k}+i-j} A^{kj+k-1} \right) + \\ & + \sum_{j=0}^{i-1} \Big[(u^0_{i+j} + u^{k-1}_{i-j-1}) A^{\delta-kj} + (u^1_{i+j} + u^{k-2}_{i-j-1}) A^{\delta-kj+1} + \cdots + \\ & + (u^{k-1}_{i+j} + u^0_{i-j-1}) A^{\delta-kj+k-1} \Big]. \end{aligned}$$

If $B_{\frac{\delta}{k}+i} \neq 0$, for all $i = 1, 2, \ldots, \frac{\delta}{k} + 1$, then $B_{\frac{\delta}{k}+i}$ has full row rank because it is an element of $\mathbb{F}_q[A]$, and therefore $V_{\frac{\delta}{k}+i} = XB_{\frac{\delta}{k}+i}$ has full row rank and $\sum_{i=\frac{\delta}{k}+1}^{2\frac{\delta}{k}+1} \operatorname{rank}(V_i) = n(\frac{\delta}{k}+1)$. So, we have that

$$\operatorname{rwt}(V(D)) \geq \sum_{i=0}^{2\frac{\delta}{k}+1} \operatorname{rank}(V_i) = 2n\left(\frac{\delta}{k}+1\right).$$

Let us now assume that there exists a set of integers $1 \leq i_1 < i_2 < \cdots < i_R \leq \frac{\delta}{k} + 1$ such that

$$V_{\frac{\delta}{k}+i_1} = V_{\frac{\delta}{k}+i_2} = \cdots = V_{\frac{\delta}{k}+i_R} = 0.$$

and $V_{\frac{\delta}{k}+j} \neq 0$ for $j \in \{1, 2, \ldots, \frac{\delta}{k}+1\} \setminus \{i_1, i_2, \ldots, i_R\}$. Note that $R \leq \frac{\delta}{k}+1$ Therefore we have that

$$\sum_{j=\frac{\delta}{k}+1}^{2\frac{\delta}{k}+1} \operatorname{rank}(V_j) = n\left(\frac{\delta}{k}+1-R\right).$$

Note that when we assume that $V_{\frac{\delta}{k}+i_z} = 0$ for some $z \in \{1, 2, \ldots, R\}$, then we have that

$$u_{2i_z} = u_{2i_z+1} = \cdots = u_{\frac{\delta}{k}+z-1} = u_{\frac{\delta}{k}+z} = 0, \tag{6}$$

and for $j = 0, 1, \ldots, i_z - 1$,

$$u_{2i_z-1-j} = -\hat{u}_j \quad \text{where} \quad \hat{u}_j = u_j \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix}. \tag{7}$$

More precisely we have that

$$u^0_{i_z+j} + u^{k-1}_{i_z-j-1} = u^1_{i_z+j} + u^{k-2}_{i_z-j-1} = \cdots = u^{k-1}_{i_z+j} + u^0_{i_z-j-1} = 0.$$

In particular,

$$u_{2i_R-1} = -u_0, \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} \Rightarrow u_{2i_R-1} + \hat{u}_0 = 0,$$

and $u_{2i_R-1} \neq 0$. Thus is easy to see that the degree of $u(D)$ is such that $\ell \geq 2i_R - 1 \geq 2R - 1$. Note that the degree of $V(D) = \psi(u(D)G(D))$ is $2\frac{\delta}{k} + 1 + \ell \geq 2\frac{\delta}{k} + 2R$.

Since $u_\ell \neq 0$ is easy to see that the last R coefficients of $V(D)$ have full row rank since $B_{2\frac{\delta}{k}+\ell-R+2}, \dots, B_{2\frac{\delta}{k}+\ell+1}$ are nonzero due to the same reasons as the first $\frac{\delta}{k} + 1$ (they are linear combinations of the elements of the matrices $I, A, \dots, A^{\delta+k-1}$ with at least one coefficient different from zero). Then, to conclude, we obtain that

$$\mathrm{rwt}(V(D)) \geq 2n \left(\frac{\delta}{k} + 1 \right).$$

So, we proved that $\mathcal{C}$ is MRD. □

The next example illustrates the above theorem.

