Proceedings of the 25th International Symposium on Mathematical Theory of Networks and Systems
Bayreuth, Germany, 12-16 September 2022

On rank metric convolutional codes and concatenated codes [⋆]

Diego Napp [*] **Raquel Pinto** [**] **Carlos Vela** [**]

[*] *Department of Mathematics, University of Alicante, Alicante, Spain (e-mail: diego.napp at ua.es).*
[**] *Department of Mathematics, University of Aveiro, 3810-197 Aveiro, Portugal (e-mail: carlos.vela, raquel at ua.pt)*

Abstract: In the recent history of the theory of network coding the multi-shot network coding has been prove as a good alternative for the classical one-shot network theory which is managed by using block codes. To perform communications in this multi-shot context we have, among others, rank-metric convolutional codes and concatenated codes (using a convolutional code as an outer code and a rank-metric code as inner code). In this work we analyse their performance over the rank deficiency channel (described by Gilbert-Elliot channel model) in terms of the correction capabilities and the complexity of the two decoding schemes.

Keywords: concatenated codes, rank-metric codes, convolutional codes, rank-deficiency channel, complexity

1. INTRODUCTION

Since its raising at the beginning of 2000's, network coding has been a research topic that has attracted significant interest in many areas, including electrical engineering, computer science and applied mathematics. 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.

Most of the literature deals with the situation in which the network is used only once to propagate the information. Such scenario is referred to as *one-shot* network coding, as the encoding and transmission is performed over one use (shot) of the network. If one needs to transmit more data (packets), then these packets are again encoded and transmitted in the following instant, independently on the previous transmissions. However, one can improve the error-correction capability of the code in the scenario where we need to use the network several times (*multi-shot*) by creating correlation among the transmitted data in different shots. This new approach has recently attracted much attention due to possible interesting applications, e.g., in streaming communications Mahmood et al. (2015). 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 Wachter-Zeh et al. (2015); Napp et al. (2017a); Mahmood et al. (2015); Almeida et al. (2020).

In this work we present a comparison of two different and important schemes for multi-shot network coding: rank metric convolutional codes and concatenated codes (concatenation of a convolutional code and a rank metric code) Napp et al. (2018). In particular, we compare their performance over a rank-deficiency channel focusing on the correction capabilities and the complexity of the encoding and decoding procedures of each proposal. For practical reasons, in our comparison we limit the field size. Since the construction of optimal rank-metric codes for this channel exists Mahmood et al. (2015) only for large finite fields, such codes cannot be used in this context. The concatenated codes, however, can be constructed optimally. In Section 2 we present the necessary background about convolutional codes, rank-metric convolutional codes and concatenated codes and the nature of the used channel. In Section 3 we make a comparison of the performance of both codes over this kind of channel. Later, in Section 4 we compare the complexity in the decoding process under the circumstances established in the previous section. Finally, in Section 5 we make some review of this work and present future possible works.

2. PRELIMINARIES

2.1 Convolutional codes

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_q[D]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. A *convolutional code* $\mathcal{C}$

[⋆] 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. The second author was also supported by the Ministerio de Ciencia e Innovación under the grant with ref. PID2019-108668GB-I00.

of rate k/n is a rank k $\mathbb{F}_q[D]$-submodule of $\mathbb{F}_q[D]^n$. If $G(D) \in \mathbb{F}_q[D]^{k\times n}$ is a full row rank matrix such that

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

then $G(D)$ is called an encoder of $\mathcal{C}$.

Any other encoder $\tilde{G}$ of $\mathcal{C}$ differs from $G(D)$ by a unimodular matrix $U(D) \in \mathbb{F}_q[D]^{k\times k}$. *i.e.*, $\tilde{G}(D) = U(D)G(D)$. Therefore, we can consider $G(D)$ to be minimal, *i.e.*, in row reduced form Johannesson and Zigangirov (1999). In this case, the sum of the row degrees of $G(D)$ attains its minimum among all the encoders. This value is usually denoted by δ and called the degree of $\mathcal{C}$. A convolutional code with rate k/n and degree δ is called an (n, k, δ) convolutional codes, McEliece (1998). 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 Mahmood et al. (2015).

