23rd International Symposium on Mathematical Theory of Networks and Systems
Hong Kong University of Science and Technology, Hong Kong, July 16-20, 2018

Faster Decoding of Rank Metric Convolutional Codes

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

***Abstract*— A new construction of maximum rank distance systematic rank metric convolutional codes is presented, which permits to reduce the computational complexity of the decoding procedure, i.e., of the underlying Viterbi algorithm. This result is achieved by lowering the number of branch metrics to be calculated and by setting to the highest value the metric of the remaining edges in the trellis.**

I. Introduction

Constant-dimension subspace codes, which are one of the basic tools in Random Linear (One-Shot) Network Coding, as introduced in [1], can be easily obtained by lifting rank metric codes. Analogously, convolutional codes for Multi-Shot Network Coding (which present improved error-correction capabilities [2]–[4]) can be based on rank metric convolutional codes. The Authors established in [5] a general framework for the latter kind of codes, defining a suitable (rank) distance, deriving a Singleton-like upper bound, and showing its tightness by means of the concrete construction of Maximum Rank Distance (MRD) convolutional codes. However, the decoding process, that depends on the Viterbi algorithm, may suffer from computational issues. In this contribution, an equivalent construction of a *systematic* rank metric convolutional code will be presented, which permits to simplify both the encoding and the decoding procedures. In particular, the trellis (and, therefore, the decoding) complexity can be reduced under some assumptions on the error patterns.

The most important definitions and results from [5] will be resumed in Section II; a general construction and a state representation of the code will be given in Section III; the new construction will be introduced in Section IV and the coding and decoding strategy will be clarified by an example in Section V.

Notation

Vectors over some ring R will be represented as rows. Moreover, indices of vector and matrices, like powers of polynomials, will start from zero. Therefore, the vector $v \in R^n$ will be written componentwise as $v = (v_0, \ldots, v_{n-1})$ or $v = [v_0 \cdots v_{n-1}]$. Consequently, we assume that $0 \in \mathbb{N}$.

[1]Department of Mathematics, University of Aveiro, 3810-197 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, Winterthurerstrasse 190, CH-8057 Zürich, Switzerland. Email: rosenthal at math.uzh.ch
Partially supported by the the Swiss National Science Foundation under grant no. 169510.

We will denote by $\mathrm{rowvec} : M \mapsto v$ the R-isomorphism $R^{n\times m} \to R^{mn}$ such that $v_{mi+j} = M_{i,j}$, with $0 \le i < n$ and $0 \le j < m$, constructing a block row vector with the matrix rows. This is the 'row' equivalent of the the standard (column) vectorization of a matrix, i.e., the vec map, being $\mathrm{rowvec}(M) = \mathrm{vec}(M^\top)^\top$.

The inverse of the rowvec map, stacking the $1 \times m$ blocks of an R^{mn} vector into an $n \times m$ matrix, will be denoted by rowmat or $\mathrm{rowmat}_{n\times m}$.

II. Rank Metric Convolutional Codes

Being based on rank metric codes as introduced by Delsarte in [6], and not on Gabidulin codes [7], the approach of this paper differs from the one that can be found in the literature on rank metric convolutional codes (see [3], [4]). Actually, following [8], we will start recalling completely general definitions of linear (matrix) rank metric codes and of convolutional codes over a finite field $\mathbb{F}_q$ of size q.

Definition 1: [5] An $(n \times m, k)$ *linear rank metric code* $\mathscr{C}$ is the image of a monomorphism $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^{n\times m}$, equipped with the rank distance: $d(A,B) = \mathrm{rank}(A - B)$, $A, B \in \mathscr{C}$.

Note that the monomorphism φ can be seen as a composition of a monomorphism $\gamma : \mathbb{F}_q^k \to \mathbb{F}_q^{nm}$, represented by a matrix $G \in \mathbb{F}_q^{k\times nm}$, and of an isomorphism $\psi : \mathbb{F}_q^{nm} \to \mathbb{F}_q^{n\times m}$.

Definition 2: A convolutional code is a submodule of $\mathbb{F}_q[z]^n$.