Example 4.1. *Consider the companion matrix*

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

of the irreducible polynomial $\chi(\lambda) = \lambda^4 + \lambda + 1 \in \mathbb{F}_2[\lambda]$. *and the full row rank matrix*

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

Let $\delta = 2$ *and* $k = 2$ *(note that* $\delta = m - k$ *and* $k \mid m$*).*

The rank metric convolutional code with encoder $G(D) = G_0 + G_1 D + G_2 D^2 + G_3 D^3$ *with*

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

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

$$\begin{aligned} G_2 &= \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_1 \\ &= \begin{bmatrix} \psi^{-1}(XA^3) \\ \psi^{-1}(XA^2) \end{bmatrix} = \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{array}\right] \end{aligned}$$

and

$$G_3 = \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_0$$

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

is a $(3 \times 4, 2, 6)$ *MRD convolutional code.*

The construction presented in this subsection allows to obtain an $(n \times m, k, \delta)$ MRD convolutional code for $\delta \leq 2m - k$. To build an encoder of an $(n \times m, k, \delta)$ MRD convolutional code for $\delta < 2m - k$ it is enough to consider an encoder

$$G(D) = \sum_{i=0}^{\lfloor \frac{\delta}{k} \rfloor} G_i D^i + \tilde{G}_{\lfloor \frac{\delta}{k} \rfloor + 1} D^{\lfloor \frac{\delta}{k} \rfloor + 1},$$

where G_i, $i = 0, 1, \ldots, \lfloor \frac{\delta}{k} \rfloor$, are the first $\lfloor \frac{\delta}{k} \rfloor + 1$ matrix coefficients of the matrix defined in (4) and the matrix $\tilde{G}_{\lfloor \frac{\delta}{k} \rfloor + 1}$ has the first $\delta - \lfloor \frac{\delta}{k} \rfloor k$ rows equal to the first $\delta - \lfloor \frac{\delta}{k} \rfloor k$ rows of $G_{\delta - (\lfloor \frac{\delta}{k} \rfloor k + 1)}$ as defined in (4) and the remaining rows equal to zero.

4.2 Construction for the case $k \nmid m$

Next we address the case in which n, m and k be integers with $n \leq m$, $k < nm$ such that $k \nmid m$ and $\delta = m - k$ (note that $k \nmid \delta$). In this subsection, we will construct an $(n \times m, k, k\left(2\lfloor \frac{\delta}{k} \rfloor + 3\right))$ MRD convolutional codes.

Let $A \in \mathbb{F}_q^{m \times m}$ be a matrix with irreducible characteristic polynomial and $X \in \mathbb{F}_q^{n \times m}$ a full row rank matrix.

Let

$$G_i = \begin{bmatrix} \psi^{-1}(XA^{ki}) \\ \psi^{-1}(XA^{ki+1}) \\ \vdots \\ \psi^{-1}(XA^{ki+k-1}) \end{bmatrix}, \; 0 \leq i \leq \left\lfloor \frac{\delta}{k} \right\rfloor$$

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

and

$$G_i = \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_{2\lfloor \frac{\delta}{k} \rfloor + 3 - i},$$

for $\lfloor \frac{\delta}{k} \rfloor + 2 \leq i \leq 2 \lfloor \frac{\delta}{k} \rfloor + 3$.

Let $\mathcal{C}$ be the rank metric convolutional code with encoder

$$G(D) = \sum_{i=0}^{2\left\lfloor \frac{\delta}{k} \right\rfloor + 3} G_i D^i \in \mathbb{F}[D]^{k \times nm}. \tag{8}$$

The next lemma states that $\mathcal{C}$ has degree $k\left(2\left\lfloor \frac{\delta}{k} \right\rfloor + 3\right)$.

Lemma 4.2. *Let m, n, k be integers with $n \leq m$, $k < nm$, such that $k \nmid m$, and $\delta = m - k$. Let $A \in \mathbb{F}_q^{m \times m}$ be a matrix with irreducible characteristic polynomial and $X \in \mathbb{F}_q^{n \times m}$ a full row rank matrix. Let $\mathcal{C}$ be the rank metric convolutional code with encoder $G(D)$ as defined in (8). Then $\mathcal{C}$ is an $\left(n \times m, k, k\left(2\left\lfloor \frac{\delta}{k} \right\rfloor + 3\right)\right)$ rank metric convolutional code.*

Proof. By a similar reasoning to the proof of Lemma 4.1 we show that $[G]^{hc} = \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_0$ has full row rank and so we conclude that $G(D)$ is row reduced. Therefore, the degree of the code is equal to $\text{extdeg}(G(D)) = k\left(2\left\lfloor \frac{\delta}{k} \right\rfloor + 3\right)$. □

The next theorem shows that $\mathcal{C}$ is an $\left(n \times m, k, k\left(2\left\lfloor \frac{\delta}{k} \right\rfloor + 3\right)\right)$ MRD convolutional code.