An important distance measure for convolutional codes $\mathcal{C}$ is its free distance which is defined as

$$d_{free}(\mathcal{C}) = \min_{v(D)\in\mathcal{C}, v(D)\neq 0} wt(v(D)),$$

where $wt(v(D))$ 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

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

being $wt(v_i)$ the number of the nonzero components of v_i. Another important distance measure is the *j-th column distance*,

$$d_H^j(\mathcal{C}) = \min\left\{wt(v(D)|_{[0,j]}) \mid v(D) \in \mathcal{C}, v_0 \neq 0\right\}$$

where $v(D) = \sum_{i\in\mathbb{N}} v_i D^i$ and $v(D)|_{[0,j]} = \sum_{i=0}^{j} v_i D^i$. This measure is also upper-bounded in Johannesson and Zigangirov (1999):

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

for $j \leq L$ where $L = \lfloor \delta/k \rfloor + \lfloor \delta/(n-k) \rfloor$. The convolutional code achieving the bound for all $j \in \{0, \ldots, L\}$ is called *maximum distance profile* (MDP) convolutional code Gluesing-Luerssen et al. (2006).

2.2 Rank-metric codes

Let $A, B \in \mathbb{F}_q^{n\times m}$. The rank distance between two matrices is

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

This defines a distance, called *rank distance*, and rank-metric codes are subsets of $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ equipped with the rank distance. Rank metric codes in $\mathbb{F}_q^{n\times m}$ are usually constructed as block codes of length n over the extension field $\mathbb{F}_{q^m}$ as in Kötter and Kschischang (2008). For a given basis of $\mathbb{F}_{q^m}$ viewed as an m vector space over $\mathbb{F}_q$, any element of $\mathbb{F}_{q^m}$ can be seen as a vector in $\mathbb{F}_q^m$. In this paper we will follow this approach and consider rank-metric codes as linear codes $[n, k]$ over $\mathbb{F}_{q^m}$. For the sake of simplicity we assume that $m \leq n$. In this case, linear rank metric codes of length n and dimension k over $\mathbb{F}_{q^m}$ must satisfy the following Singleton-type bound:

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

A code that achieves this bound is called *Maximum Rank Distance* (MRD). Gabidulin codes are a well-known class of MRD codes as showed in Gabidulin (1985).

2.3 Rank-metric convolutional codes

Rank metric convolutional codes over $\mathbb{F}_{q^m}$ were first introduce in Wachter-Zeh et al. (2015) for unitmemory codes and for unrestricted memory in Mahmood et al. (2015); Almeida et al. (2020). 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 Napp et al. (2017b).

In Mahmood et al. (2015) a new column rank-base distance is considered. Let $\mathcal{C}$ be a (n, k, μ) be a convolutional code over $\mathbb{F}_{q^M}$. The *j-th column rank 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). These codes are showed to exists and a construction is given Mahmood et al. (2015). The larger the column distance is, the better is the correction capability within an interval of time. Hence, rank metric convolutional codes with optimal column distance profile are ideal for fast decoding, *i.e.*, for streaming application with low delay constrains. For these reasons we shall consider in this work MSR convolutional codes for our analysis.

2.4 Concatenated codes

In this section we introduce a completely different class of codes in the context of multi-shot network coding. Such a scheme comprises the concatenation of a Hamming metric convolutional code as an "outer code" and a rank metric block code as an "inner code". These codes are described by the concatenation scheme proposed in Napp et al. (2018) as follows: Let $\mathcal{C}_I$ be a linear (n_I, k_I) rank metric code over $\mathbb{F}_{q^m}$ with (rank) distance $d_{rank}(\mathcal{C}_I)$ and generator matrix $G_I \in \mathbb{F}_{q^m}^{k_I\times n_I}$. Let $\mathcal{C}_O$ be an (n_O, k_O, δ) convolutional code over the field $\mathbb{F}_{q^{mk_I}}$ with Free distance $d_H(\mathcal{C}_O)$, column distance $d_H^j(\mathcal{C}_O)$ and a generator matrix $G_O(D) \in \mathbb{F}_{q^{mk_I}}[D]^{k_O\times n_O}$.

