A new metric for multi-shot network coding

J.-J. Climent\(^1\), D. Napp\(^2\) and V. Requena\(^1\)

Abstract—In this paper we study convolutional codes in the context of multi-shot network coding. Within this context, several classes of rank metric convolutional codes have been recently proposed in the literature. The metric considered so far in this context is the so-called sum rank distance, which makes the unnecessary assumption that the natural delay in the transmission (due, for instance, to the delay of the nodes) is so small that can be disregarded. In this work we introduce a new metric that overcomes this restriction and therefore is suitable to handle networks with delays. We shall call it the column rank distance.

Index Terms—Network coding, convolutional codes, rank metric, column distance, rank deficiency.

AMS subject classifications — 68P30, 11T71.

I. INTRODUCTION

In many packet communications applications a transmitter sends packets through a network and the intermediate nodes perform a random linear combination of the packets received and forward this random combination to adjacent nodes. Mathematically, we can consider the transmitted packet as columns of a matrix with entries in a finite field \(\mathbb{F}_q\), and the linear combinations performed in the nodes correspond to columns operations on this matrix. If no errors occur during the transmission over such a network, the column space of the transmitted matrix remains invariant. To achieve a reliable communication over this channel, matrix codes are employed forming the so-called rank metric codes \([1]\). Rank metric codes such as Gabidulin codes are known to be able to protect packets in such a scenario. We call these codes one-shot codes, as they use the (network) channel only once.

The theory of random linear network coding developed so far is concerned to large extent with one-shot network coding. However, coding can also be performed over multiple uses of the network as it has been recently shown by several authors, see for instance \([2]\), \([3]\), \([4]\), \([5]\), \([6]\). The general idea stems from the fact that creating dependencies among the transmitted codewords (subspaces) of different shots can improve the error-correction capabilities of the code. Thus, multi-shot codes constitute an attractive class of codes for such situations.

In \([5]\) a first attempt to explain the context of multi-shot network coding was presented and a type of concatenated \(n\)-shot codes \((n \geq 1)\) was proposed based on a multilevel code. In \([7]\), a concatenation scheme was presented using a Hamming metric convolutional code as an outer code and a rank metric code as an inner code. Apart from concatenated codes, another very natural way to spread redundancy across codewords is by means of convolutional codes \([8]\), \([9]\), \([10]\), \([11]\), \([12]\). Adapting this class of codes to the context of networks gave rise to rank metric convolutional codes and interestingly there have been little research on these codes, see \([2]\), \([13]\), \([3]\), \([6]\). The work in \([6]\) was pioneer in this direction by presenting the first class of rank metric convolutional codes together with a decoding algorithm able to deal with errors, erasures and deviations. However, the results were only valid for unit memory convolutional codes and in \([2]\), \([13]\), \([3]\) (see also the references therein) an interesting and more general class of rank metric convolutional codes was introduced to cope with network streaming applications. For a more general theoretical framework to rank metric convolutional codes, see \([4]\).

In this multi-shot setting a new distance, called sum rank distance, was introduced as a generalization of the rank distance used for one-shot network coding. This new distance has proven to be the proper notion in order to deal with delay-free networks, i.e., assuming that the natural delay in the transmission (due, for instance, to the delay of the nodes) is so small that can be disregarded. In this work we show that in order to handle networks with delays, a new metric needs to be introduced. In this work, we propose such a (rank) metric and called it column rank distance. This new metric can be considered as an analog of the column distance of Hamming convolutional codes and extends the already existing notion of column sum rank distance.

Finally, we note that in the last years others papers have also appeared dealing with convolutional network coding using very different approaches \([14]\), \([15]\). These codes do not transmit over the operator channel and therefore are not equipped with the rank metric.

II. PRELIMINARIES

In order to state more precisely the results to be presented we introduce in this section the necessary material and notation on standard theory of rank metric codes and convolutional codes.

A. Rank Metric

A rank metric code \(C\) is defined as any nonempty subset of \(\mathbb{F}_q^{M \times n}\). A natural metric for matrix codes is induced by the distance measure \(d_{\text{un}}(V, W) = \text{rank}(V - W)\), where \(V, W \in \mathbb{F}_q^{M \times n}\) \([16]\). In the context of the rank metric, a matrix code is called rank metric code. Rank metric codes in \(\mathbb{F}_q^{M \times n}\) are usually constructed as block codes of length...
The rank distance of a code $C \subseteq \mathbb{F}_q^n$ is defined as

$$d_{\text{rk}}(C) = \min_{V,W \in C, V \neq W} d_{\text{rk}}(V,W).$$

Obviously $\mathbb{F}_q^n \cong \mathbb{F}_q^M$ and let $\phi: \mathbb{F}_q^M \to \mathbb{F}_q^{M \times n}$ an isomorphism that converts vectors $v \in \mathbb{F}_q^M$ into matrices $\phi(v) = V \in \mathbb{F}_q^{M \times n}$. We abuse notation by writing rank($v$) for rank($\phi(v)$) = rank($V$). In this paper we will consider linear codes over $\mathbb{F}_q^M$ and we use $k$ for the dimension of the linear code over $\mathbb{F}_q^M$. To simplify presentation we will assume that $M \gg n$.

