The Capacity of Random Linear Coding Networks as Subspace Channels

Bartolomeu F. Uchôa-Filho and Roberto W. Nóbrega
Communications Research Group
Department of Electrical Engineering
Federal University of Santa Catarina
Florianópolis, SC, 88040-900, Brazil
E-mail: {uchoa,rwnobrega}@eel.ufsc.br

Abstract—In this paper, we consider noncoherent random linear coding networks (RLCNs) as a discrete memoryless channel (DMC) whose input and output alphabets consist of subspaces. This contrasts with previous channel models in the literature which assume matrices as the channel input and output. No particular assumptions are made on the network topology or the transfer matrix, except that the latter may be rank-deficient according to some rank deficiency probability distribution. We introduce a random vector basis selection procedure which renders the DMC symmetric. The capacity we derive can be seen as a lower bound on the capacity of noncoherent RLCNs, where subspace coding suffices to achieve this bound.

I. INTRODUCTION

Random linear network coding (RLNC), proposed by Ho et al. [1], is a very attractive way to obtain the benefits of linear network coding [2, 3] in dynamically changing or large scale networks. In a decentralized way, by requiring the intermediate nodes to randomly combine incoming packets over a finite field, RLNC achieves the network min-cut with probability approaching one as the field size goes to infinity. For this reason, RLNC is an important research topic and has recently received a great deal of attention. Following [4], we call a network employing RLNC a random linear coding network (RLCN).

In order to recover the transmitted packets, a receiving node needs to know its associated network transfer matrix. In reality, the transfer matrix depends on the network topology and the network code used. However, to allow for some analysis, in previous works on RLCNs authors have made different assumptions on the characteristics of the transfer matrix, which has been assumed to have full rank [5], bounded rank deficiency [7], or entries selected uniformly at random [8], [9]. Also, it has been considered as being selected either by an adversary [7] or uniformly at random among all nonsingular matrices [5].

In some works, the approach for the capacity of RLCNs is combinatorial. For example, in [10], where the authors consider the noncoherent scenario in which the transfer matrix is assumed unknown to both the transmitter and the receiver, a subspace coding approach is prescribed and coding size bounds under a topology-independent operator channel model are provided.

A probabilistic approach for the capacity of RLCNs was first presented by Montanari and Urbanke [6], who have considered an additive perturbation (error) matrix chosen uniformly at random from all matrices of given dimension and rank. Later, their work was further extended by Silva et al. [5], who have considered both the transfer and the error matrices as chosen according to more general probability distributions.

Recently, Yang and Yang [4] have called the attention to the importance of understanding how network topologies affect RLNC. More specifically, they studied a particular family of unicast networks and identified a worst-case unicast network topology: the S-networks. They derived a capacity formula for S-networks, and showed that for this topology subspace coding is optimal in the sense that it suffices to achieve capacity. Similar conclusions regarding the use of subspace coding were reached in [8], [9]. However, in these works, RLCNs are seen as a channel not with subspaces but with matrices as inputs and outputs.

In this paper, we consider the noncoherent scenario of [10] and make no particular assumption on the network topology or the network code used. Since the transmission strategy using subspaces is oblivious to the underlying network topology and to the particular linear combinations performed at the network nodes [10], and since no other coding approach seems more suitable to the noncoherent scenario, we begin by treating RLCNs as a discrete memoryless channel (DMC) with subspaces as inputs and outputs. We build up a channel model for RLCNs that depends solely on the dimension of the subspaces that constitute the input alphabet and the rank deficiency probability distribution associated with the RLCN. The problem is that it is difficult to characterize such channel because, as we will see, under certain conditions, the received subspace depends on the choice of the transmitted matrix. Also, due to the many forms the transfer matrix can take, it is difficult, if not impossible, to characterize this channel simply from the rank deficiency probability distribution.

We overcome these drawbacks by introducing a random basis selector, a device which selects a matrix uniformly at random from the set of all ordered bases for the subspace. This idea has been mentioned in [10] as a way to saying that in subspace coding there is no benefit in choosing a particular basis for transmitting a given subspace. A similar
randomization procedure is also followed in [6], with the purpose of facilitating the decoding algorithm. Completely innocuous from the subspace coding perspective, this random basis selection plays a fundamental role in the characterization of the channel and in the derivation of its capacity, as we show in the present paper.

Interestingly, the capacity formula we derive exactly corresponds to the one in [4], which has been derived for a specific network topology. Our conclusions regarding noncoherent RL-CNs parallel those in [4]: while Yang and Yang conclude that the capacity of unicast networks with given topology is lower bounded by the capacity of S-networks, we conclude that the same lower bound applies to the capacity of noncoherent RL-CNs for general (unknown) topology, and that subspace coding is sufficient to achieve this bound.