The information (row) vector $u(D) = u_0 + u_1 D + u_2 D^2 + \cdots \in \mathbb{F}_{q^{mk_I}}[D]^{k_O}$ is encoded through $G_O(D)$ to generate

$$v(D) = v_0 + v_1 D + v_2 D^2 + \cdots = u(D)G_O(D) \in \mathcal{C}_O.$$

We write $v_i = (v_i^0, v_i^1, \ldots, v_i^{n_O-1}), v_i^j \in \mathbb{F}_{q^{mk_I}}$. Now, we identify $v_i^j \in \mathbb{F}_{q^{mk_I}}$ with a vector $\nu_i^j \in \mathbb{F}_{q^m}^{k_I}$ (for a given basis of $\mathbb{F}_{q^{mk_I}}$) and write $\nu_i = (\nu_i^0, \nu_i^1, \dots, \nu_i^{n_O-1}) \in (\mathbb{F}_{q^m}^{k_I})^{n_O}$ and therefore

$$\nu(D) = \nu_0 + \nu_1 D + \nu_2 D^2 + \cdots \in \mathbb{F}_{q^m}^{k_I}[D]^{n_O}.$$

Finally, the codewords $x(D)$ of the concatenated code $\mathcal{C}$ are obtained through the matrix $G_I \in \mathbb{F}_{q^m}^{k_I \times n_I}$ in the following way:

$$x_i^j = \nu_i^j G_I \in \mathbb{F}_{q^m}^{n_I},$$
$$x_i = (x_i^0, x_i^1, \dots, x_i^{n_O-1}) \in (\mathbb{F}_{q^m}^{k_I})^{n_O},$$
$$x(D) = x_0 + x_1 D + x_2 D^2 + \cdots \in \mathcal{C} \subset \mathbb{F}_{q^m}^{k_I}[D]^{n_O}.$$

The sum rank metric and the j-th column sum rank distances are bounded by (see Napp et al. (2018)):

$$d_{SR}(\mathcal{C}) \leq (n_O n_I - k_O k_I)(\left\lfloor \frac{\delta}{k_O} \right\rfloor + 1) + \delta k_I + 1,$$

$$d_{SR}^j(\mathcal{C}) \leq (n_O n_I - k_O k_I)(j+1) + 1,$$

respectively.

2.5 Network model

In multi-shot network coding the information (packets) sent in the different uses of the network (shots) are correlated to improve the correction capability of the codes. The natural tool to use in this network are the convolutional codes which take into account this delay in the transference of the information. The network channel considered here is the *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 Mahmood et al. (2015) for more details. In this channel, at each shot the destination node observes $y_t = x_t A_t$, where $A_t \in \mathbb{F}_q^{n \times n}$ is the channel matrix at time t, and is known to the receiver, as explained in Ho et al. (2006). Communication over a window $[t, t+W-1]$ of W shots is described using $y_{[t,t+W-1]} = x_{[t,t+W-1]} A_{[t,t+W-1]}$, where $A_{[t,t+W-1]} = diag(A_t, \dots, A_{t+W-1})$ is a block diagonal channel matrix as described in Mahmood et al. (2015). Let $\rho_t \triangleq rank(A_t)$ denote the rank of A_t, for all $t \geq 0$, we have that $\sum_{i=t}^{t+W-1} \rho_i = rank(A_{[t,t+W-1]})$. If during the circulation of the information, some of the intermediate nodes fails, the transmission will continue to work without including it in the linear combinations of the packets If all links are functional in the shot at any time t, then $\rho_t = n$, but failing links may result in a rank-deficient channel matrix at that time.

In the context of rank deficiency channels, we shall consider channels that satisfy certain conditions within an interval of time (window), see Mahmood et al. (2015). These are called *Rank-Deficient Sliding Window Networks*, denoted by $\mathcal{CH}(S, W)$ and have the property that in any sliding window of length W, the rank of the block diagonal channel decreases by no more than S, i.e., $\sum_{i=t}^{t+W-1} \rho_i \geq nW - S$ for each $t \geq 0$. We will say that a linear code $\mathcal{C}$ over $\mathbb{F}_{q^M}$ is defined as *feasible* for the channel $\mathcal{CH}(S, W)$ if the encoding and decoding functions for the code are capable of perfectly recovering every source packet transmitted over it with delay T, *i.e.*, to achieve the information of the packet x_t received at moment t by performing the necessary operations with at most the next T received packets, that is $x_t, \dots, x_{t+T-1}$.

