22nd International Symposium on
Mathematical Theory of Networks and Systems
July 11-15, 2016. Minneapolis, MN, USA

Rank metric convolutional codes

Diego Napp[1], Raquel Pinto[1], Joachim Rosenthal[2], and Paolo Vettori[1]

***Abstract*— In this contribution, we propose a first general definition of rank-metric convolutional codes for *multi-shot* network coding. To this aim, we introduce a suitable concept of distance and we establish a generalized Singleton bound for this class of codes.**

I. INTRODUCTION

Most of the theory of Random Linear Network Coding developed so far is concerned with the so-called non-coherent one-shot network coding [1], meaning that the random (i.e., unknown) structure of the net is used just once to propagate information.

However, 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 particular, creating dependencies among the transmitted codewords of different shots can improve the error-correction capabilities [2].

To attain this goal, we propose to use rank-metric convolutional codes, as this type of codes permits adding complex dependencies to data streams in a quite simple way (see [3] for the particular case of unit memory convolutional codes). In this case, 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. It is worth mentioning that this approach has been recently used to cope very efficiently with network streaming applications such as video streaming (see [4] and the references therein).

In this extended abstract, we aim to further explore this direction. Specifically, after recalling some basic facts about convolutional and rank metric codes, we introduce a new general definition of rank-metric convolutional codes, we propose a suitable concept of distance, and we determine the Singleton bound for this class of codes.

II. CONVOLUTIONAL CODES

Let $\mathbb{F}_q$ be a finite field of order q and $\mathbb{F}_q[D]$ be the ring of polynomials with coefficients in $\mathbb{F}_q$.

A *convolutional code* $\mathscr{C}$ of rate k/n is an $\mathbb{F}_q[D]$-submodule of $\mathbb{F}_q[D]^n$ of rank k given by an *encoder matrix* $G(D) \in \mathbb{F}_q[D]^{k\times n}$ through

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

We shall consider only *basic* and *minimal* encoders, where *basic* means that $G(D)$ has a polynomial right inverse, and *minimal* means that the value of the sum of the row degrees of $G(D)$ attains its minimum δ, called the *degree* of $\mathscr{C}$.[1]

A rate k/n convolutional code $\mathscr{C}$ of degree δ is called an (n,k,δ) *convolutional code* [5].

Notice that also a dual description of a convolutional code $\mathscr{C}$ can be given through a *parity-check* matrix which is an $(n-k)\times n$ full rank polynomial matrix $H(D) = H_0 + H_1 D + \cdots + H_m D^m$ such that

$$\mathscr{C} = \ker H(D) = \left\{ v(D) \in \mathbb{F}_q[D]^n : H(D)v(D) = 0 \in \mathbb{F}_q[D]^{n-k} \right\}.$$

A measure of the error detecting or correcting capabilities of a convolutional code $\mathscr{C}$ is given by the *free distance* $d_{\text{free}}(\mathscr{C})$, defined as

$$d_{\text{free}}(\mathscr{C}) = \min\{\mathrm{wt}(v(D)) \quad | \quad v(D) \in \mathscr{C} \quad \text{and} \quad v(D) \neq 0\},$$

where $\mathrm{wt}(v(D))$ is the Hamming weight of a polynomial vector

$$v(D) = \sum_{i\in\mathbb{N}} v_i D^i \in \mathbb{F}_q[D]^n,$$

defined as

$$\mathrm{wt}(v(D)) = \sum_{i\in\mathbb{N}} \mathrm{wt}(v_i),$$

being $\mathrm{wt}(v_i)$ the number of the nonzero components of v_i.

In [6], Rosenthal and Smarandache showed that the free distance of an (n,k,δ) *convolutional code* is upper bounded by

$$d_{\text{free}}(\mathscr{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{1}$$

This bound was called the *generalized Singleton bound* since it generalizes in a natural way the Singleton bound for block codes (when $\delta = 0$): *code distance* $\leq n-k+1$. An (n,k,δ) *convolutional code* whose free distance is equal to the generalized Singleton bound is called a *maximum distance separable* (MDS) code [6].

[1]Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal, email: {diego,raquel,pvettori} at ua.pt This work was supported in part by the Portuguese Foundation for Science and Technology (FCT-Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UID/MAT/04106/2013.

[2]Department of Mathematics University of Zurich, Winterthurstrasse 190, CH-8057 Zürich, Switzerland, email: rosenthal at math.uzh.ch

[1]Therefore, the *degree* δ of a convolutional code $\mathscr{C}$ is the sum of the row degrees of one, and hence any, minimal basic encoder.

