Maximum rank distance profile codes

Raquel Pinto and Carlos Vela

Department of Mathematics of the University of Aveiro, Aveiro, Portugal

Introduction

Network coding theory provides a pragmatic instrument to disseminate information (packets) over networks where there may be many information sources and possibly many receivers. From a mathematical point of view, these packets can be modelled by columns of matrices over a finite field $\mathbb{F}_q$ and during the transmission, these columns are linearly combined at each node of the network. To achieve reliable communication over this channel, *rank-metric codes* are typically employed.
Nevertheless, network coding techniques for streaming are fundamentally different from the classical ones. To be optimised they must operate under low-latency, sequential encoding and decoding constraints, and as such they must inherently have a convolutional structure. That is the reason why most of the proposed schemes for this scenario employ convolutional codes in different ways [7, 5, 4, 1].

Rank metric convolutional codes

Rank metric convolutional codes over $\mathbb{F}_{q^m}$ were first introduce in [7] for unitmemory codes and for unrestricted memory in [4, 1]. These are convolutional codes defined over an extension field $\mathbb{F}_{q^m}$ and equipped with a rank-type metric, and as such, are referred to as (n, k, δ)-rank metric convolutional codes (over $\mathbb{F}_{q^m}$) if have length n, dimension k and degree δ. Later, a wider definition of convolutional codes over $\mathbb{F}_q$ (instead of over $\mathbb{F}_{q^m}$) was proposed in [6].
A *rank-metric convolutional code* $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ is the image of an homomorphism $\varphi : \mathbb{F}_q[D]^k \to \mathbb{F}_q[D]^{n\times m}$. It is written $\varphi = \psi \circ \gamma$ as 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 $\mathcal{C}$. If the encoder $G(D)$ is in row reduced form [3] the sum of the row degrees attains its minimum among all possible encoders. This value is usually denoted by δ and called the degree of $\mathcal{C}$. A rank metric convolutional code $\mathcal{C}$ of degree δ, defined as in (1) is called a $(n \times m, k, \delta)$-rank metric convolutional code.
The largest row degree over one, and therefore all, reduced encoders of $\mathcal{C}$ is called the memory of $\mathcal{C}$ and denoted by μ. If the memory is considered instead of the degree, a convolutional code with rate k/n and memory μ is referred to as an (n, k, μ) convolutional code [4].

"Linear block codes"

Rank-metric convolutional codes can also be considered as linear spaces over the extension field $\mathbb{F}_{q^M}^n$:

$$\begin{aligned} \varphi : \mathbb{F}_{q^M}[D]^k &\xrightarrow{\gamma} \mathbb{F}_{q^M}[D]^n \xrightarrow{\phi_n} \mathbb{F}_q[D]^{n\times M} \\ u(D) \mapsto v(D) = u(D)G(D) &\mapsto V(D) \end{aligned}$$

where $G'(D) = \sum_{i=0} G_i D^i \in \mathbb{F}_{q^M}^{k\times n}$ and G_0 is full row rank. In this case they consider $\phi_{n'}$, as a natural bijection between $\mathbb{F}_{q^M}$ and $\mathbb{F}_q^M$.

Channel problem

The network channel considered here is the *rank deficiency channel* which is a simplification of more general network channel and can be seem as the analogue of the erasure channel in the context of networks, see [4] for more details. In this channel, at each shot the destination node observes $y_t = v_t A_t^*$, where $A_t \in \mathbb{F}_q^{n\times\rho_t}$ and $\rho_t = rank(A_t^*)$ is the channel matrix at time t, and is known to the receiver [2]. Communication over a window $[t, t+W-1]$ of W shots is described using $y_{[t,t+W-1]} = v_{[t,t+W-1]} A^*_{[t,t+W-1]}$, where $A^*_{[t,t+W-1]} = diag(A_t^*, \ldots, A_{t+W-1}^*)$ is a block diagonal channel matrix as described in [4].

Optimal constructions

There exists two optimal constructions for *maximum sum-rank metric profile codes*. On one hand in [4] the authors construct the encoder $G(D)$ as a submatrix of a superregular (all its submatrices are non-singular) Toeplitz matrix. This construction holds the bounds for j-th sum-rank column distance due to the field size requiered which is $\mathbb{F}_q^M$ for $M \geq q^{n(\mu+2)-1}$ where μ is the memory of the code.
On the other hand, the construction given in [6] its based on the companion matrix of an irreducible polynomial over the base field $\mathbb{F}_q$. Nevertheless, its optimality lays in the condition that $m \geq \sigma + k$ which means that the size of the matrices increases with the size of the message and the degree of the code. Note that the greater is the window we consider the greater the degree of the code needs to be.
Actually, we are working on new constructions which holds these bounds and are close to them.