3. PERFORMANCE OF THE CODES

3.1 Discussion

In this subsection we will compare the correction capabilities of the two proposed codes over a rank-deficient sliding window channels. First, we will see under which constrains the cited codes are feasible for the channel $\mathcal{CH}(S, W)$. Secondly, we will compare their bounds on the j-th column distances and discuss the capabilities of them.

In Mahmood et al. (2015), a construction for the MSR convolutional codes is proposed. It is said that these codes are feasible for a rank-deficiency sliding window channel $\mathcal{CH}(S, W)$ with delay $T \geq W$ under the assumption $S < d_{SR}^{W-1}(\mathcal{C})$, where $\mathcal{C}$ is the MSR convolutional code. In the case in which $T < W$ it is enough to consider $S < d_{SR}^{T}(\mathcal{C})$. These codes guarantee the recover of the information under the worst channel conditions for a fixed delay and rate, i.e., they identify the largest rank deficiency S for which a code with a given rate is feasible.

On the other hand, we consider the concatenated codes constructed in Napp et al. (2018). Let $\mathcal{C}$, $\mathcal{C}_O$ and $\mathcal{C}_I$ be the concatenated code, the convolutional code and the rank-metric code, respectively as described above. The concatenated codes are also feasible for the rank-deficiency sliding window channel $\mathcal{CH}(S, W)$ with delay $T' \geq W$ if $S < d_H^{T'}(\mathcal{C}_O) d_{rank}(\mathcal{C}_I)$ where $T' = \left\lfloor \frac{W-1}{n_I} \right\rfloor$ due to the construction of the code. When $T < W$ it is enough to consider $S < d_H^{T'}(\mathcal{C}_O) d_{rank}(\mathcal{C}_I)$ where $T' = \left\lfloor \frac{T}{n_I} \right\rfloor$. The next result, establish which of these two families of codes have better distance bounds under the same conditions:

Theorem 1. Let $\mathcal{C}_{MSR}$ be a MSR convolutional code and C_{Conc}, $\mathcal{C}_O$ and C_I be a concatenated, convolutional and rank metric codes, respectively. Over a rank-deficiency sliding window channel $\mathcal{CH}(S, W)$, with fixed rate $k/n = k_O k_I / n_O n_I$ and delay T, then

$$d_H^{j'}(\mathcal{C}_O) d_{rank}(\mathcal{C}_I) < d_{SR}^{j-1}(\mathcal{C}_{MSR})$$

where $j' = \left\lfloor \frac{j-1}{n_I} \right\rfloor$ with $1 \leq j \leq T$.

Note that in the theorem above, we compare the corresponding column distance after receiving the same amount of shots. Since the bound established for $\mathcal{CH}(S, W)$ cannot be achieved by the concatenated codes, MSR convolutional codes are the only optimal codes, but huge finite fields are necessary to ensure their existence. To build a (n, k, μ) MSR convolutional code, where μ is the memory of the code, the field required for the construction presented in Mahmood et al. (2015) is $\mathbb{F}_{q^M}$ with $M = q^{n(\mu+2)-1}$. For example, to obtain the codes $(3, 1, 2)$ and $(2, 1, 2)$ the fields $\mathbb{F}_{2^{2048}}$ and $\mathbb{F}_{2^{128}}$ are needed.

This last condition is an issue from the practical point of view, since the memory required for storage and usage of these codes are enormous. For this reason, it makes sense to restrict the size of the fields for the construction of codes used in networks described as above. Taking this into account, we have two possibilities: a) to look for an alternative family of codes which achieves or improve the bounds of the Rank-Deficient Sliding Window

Network CH(S,W) over fields of minimum size or b) to find a construction for MSR codes for smaller fields.