III. RANK METRIC CODES

Let $A,B \in \mathbb{F}_q^{n\times m}$. It is known [7] that

$$d_{\text{rank}}(A,B) = \text{rank}(A-B) \tag{2}$$

is a distance between A and B, called *rank distance*. Therefore, any subset of $\mathbb{F}_q^{n\times m}$ equipped with this distance is a rank metric code.

In particular, an $(n\times m,k)$ *linear rank metric code* $\mathscr{C} \subset \mathbb{F}_q^{n\times m}$ of rate k/nm is the image of a monomorphism $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^{n\times m}$. We write $\varphi = \phi \circ \psi$ as a composition of a monomorphism ψ and an isomorphism ϕ.

$$\begin{array}{rcccc} \varphi : \mathbb{F}_q^k & \xrightarrow{\psi} & \mathbb{F}_q^{nm} & \xrightarrow{\phi} & \mathbb{F}_q^{n\times m} \\ u & \mapsto v=(v_0,\ldots,v_{nm-1}) = uG & \mapsto & V=\phi(v) & \end{array}$$

where $G \in \mathbb{F}_q^{k\times nm}$ and we let, for instance, $[V_{ij}] = v_{i+nj}$, where $0 \le i < n$ and $0 \le j < m$. As usual, the rank distance of the code, $d_{\text{rank}}(\mathscr{C})$, is the minimum distance between nonzero codewords.

In the following, we shall assume that $n \le m$ (but analogous results can be given for the other case). Then, it is not too difficult to find the expression for the Singleton bound, which is shown next.

Theorem 3.1: The rank distance of an $(n\times m,k)$ *linear rank metric code* is upper bounded by

$$d_{\text{rank}}(\mathscr{C}) \le n - \left\lfloor \frac{k-1}{m} \right\rfloor = n - \left\lceil \frac{k}{m} \right\rceil + 1. \tag{3}$$

Proof: It follows directly from the fact (see for instance [7]) that

$$\log_q |\mathscr{C}| \le \max\{n,m\}(\min\{n,m\} - d_{\text{rank}}(\mathscr{C}) + 1).$$

■

IV. RANK METRIC CONVOLUTIONAL CODES

Let $A(D) = \sum_{i\in\mathbb{N}} A_i D^i, B(D) = \sum_{i\in\mathbb{N}} B_i D^i \in \mathbb{F}_q^{n\times m}[D]$. We define the *sum-rank distance* between $A(D)$ and $B(D)$ as

$$d_{\text{SR}}(A(D),B(D)) = \sum_{i\in\mathbb{N}} \text{rank}(A_i - B_i) \tag{4}$$

Lemma 4.1: The sum-rank distance d_{SR} is actually a distance in $\mathbb{F}_q^{n\times m}[D]$.

Proof: Obviously $d_{\text{SR}}\big(A(D),B(D)\big) = d_{\text{SR}}\big(B(D),A(D)\big)$ and $d_{\text{SR}}\big(A(D),B(D)\big) \ge 0$ with $d_{\text{SR}}\big(A(D),B(D)\big) = 0$ iff $A(D) = B(D)$. Further, as $\text{rank}(X+Y) \le \text{rank}(X) + \text{rank}(Y)$ for any $X,Y \in \mathbb{F}_q^{n\times m}$, then the triangular inequality readily follows,

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

■

A *rank metric convolutional code* $\mathscr{C} \subset \mathbb{F}_q^{n\times m}$ of rate k/nm is the image of an homomorphism $\varphi : \mathbb{F}_q[D]^k \to \mathbb{F}_q[D]^{n\times m}$ provided with the sum-rank distance.

As for rank metric codes, we write $\varphi = \phi \circ \psi$ as a composition of a monomorphism ψ and an isomorphism ϕ.

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

where $G(D) \in \mathbb{F}_q^{k\times nm}$ is the *encoder* of $\mathscr{C}$, and $V_{ij}(D) = v_{i+nj}(D)$ and $v(D) = (v_0(D),\ldots,v_{nm-1}(D))$.

In order to avoid catastrophic encoders we assume that the encoder $G(D)$ is *basic*. Moreover, note that minimality (i.e. the row reduced form) of the encoder $G(D)$ can always be achieved by left multiplication with an unimodular matrix $U(D)$, since both $G(D)$ and $\hat{G}(D) = U(D)G(D)$ have the same image. Therefore, without loss of generality, we may consider $G(D)$ to be *minimal* with minimum degree δ (sum of the row degrees of $G(D)$).

In this case, all the parameters defining the code $\mathscr{C}$ can be resumed by saying that it is an $(n\times m,k,\delta)$ *rank metric convolutional code*.