The paper is organized as follows. In the next section, we describe the system model and review some important concepts for the forthcoming derivations. In Section III, where the main contribution of this work is presented, we characterize the subspace channel model for RL-CN and derive its channel capacity. Finally, in Section IV we present our conclusions and final comments.

II. PRELIMINARIES AND NOTATION

In this paper, random entities are represented using boldface letters, while italic letters are used for their samples. However, the letters $O$, $U$, and $V$ are reserved to denote subspaces.

A. Random Linear Coding Networks as a Matrix Channel

Consider a time-varying network with one source node and one sink node (unicast), with the intermediate nodes performing uniform random linear combining over a finite field $\mathbb{F}_q$, where $q$ is a prime power. At time slot $t$, the matrix channel for this network is given by

$$Y(t) = G(t)X(t),$$

where $X(t)$ is the $m \times T$ transmitted matrix and $Y(t)$ is the $n \times T$ received matrix. The rows of $X(t)$ (resp., $Y(t)$) represent the $m$ (resp., $n$) transmitted (resp., received) packets, which are seen as vectors over $\mathbb{F}_q$. $G(t)$ is the network transfer matrix, an $n \times m$ random matrix over $\mathbb{F}_q$ whose entries depend on the network topology and the network code used. The time slot is the time during which $G(t)$ remains constant, and also corresponds to $T$ uses of the network, where $T$ is the packet size. In this paper, we assume that both the transfer matrix and the network topology are unknown to both the transmitter and the receiver. Following [5, 6], however, we assume for simplicity a square transfer matrix with known dimension $m = n = h$ fixed at all times.

Due to unfortunate selection of random coefficients, the network transfer matrix may be rank-deficient. According to the channel model in [1], the rank deficiency of $G(t)$, herein denoted as $\tau_G(t)$, is a discrete-time stochastic process. We assume that $\tau_G(t)$ is first-order stationary so that a probability distribution of $\tau_G(t)$, which is independent of $t$, exists and is given by $\mathbb{P}_{\tau_G}(r)$, where $r = 0, \ldots, h$.

In practice, if this process is ergodic, its probability distribution can be estimated at the sink node by continuously updating a histogram based on the rank deficiency$^1$ of the received matrix $Y(t)$. The probability distribution can then be communicated to the source node through a low-rate feedback channel, either from time to time or once and for all when a steady distribution is reached. From now on, we will drop the time index $t$ in all variables for convenience.

B. Subspace Coding

The idea behind subspace coding is that, since the received vectors are linear combinations of the transmitted vectors, the vector space spanned by the transmitted vectors is preserved. So, in subspace coding, information is encoded in the choice of a subspace of the vector space $\mathbb{F}_q^n$ [10]. We denote by $(X)$ the subspace spanned by the rows of the transmitted matrix $X$.

A subspace code is then a subset of the projective space $P(\mathbb{F}_q^n)$, which is the collection of all subspaces of $\mathbb{F}_q^n$. A codeword of a subspace code is one of these subspaces. This contrasts with the notion of classical linear block coding, where a code is a subspace and a codeword is a vector in this subspace.

Most known subspace codes are constant-dimension codes, or codes in the Grassmannian, i.e., subspace codes whose all codewords have the same dimension. We denote the Grassmannian of dimension $h$ by $P(\mathbb{F}_q^h)$, so that $P(\mathbb{F}_q^n) = \bigcup_{h=0}^{n} P(\mathbb{F}_q^h)$. The number of distinct $\ell$-dimensional subspaces of an $n$-dimensional vector space over $\mathbb{F}_q$ is given by

$$\binom{n}{\ell}_q = \frac{q^{n-\ell} - 1}{\ell!},$$

known as the $q$-ary Gaussian coefficient.

Although the use of subspaces of multiple dimensions is optimal under certain circumstances [9], there has been an increasing interest in constant-dimension codes, chiefly due to their simpler encoding and decoding algorithms.

In [7], Silva et al. have given an important construction of constant-dimension codes which builds upon a lifting of a class of maximum rank-metric codes due to Gabidulin [11]. More recently, in [12], Silva and Kschischang have presented new fast encoding and decoding algorithms for Gabidulin codes that can be used towards their lifted counterpart.