Since $\mathbb{F}_q[z]$ is a principal ideal domain, for any convolutional code there exist a full row rank matrix $G(z) \in \mathbb{F}_q[z]^{k\times n}$, the *encoder*, such that the code is the image of $G(z)$ over $\mathbb{F}_q[z]$.

Besides the dimensions of $G(z)$, another important parameter of a convolutional code is its degree δ, i.e., the maximal degree of the $k \times k$ minors of $G(z)$. If δ_i, $0 \le i < k$ are the degrees of the rows $G_i(z)$ of $G(z)$, it can be proved that $\delta \le \delta_0 + \cdots + \delta_{k-1}$ and that this relation holds as an equality for some equivalent (*minimal*) encoder $G'(z)$. Without loss of generality, we will always assume that encoders are minimal.

To come up with a definition of rank metric convolutional codes, it is sufficient to combine the two previous definitions.

Definition 3: A *rank metric convolutional code* $\mathscr{C}$ is the image of an homomorphism $\varphi : \mathbb{F}_q[z]^k \to \mathbb{F}_q[z]^{n\times m}$.

In this case too, we may write $\varphi = \psi \circ \gamma$ as a composition of a monomorphism γ and a degree-preserving isomorphism ψ:

$$\begin{aligned} \varphi : \mathbb{F}_q[z]^k \;&\xrightarrow{\gamma}\; \mathbb{F}_q[z]^{nm} \;\xrightarrow{\psi}\; \mathbb{F}_q[z]^{n\times m} \\ u(z) \;&\mapsto v(z) = u(z)G(z) \mapsto \;\; V(z) \end{aligned} \tag{1}$$

If the degree of the code is δ, computed as in the convolutional case from the encoder $G(z)$, we say that $\mathscr{C}$ is a $(n \times m, k, \delta)$-rank metric convolutional code.

The distance of a code $\mathscr{C}$ is defined as the minimum distance between different codewords $X(z), Y(z) \in \mathscr{C}$, i.e., the minimum of the *sum rank distance* d_{SR} between $X(z) = \sum_{i\in\mathbb{N}} X^{(i)} z^i$ and $Y(z) = \sum_{i\in\mathbb{N}} Y^{(i)} z^i$ in $\mathbb{F}_q[z]^{n\times m}$:

$$d_{\mathrm{SR}}\big(X(z),Y(z)\big) = \sum_{i\in\mathbb{N}} \operatorname{rank}(X^{(i)} - Y^{(i)}). \tag{2}$$

(See [5] for the proof that (2) is actually a distance.)

The following bound on the code distance holds true.

Theorem 4: Let $\mathscr{C}$ be an $(n \times m, k, \delta)$-rank metric convolutional code with distance d. Then,

$$d \le n \left\lceil \frac{\delta+1}{k} \right\rceil - \left\lceil \frac{k\left\lceil \frac{\delta+1}{k}\right\rceil - \delta}{m} \right\rceil + 1. \tag{3}$$

A rank metric convolutional code whose distance attains the upper bound (3) is called *maximum rank distance* (MRD) convolutional code.

III. A Basic MRD Code Construction

To prove that the bound given by (3) is tight, it is sufficient to show that MRD codes exist: a general construction of an MRD $(n \times m, k, \delta)$-rank metric convolutional code over $\mathbb{F}_q$, with $m \ge n$, will be given for any degree satisfying $\delta \le m - k$.

Given any matrix $P \in \mathbb{F}_q^{m\times m}$ with irreducible characteristic polynomial, let

$$S^{\langle i\rangle} = TP^i, \tag{4}$$

where $T \in \mathbb{F}_q^{n\times m}$ is a full row rank matrix. Define the $k \times nm$ matrices

$$G^{(i)} = \begin{bmatrix} \psi^{-1}(S^{\langle ki\rangle}) \\ \psi^{-1}(S^{\langle ki+1\rangle}) \\ \vdots \\ \psi^{-1}(S^{\langle ki+k-1\rangle}) \end{bmatrix},\ 0 \le i \le \left\lfloor \frac{\delta}{k} \right\rfloor, \text{ and}$$