With this in mind, an alternative family of codes for this sort of channel are the concatenated codes. Despite the fact that their distance is significant smaller that the one of MSR codes (as indicated in Theorem 1) it is important to note that the distribution of the deficiencies within the window is crucial for recovering the missing packets. For instance, suppose that in the first t instances we send $x_0, \dots, x_t$ and received $y_0, \dots, y_t$. In order to recover x_0 at time instant t with the MSR code, we need to have less than $d_{SR}^{j-1}(\mathcal{C}_{MSR})$ deficiencies for some $j = 0, 1, \dots, t$ independently of the distribution of these deficiencies within the intervals. However, if we use a concatenated code then depending on the distribution of the deficiencies within the windows, the inner rank metric code gives very different erasures patterns to the outer code.

4. COMPLEXITY

In this section we compare the complexity of the decoding performance of both, the concatenated codes and the MSR convolutional codes. In Mahmood et al. (2015), it is said that the complexity of the decoding method, over a window of length $j-1$, for the MSR convolutional codes is $\mathcal{O}(((j-1)k)^3)$ over $\mathbb{F}_{q^M}$. This is due to the decoding method can be reduced to the inversion of a square matrix of this size.

In order to obtain the complexity of the decoding performance of the concatenated codes over a window of length $j-1$ we have to observe that it can be divide into two parts. First, the MRD code corrects the rank deficiency errors or give an erasure. Second, once all the packets are processed by the MRD code, the convolutional code corrects all the erasures in the window by solving a linear system. The performance of the MRD code over the window has complexity $\mathcal{O}((j-1)(k_I)^3)$ over $\mathbb{F}_{q^m}$, while the second part has $\mathcal{O}((n_I d_H^j(C_O))^2)$, since the convolutional code correct up to $d_H^j(C_O)$ packets that contains n_I elements over the field $\mathbb{F}_{q^{mk_I}}$. Thus the complexity of the decoding performance of the concatenated code is $\mathcal{O}((j-1)(k_I)^3)$ over $\mathbb{F}_{q^m}$. By considering, $M = m$ in order to compare comparable complexities, we have $\mathcal{O}(j(k_I)^3) \leq \mathcal{O}((jk)^3)$ which means that, exponentially, the decoding for the concatenated codes is faster.

5. CONCLUSION

In this paper we have discussed the difference in the performance of both MSR convolutional codes and concatenated codes under the same channel. We can say that the concatenated codes are faster by correcting the rank deficiencies and they correct a considerable amount of rank deficiencies with high probability. These codes can be constructed for fields of a more affordable size than the required for the existence of MSR codes.

There are some open problems that arise from this discussion. One of them is to find a construction of rank-metric convolutional codes with greater correction capability than the concatenated codes over a same size field or develop a construction for MSR codes for limited field size. In this sense, in Alfarano et al. (2020), a construction for optimal codes for Hamming column distance is presented. One last open question emerges, the search for new concatenated codes that improve the bounds presented in Napp et al. (2018) due to the flexibility of concatenation technique.

REFERENCES

Alfarano, G.N., Napp, D., Neri, A., and Requena, V. (2020). Weighted reed-solomon convolutional codes. *CoRR*, abs/2012.11417. URL `https://arxiv.org/abs/2012.11417`.

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

Gabidulin, E. (1985). Theory of codes with maximum rank distance. *prob. Inf. Transm.*, 21, 1–12.

Gluesing-Luerssen, H., Rosenthal, J., and Smarandache, R. (2006). Strongly-mds convolutional codes. *IEEE Transactions on Information Theory*, 52, 584–598.

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

Johannesson, R. and Zigangirov, K.S. (1999). *Fundamentals of Convolutional Coding*. IEEE Press, New York.

Kötter, R. and Kschischang, F. (2008). Coding for error and erasures in random network coding. *IEEE Transactions on Information Theory*, 54, 3579–3591.

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

McEliece, R.J. (1998). The algebraic theory of convolutional codes. In V. Pless and W. Huffman (eds.), *Handbook of coding theory*, volume 1, 1065–1138. Elsevier Science Publishers, The Netherlands.

Napp, D., Pinto, R., Rosenthal, J., and Santana, F. (2017a). Column rank distances of rank metric convolutional codes. In V.S. A. Barbero and O. Ytrehus (eds.), *Coding Theory and Applications*, 248–256. Springer International Publishing.

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

Napp, D., Pinto, R., and Sidorenko, V. (2018). Concatenation of convolutional codes and rank metric codes for multi-shot network coding. *Des. Codes Cryptogr*, 86, 303–318.

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