B. Convolutional codes

A convolutional code $C$ of rate $k/n$ is an $\mathbb{F}_q^M[D]$-submodule of $\mathbb{F}_q^M[D]^n$ of rank $k$. A full row rank matrix $G(D) \in \mathbb{F}_q^M[D]^{k \times n}$ with the property that

$$C = \ker G(D) = \{u(D)G(D) \mid u(D) \in \mathbb{F}_q^M[D]\},$$

is called a generator matrix. The degree $\delta$ of a convolutional code $C$ is the maximum of the degrees of the determinants of the $k \times k$ sub-matrices of one, and hence any, generator matrix of $C$. Note that an block code is a convolutional code with $\delta = 0$.

If $G(D)$ is a basic (meaning right invertible) generator matrix, then the code $C$ can be equivalently described using an $(n-k) \times n$ full rank polynomial parity-check matrix $H(D)$, defined by

$$H(D) = \sum_{i=0}^{m} H_i D^i,$$

and the associated sliding matrix of $H(D)$ is

$$H_j = \begin{pmatrix} H_0 & \cdots & \cdots \\ H_1 & H_0 & \cdots \\ \vdots & \vdots & \ddots \\ H_j & H_{j-1} & \cdots & H_0 \end{pmatrix}$$

with $H_j = 0$ when $j > m$, $j \in \mathbb{N}$.

III. FROM ONE-SHOT TO MULTI-SHOT NETWORK CODING

In this section we explain how to extend the classical theory of (one-shot) network coding to the context of multi-shot network coding. In fact, this is possible as each packet carries a label identifying the shot (or generation) to which it corresponds. Despite the little research in the area, this possibility was already observed in the seminal papers [16], [1].

Let $v \in \mathbb{F}_q^M \cong \mathbb{F}_q^{M \times n}$ represents the $n$ packets of length $M$ to be sent through the network at one time instance. We shall follow the approach proposed in [16], [1] and consider the operator channel for one shot given by

$$x = vA + z,$$

where $x \in \mathbb{F}_q^n$ represents the received packets, $A \in \mathbb{F}_q^{n \times n}$ is the rank deficiency channel matrix and $z \in \mathbb{F}_q^n$ is the additive error. The adversaries of the matrix channel (1) come as rank deficiency of the channel matrix and as the additive error matrix. The channel matrix $A$ corresponds to the overall linear transformations applied by the network over the base field $\mathbb{F}_q$ and it is known by the receiver (as the combinations are carried over in the header bits of the packets). For perfect communications we have that $z = 0$ and rank($A$) = $n$. We call $n - \text{rank}(A)$ the rank deficiency of the channel.

The transmitter receives at each time instance $t$ a source packet $u_t \in \mathbb{k}^M$ (constituted by a set of $k$ packets) and a channel packet $v_t \in \mathbb{F}_q^n$ (constituted by a set of $n$ packets) is constructed using not only $u_t$ but also previous source packets $u_0, \ldots, u_{t-1}$.

The multi-shot setting can be described as follows: A channel packet $v_t$ is sent through the network at each shot (time instance) $t$. The receiver collects the packets $x_t$, as they arrive causally and tries to infer $v_t$ from $x_0, \ldots, x_t$.

Following the operator channel in (1) at each shot $t$ the received packets $x_t \in \mathbb{F}_q^n$ are corrupted by corrupted packets $z$ and linear combinations of the packets of $v_t$ and, if there is delay in the transmission, also of combinations of the previous packets $v_0, \ldots, v_{t-1}$. Hence, we have

$$x_{[0,j]} = v_{[0,j]} A_{[0,j]} + z$$

where $x_{[0,j]} = (x_1, x_2, \ldots, x_j)$, $v_{[0,j]} = (v_0, v_1, \ldots, v_j) \in \mathbb{F}_q^{n(j+1)}$, $A_{[0,j]} \in \mathbb{F}_q^{n(j+1) \times n(j+1)}$ is a block upper triangular truncated channel matrix and $z \in \mathbb{F}_q^{n(j+1)}$ the additive error. So far this channel model has not been proposed nor addressed in the literature in this generality and only the delay-free case has been considered, see [13] and reference therein. In the delay-free case only combinations of packets of $v_t$ arrive at time instance $t$ and not of packets of $v_i$, $i < t$ and therefore in this case the rank deficiency matrix $A_{[0,j]}$ is a block diagonal matrix.