Theorem 4.2. *Let $m, n, k, \delta, A, X, G(D)$ and $\mathcal{C}$ be as defined in Lemma 4.2. Then $\mathcal{C}$ is an $\left(n \times m, k, k\left(2\left\lfloor \frac{\delta}{k} \right\rfloor + 3\right)\right)$ MRD convolutional code.*

Proof. From Theorem 3.2 it follows that we need to show that

$$d_{\text{SR}}(\mathcal{C}) = 2n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right).$$

To this end, we will see that $\text{rwt}(V(D)) \geq 2n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right)$ for any nonzero $V(D) \in \mathcal{C}$. Let $u(D) = \sum_{i=0}^{\ell} u_i D^i \in \mathbb{F}_q[D]^k$, with $u_\ell \neq 0$, be a nonzero vector $v(D) = u(D)G(D) \in \mathbb{F}_q[D]^{nm}$ and $V(D) = \psi(v(D)) = \sum_{i \in \mathbb{N}_0} V_i D^i \in \mathcal{C}$. We can assume, without loss of generality, that $u_0 \neq 0$. Let us represent $u_i = \begin{bmatrix} u_i^0 & u_i^1 & \cdots & u_i^{k-1} \end{bmatrix}$, $i \in \mathbb{N}_0$.

Using the same reasoning of Theorem 4.1 we conclude that the first $\left\lfloor \frac{\delta}{k} \right\rfloor + 1$ coefficients of $V(D)$ are full row rank, hence

$$\sum_{i=0}^{\left\lfloor \frac{\delta}{k} \right\rfloor} \text{rank}(V_i) = n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right).$$

The coefficient of $v(D)$ of degree $\left\lfloor \frac{\delta}{k} \right\rfloor + 1$ is given by

$$\begin{aligned} v_{\left\lfloor \frac{\delta}{k} \right\rfloor + 1} &= u_0 G_{\left\lfloor \frac{\delta}{k} \right\rfloor + 1} + u_1 G_{\left\lfloor \frac{\delta}{k} \right\rfloor} + \cdots + u_{\left\lfloor \frac{\delta}{k} \right\rfloor} G_1 + u_{\left\lfloor \frac{\delta}{k} \right\rfloor + 1} G_0 \\ &= \left[\sum_{j=1}^{\left\lfloor \frac{\delta}{k} \right\rfloor} u_{\left\lfloor \frac{\delta}{k} \right\rfloor + 1 - j} G_j \right] + u_0 G_{\left\lfloor \frac{\delta}{k} \right\rfloor} + u_{\left\lfloor \frac{\delta}{k} \right\rfloor + 1} G_0 \end{aligned}$$

and therefore, $V_{\lfloor \frac{\delta}{k} \rfloor+1} = XB_{\lfloor \frac{\delta}{k} \rfloor+1}$ with

$$\begin{aligned} B_{\lfloor \frac{\delta}{k} \rfloor+1} &= \sum_{j=0}^{\delta-k\lfloor \frac{\delta}{k} \rfloor-1} u_0^j A^{k\lfloor \frac{\delta}{k} \rfloor+k+j} + \sum_{j=1}^{\lfloor \frac{\delta}{k} \rfloor} \left[\sum_{h=1}^{k-1} u^h_{\lfloor \frac{\delta}{k} \rfloor+1-j} A^{kj+h} \right] \\ &+ \left(\sum_{j=0}^{(k-1)-(\delta-k\lfloor \frac{\delta}{k} \rfloor)} \left[u_0^{\delta-k\lfloor \frac{\delta}{k} \rfloor+j} + u^j_{\lfloor \frac{\delta}{k} \rfloor+1} \right] A^j \right) + \\ &+ \sum_{j=(k-1)-(\delta-k\lfloor \frac{\delta}{k} \rfloor)+1}^{k-1} u^j_{\lfloor \frac{\delta}{k} \rfloor+1} A^j. \end{aligned} \tag{9}$$

