MRD Rank Metric Convolutional Codes

Diego Napp*, Raquel Pinto*, Joachim Rosenthal†, and Paolo Vettori*

*Department of Mathematics, University of Aveiro
3810-197 Aveiro, Portugal
Email: {diego, raquel, pvettori} at ua.pt
†Department of Mathematics, University of Zurich
Winterthurstrasse 190, CH-8057 Zürich, Switzerland
Email: rosenthal at math.uzh.ch

Abstract—So far, in the area of Random Linear Network Coding, attention has been given to the so-called one-shot network coding, meaning that the network is used just once to propagate the information. In contrast, one can use the network more than once to spread redundancy over different shots. In this paper, we propose rank metric convolutional codes for this purpose. The framework we present is slightly more general than the one which can be found in the literature. We introduce a rank distance, which is suitable for convolutional codes, and derive a new Singleton-like upper bound. Codes achieving this bound are called Maximum Rank Distance (MRD) convolutional codes. Finally, we prove that this bound is optimal by showing a concrete construction of a family of MRD convolutional codes.

I. INTRODUCTION

Random Linear Network Coding (RLNC), as introduced in [1], provides the mathematical foundation for multicast communications and, in particular, for networks with unknown or changing topology. In this scenario, networks operate with packets. If one considers a packet as a row of a matrix with entries in a finite field, then the linear combinations performed in the nodes are row operations on this matrix. For perfect communications, the row space of the transmitted matrix remains unchanged. RLNC has since then opened a major research area in communications with widespread applications to wireless networks, internet or cloud computing. Most of the large body of literature in this area is concerned with the so-called one-shot network coding, meaning that the unknown structure of the network is used once to disseminate the information.

As opposed to this situation, coding can also be performed over multiple uses of the network, whose internal structure may change at each shot, giving rise to the so-called multi-shot coding. In fact, it has been recently shown that spreading redundancy among the transmitted codewords (row spaces) at different instances (shots) can improve the error-correction capabilities of the code [2]–[4].

To this end, in this work we propose to use rank metric convolutional codes, as this class of codes allows to create dependencies between data streams in a quite simple way. In this setting, an extension of the standard rank metric over multiple shots, which is analogous to the extended subspace distance defined in [2], will provide the proper measure for the number of rank erasures that a code can tolerate. We point out that this more involved multi-shot framework has proven to cope with network streaming applications with tight latency constrains (see [4] and the references therein).

The framework presented in this paper is slightly more general than the existing one in the literature on rank metric convolutional codes, which is mainly based (see [3], [4]) on rank metric Gabidulin codes [7]. Indeed, as proposed in [8], we shall define rank metric codes for all rates and fields.

In this contribution, we aim to further explore this approach. Specifically, after recalling some basic facts about convolutional and rank metric codes, we introduce a first general definition of rank metric convolutional codes, we propose a suitable concept of distance, and we study the Singleton-like bound for this class of codes. To conclude, we provide a family of rank metric convolutional codes, by direct construction, which achieves the Singleton bound.

II. CONVOLUTIONAL CODES

Let \( \mathbb{F}_q \) be a finite field and \( \mathbb{F}_q[D] \) be the ring of polynomials with coefficients in \( \mathbb{F}_q \). A convolutional code \( \mathcal{C} \) of rate \( k/n \) is
a rank \( k \) \( F_q[D] \)-submodule of \( F_q[D]^n \). If \( G(D) \in F_q[D]^{k \times n} \) is a full row rank matrix such that
\[
\mathcal{C} = \text{Im}_{F_q[D]} G(D) = \{ u(D) G(D) : u(D) \in F_q[D]^k \},
\]
then \( G(D) \) is called an encoder of \( \mathcal{C} \).

Any other encoder \( \tilde{G}(D) \) of \( \mathcal{C} \) differs from \( G(D) \) by a unimodular matrix \( U(D) \in F_q[D]^{k \times k} \), i.e., \( \tilde{G}(D) = U(D) G(D) \). Therefore, we can consider \( G(D) \) to be minimal, i.e., in row reduced form.\(^1\) In this case, the sum of the row degrees of \( G(D) \) attains its minimum among all the encoders of \( \mathcal{C} \), which is usually denoted by \( \delta \) and called the degree of \( \mathcal{C} \).

A rate \( k/n \) convolutional code \( \mathcal{C} \) of degree \( \delta \) is called an \((n,k,\delta)\) convolutional code [5].