IV. A NEW METRIC

The sum rank distance is the distance that has been widely considered for multi-shot network coding and can be seen as the analog of the rank distance for one-shot network coding. This distance was first introduced in [5] under the name of extended rank distance and is defined as follows.

Let $v = (v_0, \ldots, v_t)$ and $w = (w_0, \ldots, w_t)$ be two $(t+1)$-tuples of vectors in $\mathbb{F}_q^n$. The sum rank distance (SRD) between them is

$$d_{\text{SRD}}(v,w) = \sum_{i=0}^{t} \text{rank}(v_i - w_i).$$

For an $(n,k,\delta)$-convolutional code $C$ and $v(D) = v_0 + v_1 D + v_2 D^2 + \cdots \in C$ we define its free sum rank distance as

$$d_{\text{SR}}(C) = \min \left\{ \sum_{i=0}^{t} \text{rank}(v_i) \mid v(D) \in C \text{ and } v(D) \neq 0 \right\},$$
and its column sum rank distance as
\[ d_{SR}^C(C) = \min \left\{ \sum_{i=0}^j \text{rank}(v_i) \mid v(D) \in C \text{ and } v_0 \neq 0 \right\}. \]

As we will see below, the SRD is a metric that can be used to fully characterize the error-correcting capabilities of multi-shot codes in the context of delay-free networks. For the general case we propose the following distance, called Column Rank Distance (CRD),
\[ d_{CR}(v, w) = \text{rank}(v-w) = \text{rank}((v_0, \ldots, v_j)-(w_0, \ldots, w_j)). \]

Moreover, based on the CRD we introduce the Column Rank Distance for convolutional codes as follows:
\[ d_{SR}^C(C) = \min \{ \text{rank}(v_0, \ldots, v_j) \mid v(D) \in C \text{ and } v_0 \neq 0 \}. \]

This is a straightforward generalization of the rank distance for one-shot network codes but it is new in the context of multi-shot network codes. In the next section we will show that it is the proper metric to deal with network that allows delays.

In [6], concrete decoding algorithms for unit memory rank metric convolutional codes were presented using another distance, namely the active rank distance. However, in [17], it was shown that this metric fails to determine the error-correcting capabilities of rank metric convolutional codes with arbitrary memory and the column SRD needs to be considered. In fact, necessary and sufficient conditions were inferred to recover rank deficiencies within a given time interval in delay-free networks when no errors occur (i.e., when \( z = 0 \) in (2)).

**Theorem 1:** [17, Theorem 2] Let \( C \) be a rank metric convolutional code and \( v(D) = v_0 + v_1 D + \cdots \in C \) with \( v_0 \neq 0 \). Assume a delay-free transmission and let \( A_{[0,T]} = \text{diag}(A_0, \ldots, A_T) \) represent the block diagonal truncated channel matrix with \( A_i \in \mathbb{F}_q^{6 \times 6} \), i.e., \( x_{[0,T]} = v_{[0,T]} A_{[0,T]} \) is the received set of packets with \( x_i = v_i A_i, \ i = 0, 1, \ldots, T \). Note that in this case \( \text{rank}(A_{[0,T]}) = \sum_{j=0}^T \text{rank}(A_j) \). Then, we can recover \( v_0 \) if
\[ d_{SR}^C(C) > n(T + 1) - \text{rank}(A_{[0,T]}). \] (3)

**Theorem 2:** Let \( C \subset \mathbb{F}_q^{6 \times 6} \) be a \((n, k, \delta)\) rank metric convolutional code, \( v(D) \in C \) and \( A_{[0,T]} \) be the truncated channel matrix. Then, we can recover \( v_{[0,T]} \) if
\[ d_{SR}^C(C) > n(T + 1) - \text{rank}(A_{[0,T]}). \] (4)

**Proof:** Let \( x_{[0,T]} = v_{[0,T]} A_{[0,T]} \). Due to the linearity of the code it is enough to show that all output channel sequence are distinguishable from the zero sequence, i.e., we need to prove that \( v_{[0,T]} A_{[0,T]} = 0 \) is impossible if \( \text{rank}(A_{[0,T]}) \) satisfies (4). It is easy to see that \( \text{rank}(v_{[0,T]}) \leq n(T + 1) - \text{rank}(A_{[0,T]}) \). Using this, together with assumption (4), it follows that \( \text{rank}(v_{[0,T]}) < d_{SR}^C(C) \) which is impossible by definition of \( d_{SR}^C(C) \).