The next $\lfloor \frac{\delta}{k} \rfloor + 2$ coefficients of $v(D)$ are given by

$$\begin{aligned} v_{\lfloor \frac{\delta}{k} \rfloor+1+i} &= u_{\lfloor \frac{\delta}{k} \rfloor+1+i} G_0 + \cdots + u_{2i} G_{\lfloor \frac{\delta}{k} \rfloor+1-i} + u_{2i-1} G_{\lfloor \frac{\delta}{k} \rfloor+2-i} + \cdots + u_i G_{\lfloor \frac{\delta}{k} \rfloor+1} \\ &+ u_{i-1} \begin{bmatrix} 0 & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & 0 \end{bmatrix} G_{\lfloor \frac{\delta}{k} \rfloor+1} + \cdots + u_0 \begin{bmatrix} 0 & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & 0 \end{bmatrix} G_{\lfloor \frac{\delta}{k} \rfloor+2-i} \end{aligned} \tag{10}$$

for $1 \leq i \leq \lfloor \frac{\delta}{k} \rfloor + 2$. Then, for $1 \leq i \leq \lfloor \frac{\delta}{k} \rfloor + 2$, $V_{\lfloor \frac{\delta}{k} \rfloor+1+i} = XB_{\lfloor \frac{\delta}{k} \rfloor+1+i}$ where

$$\begin{aligned} B_{\lfloor \frac{\delta}{k} \rfloor+1+i} = & \sum_{j=0}^{k-1-(\delta-k\lfloor \frac{\delta}{k} \rfloor)} \left(u^j_{\lfloor \frac{\delta}{k} \rfloor+1+i} + u_i^{\delta-k\lfloor \frac{\delta}{k} \rfloor+j} + u_{i-1}^{k-1-(\delta-k\lfloor \frac{\delta}{k} \rfloor)-j} \right) A^j \\ &+ \sum_{j=1}^{\lfloor \frac{\delta}{k} \rfloor+1-i} \left[\sum_{h=0}^{k-1} u^h_{\lfloor \frac{\delta}{k} \rfloor+1+i-j} A^{kj+h} \right] \\ &+ \sum_{h=0}^{i-2} \sum_{j=0}^{k-1} \left(u^j_{2i-1-h} + u_h^{k-1-j} \right) A^{k(\lfloor \frac{\delta}{k} \rfloor+2-i+h)+j} \\ &+ \sum_{j=0}^{\delta-k\lfloor \frac{\delta}{k} \rfloor-1} \left(u_i^j + u_{i-1}^{k-1-j} \right) A^{k\lfloor \frac{\delta}{k} \rfloor+k+j} \\ &+ \sum_{j=k-(\delta-k\lfloor \frac{\delta}{k} \rfloor)}^{k-1} u^j_{\lfloor \frac{\delta}{k} \rfloor+i+1} A^j. \end{aligned}$$

Let us consider the following cases.

Case 1: If $B_{\lfloor \frac{\delta}{k} \rfloor+i} \neq 0$, for all $i = 1, 2, \ldots, \lfloor \frac{\delta}{k} \rfloor + 3$, then $B_{\lfloor \frac{\delta}{k} \rfloor+i}$ is full row rank and $V_{\lfloor \frac{\delta}{k} \rfloor+i}$ is full row rank. Consequently, $\sum_{i=\lfloor \frac{\delta}{k} \rfloor+1}^{2\lfloor \frac{\delta}{k} \rfloor+3} \text{rank}(V_i) = n(\lfloor \frac{\delta}{k} \rfloor + 2)$ and therefore

$$\text{rwt}(V(D)) \geq \sum_{i=0}^{2\lfloor \frac{\delta}{k} \rfloor+3} \text{rank}(V_i) = 2n \left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2 \right).$$