An important distance measure for a convolutional code \( \mathcal{C} \) is its free distance \( d_{\text{free}}(\mathcal{C}) \) defined as
\[
d_{\text{free}}(\mathcal{C}) = \min_{v(D) \in \mathcal{C}, v(D) \neq 0} \text{wt}(v(D)),
\]
where \( \text{wt}(v(D)) \) is the Hamming weight of a polynomial vector
\[
v(D) = \sum_{i \in \mathbb{N}} v_i D^i \in F_q[D]^n,
\]
defined as
\[
\text{wt}(v(D)) = \sum_{i \in \mathbb{N}} \text{wt}(v_i),
\]
being \( \text{wt}(v_i) \) the number of the nonzero components of \( v_i \).

In [6], Rosenthal and Smarandache showed that the free distance of an \((n,k,\delta)\) convolutional code is upper bounded by
\[
d_{\text{free}}(\mathcal{C}) \leq \left( n - k \right) \left( \left\lceil \frac{\delta}{k} \right\rceil + 1 \right) + \delta + 1.
\]
This bound was called the generalized Singleton bound since it generalizes in a natural way the Singleton bound for block codes (when \( \delta = 0 \)). An \((n,k,\delta)\) convolutional code whose free distance is equal to the generalized Singleton bound is called maximum distance separable (MDS) code [6].

### III. RANK METRIC CODES

Let \( A,B \in F_q^{n \times m} \). It is known [7] that
\[
d_{\text{rank}}(A,B) = \text{rank}(A - B)
\]
defines a distance, called rank distance, between \( A \) and \( B \). Therefore, any subset of \( F_q^{n \times m} \) equipped with this distance is a rank metric code.

In particular, an \((n \times m,k)\) linear rank metric code \( \mathcal{C} \subset F_q^{n \times m} \) of rate \( k/\min(n,m) < 1 \) is the image of a monomorphism \( \varphi : F_q^k \rightarrow F_q^{n \times m} \). We write \( \varphi = \psi \circ \gamma \) as a composition of an isomorphism \( \psi \) and a monomorphism \( \gamma \):
\[
\varphi : F_q^k \xrightarrow{\gamma} F_q^{n \times m} \xrightarrow{\psi} F_q^{m \times n}
\]
\[
u \mapsto u \xmapsto{\gamma} v \xmapsto{\psi} \psi(v)
\]
\(^1\)The polynomial matrix \( G(D) \in F_q[D]^{k \times n} \) is in row reduced form if it has a full row rank leading row coefficient matrix \( G_{\text{rc}} \), whose entries are the coefficients of the powers with highest degree (called row degree) in each row of \( G \).

where \( G \in F_q^{k \times m} \). If \( \psi = \text{rowmat}_{n \times m} \), the rows of \( V \) are simply the \( n \) consecutive blocks with \( m \) elements of \( v \).

As usual, the rank distance of the code, \( d_{\text{rank}}(\mathcal{C}) \), is the minimum distance between nonzero codewords.

In the following, we will assume that \( n \leq m \) (but analogous results can be given for the other case). Also for this class of codes, a Singleton-like bound exists, which provides a limit for the value of the code distance.

**Theorem 1.** The rank distance of an \((n \times m,k)\) linear rank metric code is upper bounded by
\[
d_{\text{rank}}(\mathcal{C}) \leq n - \left\lceil \frac{k-1}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor + 1.
\]

**Proof:** It follows directly from the fact (see for instance [7]) that
\[
\log_q|\mathcal{C}| \leq \max\{n,m\} \left( \min\{n,m\} - d_{\text{rank}}(\mathcal{C}) + 1 \right).
\]

---

**IV. RANK METRIC CONVOLUTIONAL CODES**

In this section we will define rank metric convolutional codes whose codewords are polynomials matrices in \( F_q[D]^{n \times m} \).