$$G^{(\lceil \frac{\delta+1}{k} \rceil)} = \begin{cases} 0 & \text{if } k \text{ divides } \delta, \\ \begin{bmatrix} \psi^{-1}(S^{\langle k\lfloor \frac{\delta}{k}\rfloor + k\rangle}) \\ \vdots \\ \psi^{-1}(S^{\langle k+\delta-1\rangle}) \\ 0 \\ \vdots \\ 0 \end{bmatrix} & \text{otherwise.} \end{cases} \tag{5}$$

Theorem 5: [5] The $(n \times m, k, \delta)$-rank metric convolutional code $\mathscr{C}$, with encoder

$$G(z) = \sum_{i=0}^{\lceil \frac{\delta+1}{k} \rceil} G^{(i)} z^i \in \mathbb{F}_q[z]^{k\times nm}, \tag{6}$$

whose coefficients are defined in (5), is MRD when $m \ge \delta + k$.

In order to apply the Viterbi algorithm, a state space representation is needed. Using the notation of (1), the input of the system is given by message $u(z)$ and the output by $v(z)$, which is then transformed into codeword $V(z)$ by isomorphism ψ. Therefore, a state space representation is be given by the following equations:

$$\begin{cases} x^{(i+1)} = x^{(i)}A + u^{(i)}B, & x^{(0)} = 0, \\ v^{(i)} = x^{(i)}C + u^{(i)}D, V^{\langle i\rangle} & = \psi(v^{\langle i\rangle}). \end{cases} \tag{7}$$

One possible choice of matrices A, B, C, D is the following: consider the (block) matrix

$$M = \left[\begin{array}{c|c} I_\delta & \begin{matrix} \psi^{-1}(S^{\langle 0\rangle}) \\ \psi^{-1}(S^{\langle 1\rangle}) \\ \vdots \end{matrix} \\ \hline 0 & \psi^{-1}(S^{\langle k+\delta-1\rangle}) \end{array}\right] \in \mathbb{F}_q^{(\delta+k)\times(\delta+mn)}.$$

Then the system is defined by partitioning M as follows:

$$M = \left[\begin{array}{c|c} B & D \\ \hline A & C \end{array}\right] \in \mathbb{F}_q^{(k+\delta)\times(\delta+mn)},$$

where $A \in \mathbb{F}_q^{\delta\times\delta}$ is the state update matrix.

A concrete example of the constructions presented in this section will be given in Section V.

IV. Better Encoding, Faster Decoding

As is well known, the number of states of the Viterbi algorithm is q^δ, growing exponentially, but the bigger problem is here constituted by the even higher number of rank distances to be computed, i.e., $q^{k+\delta}$. Besides, the first m powers of an $m \times m$ matrix are needed for the encoder. In order to understand how the situation can be simplified, it is better to have a closer look at the encoder (6).

Consider a polynomial message $u(z) = \sum_{i\in\mathbb{N}} u^{(i)} z^i$. The codeword is $V(z) = \psi\big(u(z)G(z)\big)$ and thus, by (5),

$$\begin{aligned} V^{(0)} &= \psi\left(u^{(0)}G^{(0)}\right) = \psi\left(\sum_{i=0}^{k-1} u_i^{(0)} \psi^{-1}(S^{\langle i\rangle})\right) \\ &= \sum_{i=0}^{k-1} u_i^{(0)} \psi\left(\psi^{-1}(S^{\langle i\rangle})\right) = \sum_{i=0}^{k-1} u_i^{(0)} S^{\langle i\rangle}. \end{aligned}$$

Analogously, $V^{(1)}$ will be the linear combination of $S^{\langle 0\rangle}, \dots, S^{\langle 2k-1\rangle}$ whose coefficients are the $2k$ components of $u^{(1)}$ and $u^{(0)}$ (in that order), and so on for $V^{(2)}, V^{(3)}, \dots$.