Case 2: Let us now assume that $V_{\lfloor \frac{\delta}{k} \rfloor+1} = 0$. Then

$$u_1 = u_2 = \cdots = u_{\lfloor \frac{\delta}{k} \rfloor} = 0,$$

$$u_0^0 = \cdots = u_0^{\delta - k\lfloor \frac{\delta}{k} \rfloor - 1} = u_{\lfloor \frac{\delta}{k} \rfloor + 1}^{k-(\delta - k\lfloor \frac{\delta}{k} \rfloor)} = \cdots = u_{\lfloor \frac{\delta}{k} \rfloor + 1}^{k-1} = 0 \tag{11}$$

and

$$\begin{bmatrix} u_{\lfloor \frac{\delta}{k} \rfloor + 1}^0 & \cdots & u_{\lfloor \frac{\delta}{k} \rfloor + 1}^{k-1-\left(\delta - k\lfloor \frac{\delta}{k} \rfloor\right)} \end{bmatrix} = - \begin{bmatrix} u_0^{\delta - k\lfloor \frac{\delta}{k} \rfloor} & \cdots & u_0^{k-1} \end{bmatrix}.$$

Since $u_0 \neq 0$ and considering equation (11) it follows that

$$\begin{bmatrix} u_0^{\delta - k\lfloor \frac{\delta}{k} \rfloor} & \cdots & u_0^{k-1} \end{bmatrix} \neq 0$$

as well as

$$\begin{bmatrix} u_{\lfloor \frac{\delta}{k} \rfloor + 1}^0 & \cdots & u_{\lfloor \frac{\delta}{k} \rfloor + 1}^{k-1-\left(\delta - k\lfloor \frac{\delta}{k} \rfloor\right)} \end{bmatrix} \neq 0. \tag{12}$$

Thus $V_{\lfloor \frac{\delta}{k} \rfloor + 2} = XB_{\lfloor \frac{\delta}{k} \rfloor + 2}$ and $V_{\lfloor \frac{\delta}{k} \rfloor + 3} = XB_{\lfloor \frac{\delta}{k} \rfloor + 3}$ with

$$B_{\lfloor \frac{\delta}{k} \rfloor + 2} = \sum_{j=0}^{k-1} u_{\lfloor \frac{\delta}{k} \rfloor + 2}^j A^j + \sum_{j=0}^{k-1-\left(\delta - k\lfloor \frac{\delta}{k} \rfloor\right)} u_{\lfloor \frac{\delta}{k} \rfloor + 1}^j A^{k+j} + \sum_{j=0}^{\delta - k\lfloor \frac{\delta}{k} \rfloor - 1} u_0^{k-1-j} A^{k\lfloor \frac{\delta}{k} \rfloor + k + j}$$

and

$$\begin{aligned} B_{\lfloor \frac{\delta}{k} \rfloor + 3} &= \sum_{j=0}^{k-1} u_{\lfloor \frac{\delta}{k} \rfloor + 3}^j A^j + \sum_{j=0}^{k-1} u_{\lfloor \frac{\delta}{k} \rfloor + 2}^j A^{k+j} + \\ &+ \sum_{j=0}^{k-1-\left(\delta - k\lfloor \frac{\delta}{k} \rfloor\right)} u_{\lfloor \frac{\delta}{k} \rfloor + 1}^j A^{2k+j} + \sum_{j=0}^{\delta - k\lfloor \frac{\delta}{k} \rfloor - 1} u_0^{k-1-j} A^{k\lfloor \frac{\delta}{k} \rfloor + j}. \end{aligned}$$

Both $B_{\lfloor \frac{\delta}{k} \rfloor + 2}$ and $B_{\lfloor \frac{\delta}{k} \rfloor + 3}$ are a nontrivial linear combination of the matrices $I, A, \ldots, A^{\delta + k - 1}$, because (12). This means that $V_{\lfloor \frac{\delta}{k} \rfloor + 2}$ and $V_{\lfloor \frac{\delta}{k} \rfloor + 3}$ are full row rank and therefore

$$\sum_{i=0}^{\lfloor \frac{\delta}{k} \rfloor + 3} \operatorname{rank}(V_i) = n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 3\right).$$

Moreover, since the degree ℓ of $u(D)$ is greater or equal than $\lfloor \frac{\delta}{k} \rfloor + 1$, the degree of $V(D)$ is greater or equal than $3\lfloor \frac{\delta}{k} \rfloor + 4$. Then the last $\lfloor \frac{\delta}{k} \rfloor + 1$ coefficients of $V(D)$, $V_{\lfloor \frac{\delta}{k} \rfloor + 3 + \ell}, \ldots, V_{2\lfloor \frac{\delta}{k} \rfloor + \ell + 3}$ are full row rank due to the same reasons as the first $\lfloor \frac{\delta}{k} \rfloor + 1$ coefficients, and we have that

$$\operatorname{rwt}(V(D)) \geq 2n(\left\lfloor \frac{\delta}{k} \right\rfloor + 2).$$

Case 3: Let us consider that $V_{\lfloor \frac{\delta}{k} \rfloor + 1} \neq 0$ and that $V_{\lfloor \frac{\delta}{k} \rfloor + 2} = 0$.