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

$$\begin{aligned} d_{\text{SR}}(\mathscr{C}) &= \min_{V(D),U(D)\in\mathscr{C} \text{ and } V(D)\neq U(D)} d_{\text{SR}}\big(V(D),U(D)\big) \\ &= \min_{0\neq V(D)\in\mathscr{C}} \text{rank}\big(V(D)\big) \end{aligned}$$

We are now in a position to obtain an upper bound on the sum-rank distance of a rank metric convolutional code.

Theorem 4.1: Let $\mathscr{C}$ be an $(n\times m,k,\delta)$ *rank metric convolutional code*. Then, the sum-rank distance of $\mathscr{C}$ is upper bounded by

$$d_{\text{SR}}(\mathscr{C}) \le n\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \left\lceil \frac{k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \delta}{m} \right\rceil + 1. \tag{5}$$

Proof: Let $\nu_1,\nu_2,\ldots,\nu_k$ be the row degrees of $G(D)$ and $\nu = \min\{\nu_1,\nu_2,\ldots,\nu_k\}$ denote the value of the smallest row degree. Finally, let t be the number of indexes ν_i among the indexes $\nu_1,\nu_2,\ldots,\nu_k$ having the value ν. Without loss of generalization, let $\nu_1 \ge \nu_2 \ge \cdots \ge \nu_{k-t} = \cdots = \nu_k = \nu$ and $G(D) = G_0 + G_1 D + G_2 D^2 + \cdots + G_{\nu_1} D^{\nu_1}$. Take $u(D) = u = (0,\ldots,0,u_{k-t},\ldots,u_k) \in \mathbb{F}_q^k$ constant to obtain $uG(D) = v(D) = v_0 + v_1 D + v_2 D^2 + \cdots + v_\nu D^\nu$ (note that the degree of $v(D)$ is bounded by ν and not by ν_1). Denote $V(D) = \phi(v(D)) = V_0 + V_1 D + \cdots + V_\nu D^\nu$. As $G(D)$ is basic, G_0 is full row rank and we can select $u_{k-t},\ldots,u_k$ such that $v_0 = uG_0$ satisfies $\text{wt}(v_0) \le nm - t + 1$ and therefore $\text{rank}(\phi(v_0)) = \text{rank}(V_0) \le n - \left\lfloor \frac{t-1}{m} \right\rfloor = n - \left\lceil \frac{t}{m} \right\rceil + 1$. Thus,

$$\begin{aligned} \text{rank}(V(D)) &= \sum_{0\le i\le\nu} \text{rank}(V_i) \\ &\le n\nu + (n - \left\lceil \frac{t}{m} \right\rceil + 1) \\ &= n(\nu+1) - \left\lceil \frac{t}{m} \right\rceil + 1. \end{aligned}$$

This upper bound is maximized when ν is as large as possible and t as small as possible. However, note that, roughly

speaking, increasing ν by a unit is equivalent to decreasing t by mn. Therefore, we first maximize ν and then minimize t. For given k and $\delta = \sum_{1 \le i \le k} \nu_i$, it is clear that $\nu \le \left\lfloor \frac{\delta}{k} \right\rfloor$. Once $\nu = \left\lfloor \frac{\delta}{k} \right\rfloor$, one can check that $t \ge k\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) - \delta$, the equality holding when the maximum row degree is $\nu + 1$. This concludes the proof. ■

Observe that, similarly to (1), also formula (5) provides a generalized Singleton bound, being equal to (3) when $\delta = 0$.

REFERENCES

[1] R. Kötter and F. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3579–3591, 2008. DOI: 10.1109/tit.2008.926449.

[2] R. Nóbrega and B. Uchoa-Filho, "Multishot codes for network coding using rank-metric codes," in *Wireless Network Coding Conference (WiNC), 2010 IEEE*, 2010, pp. 1–6. DOI: 10.1109/winc.2010.5507933.

[3] A. Wachter-Zeh, M. Stinner, and V. Sidorenko, "Convolutional codes in rank metric with application to random network coding," *IEEE Trans. Inform. Theory*, vol. 61, no. 6, pp. 3199–3213, 2015. DOI: 10.1109/tit.2015.2424930.

[4] R. Mahmood, "Rank metric convolutional codes with applications in network streaming," Master of Applied Science, Graduate Department of Electrical and Computer Engineering, University of Toronto, 2015. [Online]. Available: https://tspace.library.utoronto.ca/handle/1807/70480.

[5] R. J. McEliece, "The algebraic theory of convolutional codes," in *Handbook of Coding Theory*, V. Pless and W. Huffman, Eds., vol. 1, Amsterdam, The Netherlands: Elsevier Science Publishers, 1998, pp. 1065–1138.

[6] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 10, no. 1, pp. 15–32, 1999.

[7] É. Gabidulin, "Theory of codes with maximum rank distance," English, *Probl. Inf. Transm.*, vol. 21, pp. 1–12, 1985.