By a property of matrices over finite fields, every nonzero linear combination of the first m powers of P has full rank (equal to m). Consequently, every linear combination of $S^{\langle 0\rangle}, \dots, S^{\langle k+\delta-1\rangle}$ has full rank (n) if $k + \delta \le m$. This fact guarantees that the sum rank distance is maximized and thus the code is MRD.

However, any other choice of matrices $S^{\langle i\rangle}$, exhibiting the same behavior, would also generate an MRD code.

Suppose that $m \ge 2n$ and let r be the remainder of the integer division of m by n, i.e., $m = (\ell+1)n + r$, $0 \le r < n$. Consider then matrices P and Q, which are the companion matrices of two irreducible polynomials of degree, respectively, n and $n+r$ (the polynomials coefficients appearing on the last row). If $r = 0$, then let simply $Q = P$. For example,

$$P = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \tag{8}$$

is the companion matrix of the irreducible polynomial $p(x) = 1+x+x^2$ in $\mathbb{F}_2$.

Finally, let $T = \left[I_n \mid 0\right]$. Then, matrices $S^{\langle\cdot\rangle} \in \mathbb{F}_q^{n\times m}$ can be constructed as follows, with $0 \le i < n$ and $0 \le j < n+r$:

$$\begin{aligned} S^{\langle i\rangle} &= \left[P^i \,|\, 0_{n\times(m-n)}\right], \\ S^{\langle n+i\rangle} &= \left[0_{n\times n} \,|\, P^i \,|\, 0_{n\times(m-2n)}\right], \\ &\vdots \\ S^{\langle(\ell-1)n+i\rangle} &= \left[0_{n\times(\ell-1)n} \,|\, P^i \,|\, 0_{n\times(m-\ell n)}\right], \\ S^{\langle \ell n+j\rangle} &= \left[0_{n\times\ell n} \,|\, TQ^j\right]. \end{aligned}$$

These m matrices are formed by ℓ $n\times n$ and one $n\times(n+r)$ blocks and their nonzero linear combinations have full rank: indeed, at least one block would be nonzero, thus having rank n, by the aforementioned property of matrices P and Q.

The advantages of this choice with respect to the simpler one given in (4) are the following.

Encoding:

1) less powers of smaller matrices are needed;
2) powers of companion matrices have simple structure and both P^i and TQ^i have in the first row just a one in the i-th entry;
3) the code is systematic, since $u^{(i)}$ shows up in the first k entries of the first row of $V^{(i)}$.

Decoding:

4) each block can be checked for errors by 'reconstructing' it from the first row;
5) only the blocks containing errors have to be further analyzed to construct the trellis metrics;
6) the metrics which do not have to be computed are equal to the maximum (rank) distance, i.e., n.

These facts will be clarified in the following example, but the last two deserve a brief explanation. In the following, recall that the metric is the distance between the system ($n\times m$ matrix) output, associated with input and state of the branch, and the received ($n\times m$) coefficient of the codeword.

Suppose that one block (the first, for instance) of the received matrix is equal to X and does not present any errors. For any possible coefficient, let Y be the value of its first block. If $X \neq Y$, then $X-Y$ is again a linear combination of the powers of P, thus has rank n; therefore, the (rank) distance, i.e., the metric of the branch, is also n. We conclude that the branch metric might be less than n only if $X = Y$. Repeating the same reasoning for every block without errors will reduce the number of possible branches with metric less than n (which has to be computed) and set the metric to n (without computing any distance) for all the other edges of the trellis.

V. Coding and Decoding Example

Consider a $(2\times 4, 2, 2)$-rank metric convolutional code $\mathscr{C}$ over $\mathbb{F}_2$. Our constructions provide MRD codes since, by Theorem 5, $k+\delta = 2+2 \le 4 = m$.