By following the same reasoning as in the previous case we have that

$$u_2 = u_3 = \cdots = u_{\lfloor \frac{\delta}{k} \rfloor + 1} = 0,$$

$$u_{\lfloor \frac{\delta}{k} \rfloor + 2}^{k-(\delta - k\lfloor \frac{\delta}{k} \rfloor)} = \cdots = u_{\lfloor \frac{\delta}{k} \rfloor + 2}^{k-1} = 0 \tag{13}$$

and

$$\sum_{j=0}^{k-1-\left(\delta-k\left\lfloor\frac{\delta}{k}\right\rfloor\right)}\left(u^j_{\left\lfloor\frac{\delta}{k}\right\rfloor+2}+u_1^{\delta-k\left\lfloor\frac{\delta}{k}\right\rfloor+j}+u_0^{k-1-\left(\delta-k\left\lfloor\frac{\delta}{k}\right\rfloor\right)-j}\right)A^j+$$

$$+\sum_{j=0}^{\delta-k\left\lfloor\frac{\delta}{k}\right\rfloor-1}\left(u_1^j+u_0^{k-1-j}\right)A^{k\left\lfloor\frac{\delta}{k}\right\rfloor+k+j}=0. \quad (14)$$

Therefore,

$$\begin{aligned}B_{\left\lfloor\frac{\delta}{k}\right\rfloor+3}=&\sum_{j=0}^{k-1-\left(\delta-k\left\lfloor\frac{\delta}{k}\right\rfloor\right)}\left(u^j_{\left\lfloor\frac{\delta}{k}\right\rfloor+3}+u_1^{k-1-\left(\delta-k\left\lfloor\frac{\delta}{k}\right\rfloor\right)-j}\right)A^j\\&+\sum_{j=0}^{k-1}u^j_{\left\lfloor\frac{\delta}{k}\right\rfloor+2}A^{k+j}+\sum_{j=0}^{k-1}u_0^{k-1-j}A^{k\left\lfloor\frac{\delta}{k}\right\rfloor+j}\\&+\sum_{j=0}^{\delta-k\left\lfloor\frac{\delta}{k}\right\rfloor-1}u_1^{k-1-j}A^{k\left\lfloor\frac{\delta}{k}\right\rfloor+k+j}+\sum_{j=k-\left(\delta-k\left\lfloor\frac{\delta}{k}\right\rfloor\right)}^{k-1}u^j_{\left\lfloor\frac{\delta}{k}\right\rfloor+3}A^j\end{aligned} \quad (15)$$

which, again is full row rank since $u_0\neq 0$, hence $V_{\left\lfloor\frac{\delta}{k}\right\rfloor+3}$ is full row rank. Analogously to the preceding case, if the degree of $u(D)$ is greater or equal than $\left\lfloor\frac{\delta}{k}\right\rfloor+2$ we have that $V_{2\left\lfloor\frac{\delta}{k}\right\rfloor+3},\dots,V_{2\left\lfloor\frac{\delta}{k}\right\rfloor+\ell+3}$ are full row rank, and

$$\mathrm{rwt}(V(D))\geq 2n\left(\left\lfloor\frac{\delta}{k}\right\rfloor+2\right).$$