The rank weight of a polynomial matrix \( A(D) = \sum_{i \in \mathbb{N}} A_i D^i \in F_q[D]^{n \times m} \) is given by
\[
\text{rkwt}(A(D)) = \sum_{i \in \mathbb{N}} \text{rank}(A_i).
\]

If \( B(D) = \sum_{i \in \mathbb{N}} B_i D^i \in F_q[D]^{n \times m} \), we define the sum rank distance between \( A(D) \) and \( B(D) \) as
\[
d_{\text{SR}}(A(D),B(D)) = \text{rkwt}(A(D) - B(D))
\]
\[
= \sum_{i \in \mathbb{N}} \text{rank}(A_i - B_i).
\]

**Lemma 2.** The sum rank distance \( d_{\text{SR}} \) is a distance in \( F_q[D]^{n \times m} \).

**Proof:** Obviously \( d_{\text{SR}}(A(D),B(D)) = d_{\text{SR}}(B(D),A(D)) \) and \( d_{\text{SR}}(A(D),B(D)) \geq 0 \) with \( d_{\text{SR}}(A(D),B(D)) = 0 \) iff \( A(D) = B(D) \). Further, as \( \text{rank}(X+Y) \leq \text{rank}(X) + \text{rank}(Y) \) for any \( X,Y \in F_q^{n \times m} \), then the triangular inequality readily follows,
\[
d_{\text{SR}}(A(D),B(D)) = \sum_{i \in \mathbb{N}} \text{rank}(A_i - B_i)
\]
\[
\leq \sum_{i \in \mathbb{N}} \text{rank}(A_i - C_i) + \text{rank}(C_i - B_i)
\]
\[
= d_{\text{SR}}(A(D),C(D)) + d_{\text{SR}}(C(D),B(D)),
\]
for any \( C(D) = \sum_{i \in \mathbb{N}} C_i D^i \in F_q[D]^{n \times m} \).

A rank metric convolutional code \( \mathcal{C} \subset F_q[D]^{n \times m} \) is the image of an homomorphism \( \varphi : F_q[D]^k \rightarrow F_q[D]^{n \times m} \). We write \( \varphi = \psi \circ \gamma \) as a composition of a monomorphism \( \gamma \) and an isomorphism \( \psi \):
\[
\varphi : F_q[D]^k \xrightarrow{\gamma} F_q[D]^{n \times m} \xrightarrow{\psi} F_q[D]^{n \times m}
\]
\[
u \mapsto u \xmapsto{\gamma} v \xmapsto{\psi} \psi(v)
\]
where \( G \in F_q^{k \times m} \). If \( \psi = \text{rowmat}_{n \times m} \), the rows of \( V \) are simply the \( n \) consecutive blocks with \( m \) elements of \( v \).
where \( G(D) \in \mathbb{F}_q^{k \times nm} \) is a full row rank polynomial matrix, called encoder of \( \mathcal{C} \), and we may choose, as before, \( V(D) = \text{rowmat}_{n \times m}(v(D)) \), such that \( V(D) \rightarrow \text{wt}_{m \times n}(V(D)) \).

As for convolutional codes, two encoders of \( \mathcal{C} \) differ by left multiplication by a unimodular matrix and therefore \( \mathcal{C} \) always admits minimal encoders (i.e., in row reduced form). The degree of a rank metric convolutional code \( \mathcal{C} \) is the sum of the row degrees of a minimal encoder of \( \mathcal{C} \), i.e., the minimum value of the sum of the row degrees of its encoders.

A rank metric convolutional code \( \mathcal{C} \) of degree \( \delta \), defined as in (4), is called an \((n \times m, k, \delta)\)-rank metric convolutional code.

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

\[
d_{SR}(\mathcal{C}) = \min_{D \neq U(D)} d_{SR}(V(D), U(D))
\]

Next theorem, which establishes the Singleton-like bound for rank metric convolutional codes, can be found in [8]. We present its proof for completeness.

**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

\[
d_{SR}(\mathcal{C}) \leq n \left( \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) - \left\lfloor \frac{k}{m} \right\rfloor + 1. \tag{5}
\]

**Proof:** Let \( G(D) \) be a minimal encoder of \( \mathcal{C} \) with row degrees \( \nu_0, \nu_1, \ldots, \nu_{k-1} \). Let \( v = \min\{ \nu_i : 0 \leq i < k \} \) denote the value of the smallest row degree and \( t \) the number of indexes \( \nu_i \) among the indexes \( \nu_0, \nu_1, \ldots, \nu_{k-1} \) having the value \( v \). We shall assume, without loss of generality, that the row degrees of \( G(D) \) are in nonincreasing order, i.e.,

\[
v_0 \geq \cdots \geq \nu_{k-t-1} > \nu_{k-t} = \cdots = \nu_{k-1} = v
\]

and that \( v = \text{rowmat}_{n \times m}(v) \) in (4).