Note that in the previous example \( d_{SR}^C(C) = 1 \) but \( d_{SR}^C(C) = 2 \).

**V. CHARACTERIZATIONS IN TERMS OF THE PARITY-CHECK MATRICES**

In this section we investigate how to build convolutional codes with design column rank distance. To this end we first consider the block case and characterize the rank distance in terms of the properties of the corresponding parity-checks. Finally, we shall address the convolutional case.
Theorem 3: Let $C = \ker H \subset F_{q^m}^n$ be a block code and $H$ a parity-check of $C$. Then, $d_{\text{rk}}(C) = d$ if and only if every set of $d-1$ columns of $HA$, for all $A \in F_{q^m}^{n \times n}$ invertible, are linearly independent (over $F_{q^m}$) and moreover there exists $d$ columns of $HA$ linearly dependent (over $F_{q^m}$) for an $A \in F_{q^m}^{n \times n}$.

Proof: The proof can be deduced from [19, Theorem 1].

Next we state a similar result for convolutional codes as follows.

Theorem 4: Let $C = \ker H(D) \subset F_{q^m}[D]^n$ has $d_{\text{rk}}(C) = d$ if and only if none of the first $n$ columns of $H_j^C$ is contained in the span of any other $d-2$ columns of $H_j^C A_{[0,j]}$ for all $A_{[0,j]} \in F_q^{(j+1) \times n(j+1)}$ and moreover one of the first $n$ columns of $H_j^C A_{[0,j]}$ is in the span of other $d-1$ columns of $H_j^C A_{[0,j]}$ for a $A_{[0,j]} \in F_q^{n(j+1) \times n(j+1)}$.

Proof: We sketch the proof as follows. Suppose that one of the first $n$ columns of $H_j^C A_{[0,j]}$ is in the span of other $d-1$ columns of $H_j^C A_{[0,j]}$ for a $A_{[0,j]} \in F_q^{n(j+1) \times n(j+1)}$. Thus, $H_j^C A_{[0,j]}$ has $d$ columns linearly dependent, say $\{c_{i_1}, c_{i_2}, \ldots, c_{i_d}\}$ and

$$\sum_{j \in S} \alpha_j c_j = 0$$

where $S = \{i_1, i_2, \ldots, i_d\}$ and at least one element in $S$, say $i_1$, belongs to $\{1, \ldots, n\}$. Take $x = (x_{1}, x_{2}, \ldots, x_{n(j+1)}) \in F_q^{n(j+1)}$ with $x_{i} = 0$ if $i \notin S$, $x_{i} = \alpha_{i}$ if $i \in S$. Then, $A_{[0,j]} x$ is a truncated codeword with at least one of the first $n$ coordinates nonzero and has rank equal to $d$. Thus, $d_{\text{rk}}(C) \leq d$.

To show that $d_{\text{rk}}(C) \geq d$ we do it by contradiction. Assume $d_{\text{rk}}(C) < d$. Then, there exists $x \in F_q^{n(j+1)}$ with at least one of the first $n$ coordinates nonzero and rank$(x) = d - 1$ such that $H_j^C x = 0$. Take $A_{[0,j]}^{-1}$ such that $A_{[0,j]}^{-1} x$ has only $d - 1$ nonzero coordinates and with at least one of the first $n$ coordinates nonzero. Then, $H_j^C A_{[0,j]} (A_{[0,j]}^{-1} x) = 0$ which implies that one of the first $n$ columns of $H_j^C$ is contained in the span of other $d-2$ columns of $H_j^C A_{[0,j]}$.

The converse follows the same reasoning.

VI. CONCLUSIONS

We have studied rank metric convolutional codes and propose a novel metric suitable for networks with delay. We have characterized such distance in terms of the corresponding parity-check matrix. It is left for future research the concrete constructions of rank convolutional codes with design column rank distance.

ACKNOWLEDGMENT

This work was partially supported by Spanish grant AICO/2017/128 of the Generalitat Valenciana and by the Portuguese Foundation for Science and Technology (FCT-Fundaçao para a Ciencia e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UID/MAT/04106/2013

REFERENCES