If the degree of $u(D)$ is smaller than $\left\lfloor\frac{\delta}{k}\right\rfloor+2$, then by (14) we have that $u(D)=u_0+u_1D$ with $u_0\neq 0$ and $u_1\neq 0$. In this case $V_{\left\lfloor\frac{\delta}{k}\right\rfloor+3+i}=XB_{\left\lfloor\frac{\delta}{k}\right\rfloor+3+i}$ with

$$B_{\left\lfloor\frac{\delta}{k}\right\rfloor+3+i}=\sum_{j=0}^{k-1}u_0^{k-1-j}A^{k\left(\left\lfloor\frac{\delta}{k}\right\rfloor-i\right)+j}+\sum_{j=0}^{k-1}u_1^{k-1-j}A^{k\left(\left\lfloor\frac{\delta}{k}\right\rfloor+1-i\right)+j}$$

for $i=1,2,\dots,\left\lfloor\frac{\delta}{k}\right\rfloor$, which are full row rank. We also have that $V_{2\left\lfloor\frac{\delta}{k}\right\rfloor+4}=XB_{2\left\lfloor\frac{\delta}{k}\right\rfloor+4}$ with

$$B_{2\left\lfloor\frac{\delta}{k}\right\rfloor+4}=\sum_{j=0}^{k-1}u_1^{k-1-j}A^j$$

which is also full rank. Consequently,

$$\mathrm{rwt}(V(D))=\sum_{i=0}^{2\left\lfloor\frac{\delta}{k}\right\rfloor+4}=2n\left(\left\lfloor\frac{\delta}{k}\right\rfloor+2\right).$$

Case 4: Finally, let us assume that$V_{\left\lfloor\frac{\delta}{k}\right\rfloor+1}\neq 0$, $V_{\left\lfloor\frac{\delta}{k}\right\rfloor+2}\neq 0$ and that there exists a set of integers $1\leq i_1<i_2<\cdots<i_R\leq\left\lfloor\frac{\delta}{k}\right\rfloor+1$ such that

$$V_{\left\lfloor\frac{\delta}{k}\right\rfloor+2+i_1}=V_{\left\lfloor\frac{\delta}{k}\right\rfloor+2+i_2}=\cdots=V_{\left\lfloor\frac{\delta}{k}\right\rfloor+2+i_R}=0.$$

and $V_{\lfloor \frac{\delta}{k} \rfloor +2+j} \neq 0$ for $j \in \{1, 2, \ldots, \lfloor \frac{\delta}{k} \rfloor + 1\} \setminus \{i_1, i_2, \ldots, i_R\}$.
Note that $R \leq \lfloor \frac{\delta}{k} \rfloor + 1$, therefore we have that

$$\sum_{j=\lfloor \frac{\delta}{k} \rfloor +3}^{2\lfloor \frac{\delta}{k} \rfloor +3} \operatorname{rank}(V_j) = n \left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1 - R \right).$$

When we assume that $V_{\lfloor \frac{\delta}{k} \rfloor +2+i_R} = 0$, as a consequence of (10) we have that

$$u_{2i_R+1} = -\hat{u_0} \neq 0 \quad \text{where} \quad \hat{u_0} = u_0 \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix}.$$

Thus it is easy to see that the degree ℓ of $u(D)$ is such that $\ell \geq 2i_R+1 \geq 2R+1$ and therefore, the degree of $V(D) = \psi(u(D)G(D))$ is $2\lfloor \frac{\delta}{k} \rfloor + 3 + \ell \geq 2\lfloor \frac{\delta}{k} \rfloor + 2R+4$. Then the last R coefficients of $V(D)$ are nonzero due to the same reasons as in Theorem 4.1, and we obtain that

$$\operatorname{rwt}(V(D)) \geq 2n \left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2 \right).$$

By proving these four cases we finally have that $\mathcal{C}$ is MRD.

□

The next example presents an MRD convolutional code that it is possible to build using the construction proposed in Section 4.2.

Example 4.2. *Consider the companion matrix*

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \in \mathbb{F}_2^{4\times 4}$$

of the irreducible polynomial $\chi(\lambda) = \lambda^4 + \lambda + 1 \in \mathbb{F}_2[\lambda]$ and the full row rank matrix

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

Let $\delta = 1$ and $k = 3$ (note that $\delta = m - k$ and that $k \nmid m$).