Now take a nonzero and constant \( u(D) = u = (0, \ldots, 0, u_{k-t}, \ldots, u_k) \in \mathbb{F}_q^k \); note that, due to this choice of \( u(D) \), the degree of \( V(D) = u(D)G(D) \) goes up to \( v \) and not to \( \nu_0 \), being \( \nu_0 = \nu_1 + \nu_2 D + \nu_3 D^2 + \cdots + \nu_k D^k \). Denote \( V(D) = \psi(V(D)) = V_0 + V_1 D + \cdots + V_{k-t} D^{k-t} \). Observe that \( v_0 = uG(0) \) is a linear combination of the last \( t \) rows of \( G(0) \), thus we can select \( u_{k-t}, \ldots, u_k \) such that the first \( t-1 \) components of \( v_0 \) are zero. Therefore, also the first \( \left\lceil \frac{m}{1} \right\rceil \) rows of \( V_0 = \psi(v_0) \) are zero, which implies that \( \text{rank}(V_0) \leq n - \left\lceil \frac{m}{1} \right\rceil = n - \left\lfloor \frac{m}{m} \right\rfloor + 1 \). Thus,

\[
\text{rank}(V(D)) = \sum_{0 \leq i < v} \text{rank}(V_i) \\
\leq n - \left\lfloor \frac{m}{m} \right\rfloor + 1 + n v \\
= n(v + 1) - \left\lfloor \frac{m}{m} \right\rfloor + 1.
\]

This upper bound is maximized when \( v \) is as large as possible and \( t \) as small as possible. It can be checked that, for given \( k \) and \( \delta = \sum_{0 \leq i < k} \nu_i \), these values are \( v = \left\lfloor \frac{\delta}{k} \right\rfloor \) and \( t = k \left( \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) - \delta \). This concludes the proof.

A rank metric convolutional code whose degree attains the upper bound (5) is called maximum rank distance (MRD) convolutional code. Next corollary gives a necessary condition on the rows of a minimal encoder of a rank metric convolutional code \( \mathcal{C} \) so it can be MRD, and it follows immediately from the proof of Theorem 3.

**Corollary 4.** Let \( \mathcal{C} \) be a \((n \times m, k, \delta)\)-rank metric convolutional code and \( G(D) \in \mathbb{F}_q^k \) a minimal encoder of \( \mathcal{C} \). Then if \( \mathcal{C} \) is MRD, \( G(D) \) must have \( k \left( \left\lfloor \frac{\delta}{k} \right\rfloor + 1 \right) - \delta \) rows of degree \( \left\lfloor \frac{\delta}{k} \right\rfloor \) and \( \delta - k \left\lceil \frac{\delta}{k} \right\rceil \) rows of degree \( \left\lceil \frac{\delta}{k} \right\rceil + 1 \).

**V. Construction of MRD Convolutional Codes**

In this section we will show that MRD rank metric convolutional codes exist, thus proving that bound (5) is optimal. We begin considering a simple particular case, which may help to understand the following general construction.

Let \( \mathbb{F}_q \) be a finite field and \( A \in \mathbb{F}_q^{m \times m} \) a matrix with irreducible characteristic polynomial \( z(A) \). Note that \( A^i \), \( 0 \leq i < m \), are linearly independent over \( \mathbb{F}_q \) and

\[
\mathbb{F}_q[A] = \left\{ \sum_{i=0}^{m-1} u_i A^i : u_i \in \mathbb{F}_q, i = 0, \ldots, m-1 \right\} \simeq \mathbb{F}_q^m \tag{6}
\]

is a field.

We will prove that, whenever \( m > \delta \), the \((m \times m, 1, \delta)\)-rank metric convolutional code \( \mathcal{C} \) generated by

\[
G(D) = \sum_{i=0}^{\delta} \psi^{-1}(A^i) D^i \in \mathbb{F}_q[D]^{1 \times m^2} \tag{7}
\]

is MRD. In other words, its sum rank distance achieves the upper bound (5) given in Theorem 3, which in this case is equal to \( m(\delta + 1) \).

Actually, we will show that for any nonzero \( u(D) \in \mathbb{F}_q[D] \) the codeword \( V(D) = \phi(u(D)) \) has rank weight \( \text{rkwt}(V(D)) \geq m(\delta + 1) \).