Note that definition (4) would require the construction, and the linear combination, of four 2×4 matrices. Instead, according to the definition given in Section IV, just I_2 and P as in (8) are needed: matrices $S^{\langle i\rangle}$, $0 \le i < 4$ are

$$S^{\langle 0\rangle} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \qquad S^{\langle 1\rangle} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$
$$S^{\langle 2\rangle} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad S^{\langle 3\rangle} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

By defining $\psi = \mathrm{rowmat}_{2\times 4}$, the enconder $G(z)$ and the matrices A, B, C, D of the state space system are:

$$G(z) = \begin{bmatrix} 1 & 0 & z & 0 & 0 & 1 & 0 & z \\ 0 & 1 & 0 & z & 1 & 1 & z & z \end{bmatrix}, \quad A = 0_{2\times 2}, \quad B = I_2,$$
$$C = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

Thus, given some message $u(z) = u^{(0)} + u^{(1)}z + u^{(2)}z^2 + \cdots$, the codeword would be $V(z) = V^{(0)} + V^{(1)}z + V^{(2)}z^2 + \cdots$, corresponding to the following sequence of 2×4 matrices, which shows a manifest *systematic part* (the second row is not considered here)

$$(V^{(i)}) = \left(\begin{bmatrix} u^{(0)} & x^{(0)} \\ \multicolumn{2}{c}{\star} \end{bmatrix}, \begin{bmatrix} u^{(1)} & x^{(1)} \\ \multicolumn{2}{c}{\star} \end{bmatrix}, \begin{bmatrix} u^{(2)} & x^{(2)} \\ \multicolumn{2}{c}{\star} \end{bmatrix}, \ldots \right),$$

where the state is just a delayed version of the message, i.e.,

$$(V^{(i)}) = \left(\begin{bmatrix} u^{(0)} & 0 \\ \multicolumn{2}{c}{\star} \end{bmatrix}, \begin{bmatrix} u^{(1)} & u^{(0)} \\ \multicolumn{2}{c}{\star} \end{bmatrix}, \begin{bmatrix} u^{(2)} & u^{(1)} \\ \multicolumn{2}{c}{\star} \end{bmatrix}, \ldots \right).$$

As for the encoding, observe that the first row of P is equal to the last row of $I_2 = P^0$: actually, for a $n\times n$ companion matrix, every power shares the last $n-1$ rows with the following one. This means that, besides $P^0 = I_n$ ('containing' the canonical basis, whose elements appear in the first row of the successive powers of P), only $n-1$ more rows are necessary to build all the powers up to $n-1$.

In this case, the possible nonzero linear combinations of powers of P that can appear in each block are

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad P = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad I_2 + P = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} (= P^2).$$

Observe that the linear combination of P^0 and P^1, using the first row entries as coefficients, *reconstruct* any matrix; the same property holds for matrices $V^{(i)}$, as a linear combination of $S^{\langle 0\rangle}, \ldots, S^{\langle 3\rangle}$, thus permitting easy errors detection.

Finally, the Viterbi algorithm is based on a state with dimension 2, i.e., with size $q^\delta = 2^2 = 4$ and every state is connected to the following state by 4 edges (4 values of $u^{(i)}$). For the general case, as in Figure 1, 16 edges should be checked: if $\tilde{V}^{\langle i\rangle}$ is the received codeword coefficient and $V(x^{\langle i\rangle}, u^{\langle i\rangle})$ is the matrix corresponding to the transition from state $x^{\langle i\rangle}$ with message coefficient $u^{\langle i\rangle}$, then it is necessary to compute the distance $\mathrm{rank}\left(\tilde{V}^{\langle i\rangle} - V(x^{\langle i\rangle}, u^{\langle i\rangle})\right)$ for each of the 16 edges.

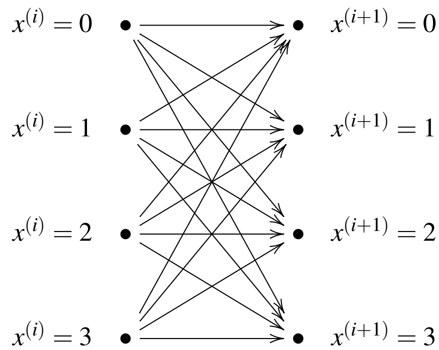

Fig. 1. Complete trellis: 16 edges.