The rank metric convolutional code with encoder $G(D) = G_0 + G_1 D + G_2 D^2 + G_3 D^3$ with

$$G_0 = \begin{bmatrix} \psi^{-1}(X) \\ \psi^{-1}(XA) \\ \psi^{-1}(XA^2) \end{bmatrix} = \left[\begin{array}{cccc|cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{array}\right],$$

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

$$\begin{aligned} G_2 &= \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_1 \\ &= \begin{bmatrix} \psi^{-1}(XA) \\ \psi^{-1}(X) \\ \psi^{-1}(XA^3) \end{bmatrix} = \left[\begin{array}{cccc|cccc|cccc} 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}\right], \end{aligned}$$

and

$$\begin{aligned} G_3 = \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} G_0 &= \begin{bmatrix} \psi^{-1}(XA^2) \\ \psi^{-1}(XA) \\ \psi^{-1}(X) \end{bmatrix} \\ &= \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right], \end{aligned}$$

is a $(3 \times 4, 1, 9)$ *MRD convolutional code.*

In the case that $k \nmid m$, the construction presented in this subsection allows one to obtain an $(n \times m, k, \delta)$ MRD convolutional code for $\delta \leq \left(2\left\lfloor \frac{m}{k} \right\rfloor + 1\right)k$. The case when $k \mid m$ was presented in the previous subsection.

Acknowledgement

This work was supported by The Center for Research and Development in Mathematics and Applications (CIDMA) through the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e Tecnologia), references UIDB/04106/2020. The first author was supported by Spanish grants PID2019-108668GB-I00 of the Ministerio de Ciencia e Innovación of the Gobierno de España.

References

[1] P. Almeida, U. Martínez-Peñas, and D. Napp. Systematic maximum sum rank codes. *Finite Fields and Their Applications*, 65:101677, 2020.

[2] P. Almeida and D. Napp. A new rank metric for convolutional codes. *Designs, Codes and Cryptography*, 89:53–73, 2021.

[3] A. Badr, A. Khisti, and R. Mahmood. Convolutional codes with maximum column sum rank for network streaming. *IEEE Trans. Inform. Theory*, 62(6):3039–3052, 2016.

[4] D. Bartoli, G. Marino, and Neri. New MRD codes from linear cutting blocking sets. *Annali di Matematica*, 202:115–142, 2023.

[5] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory*, 25(3):226–241, 1978.

[6] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–12, 1985.

[7] F. Gantmacher. *The Theory of Matrices, vol.I.* Chelsea Publishing Company, New York, 1977.

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

[9] A. Gruica and A. Ravagnani. Common complements of linear subspaces and the sparseness of MRD codes. *SIAM Journal on Applied Algebra and Geometry*, 6(2):79–110, 2022.

[10] A. Horlemann-Trautmann and K. Marshall. New criteria for MRD and Gabidulin codes and some rank-metric code constructions. *Advances in Mathematics of Communications*, 11(3):533–548, 2017.

[11] T. Kailath. *Linear Systems.* Englewood Cliffs, N.J., Prentice Hall, 1980.

[12] R. Koetter and F. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, 2008.

[13] H. Lidl, R.and Niederreiter. *Introduction to finite fields and their applications (2nd ed.).* Cambridge University Press., Cambridge, 1994.

[14] F. J. MacWilliams and N. J.A. Sloane. *The Theory of Error-Correcting Codes.* North Holland, Amsterdam, 1977.

[15] R. Mahmood, A. Badr, and A. Khisti. Streaming-codes for multicast over burst erasure channels. *IEEE Trans. Inform. Theory*, 61(8):4181–4208, 2015.

[16] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori. Rank metric convolutional codes. *Proceedings of the 22nd International Symposium on Mathematical Theory of Network and Systems (MTNS), Minnesota, USA*, 2016.

[17] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori. MRD rank metric convolutional codes. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pages 2766–2770, 2017.

[18] D. Napp and R. Smarandache. Constructing strongly MDS convolutional codes with maximum distance profile. *Advances in Mathematics of Communications*, 10(2):275–290, 2016.

[19] R.W. Nóbrega and B.F. Uchoa-Filho. Multishot codes for network coding using rank-metric codes. In *Wireless Network Coding Conference (WiNC), 2010 IEEE*, pages 1–6, 2010.

[20] D. Napp; R. Pinto and V. Sidorenko. Concatenation of convolutional codes and rank metric codes for multi-shot network coding. *Springer Science+Business Media New York*, 86:303–318, 2017.

[21] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput*, 10(1):15–32, 1999.

[22] V. Sidorenko, M. Stinner, and A. Wachter-Zeh. Convolutional codes in rank metric with application to random network coding. *IEEE Trans. Inform. Theory*, 61(6):3199–3213, 2015.

[23] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions for MDS convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001.