Let \( u(D) = \sum_{i \in \mathbb{N}} u_i D^i \) be a nonzero polynomial. Without loss of generality, we may suppose that \( u_0 \neq 0 \). Then, the first \( \delta + 1 \) coefficients of \( V(D) = \gamma(u(D)) = u(D)G(D) \) are thus given by

\[
v_i = \sum_{l=0}^{i} u_{l-i} G_l = \sum_{l=0}^{i} u_{l-i} \psi^{-1}(A^l) \\
= \psi^{-1} \left( \sum_{l=0}^{i} u_{l-i} A^l \right), \ i \leq \delta,
\]

due to linearity of \( \psi^{-1} \). It follows that the polynomial matrix \( V(D) = \psi(V(D)) \) has coefficients

\[
v_i = \psi(v_i) = \psi \left( \psi^{-1} \left( \sum_{l=0}^{i} u_{l-i} A^l \right) \right) \\
= \sum_{l=0}^{i} u_{l-i} A^l \in \mathbb{F}_q[A], \ i \leq \delta.
\]
Since the powers of $A$ with degree less than $m$ form a basis of $\mathbb{F}_q[A]$ over $\mathbb{F}_q$ and the scalar $u_0 \neq 0$ shows up in every linear combination, then $V_i \neq 0$ for every $i \leq \delta < m$. Being elements of a field, nonzero matrices are invertible and so have rank $m$. Therefore,

$$\text{rkwt}(V(D)) = \sum_{i \in \mathbb{N}} \text{rank} V_i \geq \delta \cdot \text{rank} V_i = m(\delta + 1).$$

(9)

Next example illustrates the reasoning above.

**Example 5.** Consider the companion matrix $A$ of the irreducible polynomial $\chi(\lambda) = \lambda^3 + \lambda + 1 \in \mathbb{F}_2[\lambda],$

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

and the rank metric convolutional code $\mathcal{C}$ with encoder $G(D) = \psi^{-1}(I) A^T D = \psi^{-1}(I + AD) \in \mathbb{F}_2^{3 \times q}$.

For the sake of simplicity, let $\psi = \text{rowmat}_{m \times m}$ (folding a row vector into a matrix), thus $\psi^{-1}$ is the ‘rowvec’ map (unfolding a matrix into a row vector). This means that

$$G(D) = \begin{bmatrix} 1 & D & 0 & 0 \\ 0 & 1 & D & D \\ 1 & 1 & 0 \end{bmatrix}. $$

Since $m = 3 > \delta = 1$, it follows that $\mathcal{C}$ is an MRD $(3 \times 3, 1, 1)$-rank metric convolutional code, with distance equal to the upper bound (5), i.e., $d_{SR}(\mathcal{C}) = m(\delta + 1) = 6$, as we will show.

Observe that, due to the rather simple structure of the code, its codewords are

$$V(D) = \varphi(u(D)) = \psi(u(D)G(D)) = u(D)\psi(G(D)) = u(D)(I + AD).$$

Furthermore, notice that any message starting with a nonzero coefficient is equal either to (a) $u(D) = 1 + \bar{u}(D)D^2$ or to (b) $u(D) = 1 + \bar{u}(D)D^2$, for some $\bar{u}(D) \in \mathbb{F}_2[D]$.

As a consequence, every codeword in $\mathcal{C}$ must be of the form

$$V(D) = (1 + \bar{u}(D)D^2)(I + AD) = I + AD + \bar{V}(D)D^2$$

(a)

or of the form

$$V(D) = (1 + D + \bar{u}(D)D^2)(I + AD) = I + (I + A)D + \bar{V}(D)D^2,$$

(b)

for some $\bar{V}(D) \in \mathbb{F}_2[D]^{3 \times 3}$. So, since in both cases the first two coefficients of $V(D)$ ($V_0 = I$ and $V_1 = A$ or $V_1 = I + A = A^3$) are nonzero, thus full rank matrices (invertible in the field $\mathbb{F}_2[A]$), the rank weight of any codeword of $\mathcal{C}$ is

$$\text{rkwt}(V(D)) = \text{rank} V_0 + \text{rank} V_1 + \text{rkwt}(\bar{V}(D)) \geq 6.$$
Therefore, for this construction, the choice of \( \psi \) presented in (10) will have (full row) rank \( k \) of \( \phi \), i.e.,

\[
\begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0
\end{bmatrix}
\]