If the first block does not have errors and the second has, then the value of $u^{(i)}$ is known (and it will be the next state). Therefore it is necessary to compute the metrics of the edges corresponding to the 4 states, as in Figure 2. The other edges (dotted) have rank distance $n = 2$.

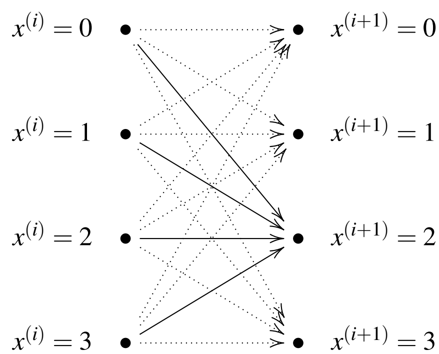

Fig. 2. Trellis with known input ($u^{(i)} = 2$)

If, on the contrary, the first block has errors and the second is error-free, then the value of the state is known. Therefore it is necessary to compute the metrics of the edges corresponding to the four values of the input u, as in Figure 3. The other edges (dotted) have rank distance $n = 2$.

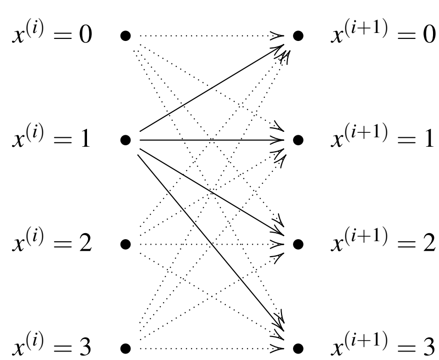

Fig. 3. Trellis with known state ($x^{(i)} = 2$)

Finally, if no errors occurred, the value of the input and the state are known and the edge connecting them has rank distance 0, as in Figure 4. All the other edges (dotted) have rank distance $n = 2$.

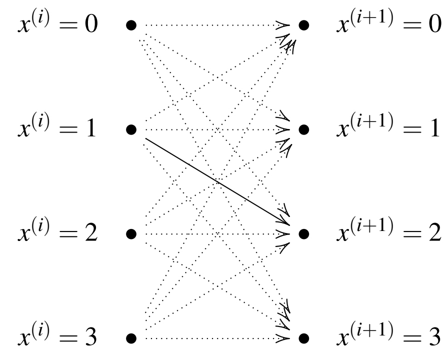

Fig. 4. Trellis with known input and state ($u^{(i)} = 2$, $x^{(i)} = 1$)

VI. Conclusions

A new encoding scheme for MRD rank metric convolutional codes has been presented. By dividing the matrix codeword into smaller blocks, the construction previously proposed in [5] was improved, enhancing both the encoding and the decoding procedures.

The encoder needs less resources and the process can be carried out in a parallel manner on each block. As for the decoder, each block can be checked for errors independently. For every block that is free of errors, the global computational complexity of the Viterbi algorithm is reduced: a low error probability or bursts affecting (parts of) a small number of blocks are therefore the most favorable situations.

As a last remark, observe that the trellis could be further reduced by first checking and correcting (even partially) each received matrix coefficient, which is itself a codeword of a rank metric (block) code. For instance, also the systematic part of the codeword could be used.

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, Aug. 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*, Jun. 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, Jun. 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] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori, “MRD rank metric convolutional codes,” in *2017 IEEE International Symposium on Information Theory (ISIT)*, Jun. 2017, pp. 2771–2775. DOI: 10.1109/ISIT.2017.8007033.

[6] P. Delsarte, “Bilinear forms over a finite field, with applications to coding theory,” *Journal of Combinatorial Theory, Series A*, vol. 25, no. 3, pp. 226–241, 1978, ISSN: 0097-3165. DOI: https://doi.org/10.1016/0097-3165(78)90015-8. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0097316578900158.

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

[8] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori, “Rank metric convolutional codes,” in *Proceedings of the 22nd International Symposium on Mathematical Theory of Networks and Systems*, Jul. 2016, pp. 361–363. [Online]. Available: http://conservancy.umn.edu/handle/11299/181518.