$$u = (10\,01\,11) \longrightarrow u(D) = (1 + D^2, D + D^2)$$

$$G(D) = \left(\begin{array}{cccccc|cccccc|cccccc} 1 & 0 & D & 0 & D^2 & 0 & 0 & 1 & 0 & D & 0 & D^2 & D^2 & D^2 & 1 & 0 & D & 0 \\ 0 & 1 & 0 & D & 0 & D^2 & D^2 & D^2 & 1 & 0 & D & 0 & 0 & D^2 & D^2 & 1 & 0 & D \end{array}\right)$$

$$u(D)G(D)$$

$$V(D) = \begin{pmatrix} 1+D^2 & D+D^2 & D & D^2 & D^2 & 0 \\ 0 & 1+D^2 & D+D^2 & D & D^2 & D^2 \\ D^2 & D^2 & 1+D^2 & D+D^2 & D & D^2 \end{pmatrix}$$

$$V(D)A^*_{[0,2]}$$

$$A_0^* = \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \\ 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}; A_1^* = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix}; A_2^* = \begin{pmatrix} 1&0&0&0&0&0 \\ 0&1&0&0&0&0 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{pmatrix}$$

$$X_0 = \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}; X_1 = \begin{pmatrix} 0&1&1&0 \\ 0&0&1&1 \\ 0&0&0&1 \end{pmatrix}; X_2 = \begin{pmatrix} 1&1&0&1&1&0 \\ 0&1&1&0&1&1 \\ 1&1&1&1&0&1 \end{pmatrix}$$

$$X^{EX}(G_2^{EX} A^*_{[0,2]})^{-1}$$

$$u_0 = (10);\ u_1 = (01);\ u_2 = (11)$$

Singleton bound

The *j-th sum-rank column distance* of $\mathcal{C}$ is:

$$d_{SR}^j(\mathcal{C}) = \min_{x_{[0,j]}\in\mathcal{C}} \sum_{t=0}^{j} rank(\phi_n(x_{[0,j]}))$$

where $\phi_n : \mathbb{F}_{q^M}^n \to \mathbb{F}_q^{n\times M}$ is the bijective mapping which allows to use the rank based metric instead of the Hamming metric. This column distance is upper-bounded by:

$$d_{SR}^j(\mathcal{C}) \leq (n-k)(j+1) + 1.$$

The codes which achieves this bound are named *Maximum Sum Rank codes* (MSR).

Decoding rank deficiencies

Theorem 1 *Let $\mathcal{C}$ be a $(n \times m, k, \delta)$ be a rank-metric convolutional code used over the window $[0, W-1]$. For $0 \leq t \leq W-1$, let $A_t^* \in \mathbb{F}_q^{n\times\rho_t}$ be full-rank matrices and $A^*_{[0,W-1]} = diag(A_0^*, \ldots, A_{W-1}^*)$ be a channel matrix. The following statements are true:*

1. *If $d_{SR}(W-1) > nW - \sum_{t=0}^{W-1} \rho_t$, then u_0 is always recoverable by time $W-1$.*
2. *If $d_{SR}(W-1) \leq nW - \sum_{t=0}^{W-1} \rho_t$, then there exists at least one channel packet sequence and channel matrix for which u_0 is not recoverable by time $W-1$.*

As a consequence of the proof of this theorem it is possible to see that for the total recover of the information is enough find the row reduced echelon form of the matrix $G_{W-1}^{EX} A^*_{[0,W-1]}$.

References

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

[2] T. Ho, M. Médard, R. Kötter, C.R. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, 52:413–430, 2006.

[3] R. Johannesson and K. Sh. Zigangirov. *Fundamentals of Convolutional Coding*. IEEE Press, New York, 1999.

[4] R. Mahmood, A. Badr, and A. Khisti. Convolutional codes with maximum column sum rank for network streaming. *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 2271–2275, 2015.

[5] D. Napp, R. Pinto, J. Rosenthal, and F. Santana. Column rank distances of rank metric convolutional codes. In V. Skachek A. Barbero and O. Ytrehus, editors, *Coding Theory and Applications*, pages 248–256. Springer International Publishing, 2017.

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

[7] A. Wachter-Zeh, M. Stinner, and V. Sidorenko. Convolutional codes in rank metric with application to random network coding. *IEEE Transactions on Information Theory*, 61:3199–3213, 2015.

Contact information: Carlos Vela, Department of mathematics, University of Aveiro, Aveiro, Portugal, 3810-193 – Email: *carlos.vela@ua.pt*
This work has been partially supported 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 UIDB/04106/2020.