C. Discrete Memoryless Channels

A DMC is defined by the triplet $(X', p_{Y|X}, Y)$, where $X'$ (resp., $Y$) is the channel input (resp., output) alphabet, and $p_{Y|X}(Y|X)$ is the conditional probability that $Y \in Y$ is received given that $X \in X'$ is sent. The channel is memoryless in the sense that what happens to the transmitted symbol at one time is independent of what happens to the transmitted symbol at any other time. Let $X$ and $Y$ be the random entities representing the input and output symbols, respectively. The

$^1$Recall that, if $X$ is full-rank then $\tau_Y = \tau_G$ if $Y = GX$. 
channel capacity of the DMC is then given by
\[ C = \max_{p_X(X)} I(X; Y) \]
\[ = \max_{p_X(X)} H(X) - H(X | Y) = \max_{p_X(X)} H(Y) - H(Y | X), \]
where \( I(X; Y), H(X) \) (resp., \( H(Y) \)), and \( H(X | Y) \) (resp., \( H(Y | X) \)) are the mutual information between \( X \) and \( Y \), the entropy of \( X \) (resp., \( Y \)), and the conditional entropy of \( Y \) (resp., \( X \)) given \( X \) (resp., \( Y \)), respectively. The maximization in (2) is over all possible input distributions \( p_X \).

The points of the distribution \( p_{Y|X}(Y | X) \) for all \( X \in \mathcal{X} \) and all \( Y \in \mathcal{Y} \) can be arranged in a matrix, called the transition probability matrix, where the \( X \)'s (resp., \( Y \)'s) are related to the rows (resp., columns).

A DMC can be pictorially described by a bipartite graph, where the nodes at left (resp., right) represent the input (resp., output) alphabet. Each input (resp., output) node has a number of sockets from (resp., to) which edges emanate (resp., connect). If an output symbol occurs with some nonzero probability given an input symbol, then there is an edge connecting the corresponding input node to the output node. Of course, the total number of sockets on the \( X \) side equals the total number of sockets on the \( Y \) side.

The following definitions and theorems have been adapted from [13], [14].

**Definition 1:** A DMC is uniformly dispersive (resp., focusing) if all the rows (resp., columns) of the transition probability matrix are permutations of each other. A DMC that is both uniformly dispersive and uniformly focusing is said to be strongly symmetric.

**Theorem 1:** For a strongly symmetric DMC, the capacity is given by
\[ C = \log |\mathcal{Y}| - H(p), \]
where \( H(p) \) denotes the entropy of the probability vector \( p \), formed by the elements of a row of the transition probability matrix. Moreover, this capacity is achieved by the uniform input distribution.

If a channel is uniformly dispersive but not uniformly focusing, it may still have a weaker form of symmetry.

**Definition 2:** A uniformly dispersive DMC is said to be symmetric (also known as component-symmetric) if, for some \( L \), it can be decomposed into \( L \) strongly symmetric channels with selection probabilities \( q_0, \ldots, q_{L-1} \).

**Theorem 2:** For a symmetric DMC, the capacity is given by
\[ C = \sum_{i=0}^{L-1} q_i C_i, \]
where \( C_i \) is the capacity of the \( i \)-th component strongly symmetric channel associated with the symmetric DMC.

**III. THE CAPACITY OF THE SUBSPACE CHANNEL AS A SYMMETRIC DMC**

We want to characterize the DMC
\[ (\mathcal{X} = \mathcal{P}(\text{I}^T_q, h), p(\mathcal{Y} | (X)), \mathcal{Y} = \bigcup_{r=0}^h \mathcal{P}(\text{I}^T_q, r)) \]
serving as a channel model for RLCNs essentially without any assumption on the network topology or the particular network code used. The main goal is to characterize the conditional probability \( p(\mathcal{Y} | (X)) \) that the subspace \( (Y) \) is received when subspace \( (X) \) is sent as a function of the rank deficiency probability distribution \( p_{\tau}(r) \). The difficulties related to the characterization of this DMC, raised in the introductory section, will be illustrated by the next two examples.

**Example 1:** Let \( U = \{000, 010, 100, 110\} \) be the input subspace. There are six different basis matrices for \( U \), two of which are
\[ X = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad X' = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}. \]
Suppose that \( G \) has rank deficiency \( \tau_G = 1 \) and is given by
\[ G = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}. \]

For the corresponding received matrices, \( Y = GX \) and \( Y' = GX' \), the associated one-dimensional output subspaces are \( \langle Y \rangle = \{000, 100\} \) and \( \langle Y' \rangle = \{000, 110\} \), respectively.

We can see from Example 1 that, given the input subspace \( U \) and a fixed non-zero, rank-deficient transfer matrix \( G \), the output subspace may depend on the selection of the basis for \( U \). The first difficulty resides on the fact that a different DMC results for each possible combination of bases selections for input subspaces, and there is an exponentially large number of them.

Characterizing our DMC is also difficult because the network code can affect the transmitted matrix \( X \) (and the input subspace \( (X) \)) in too many ways. The next example illustrates the problem.

**Example 2:** Consider the same input subspace \( U \) in Example 1 and \( X' \) as the transmitted matrix. Also, suppose again that \( \tau_G = 1 \) but with the transfer matrix given by
\[ G' = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \]

The received matrix, \( Y'' = G'X' \), gives rise to the output subspace \( \langle Y'' \rangle = \{000, 010\} \).

We can see from Example 2 that, for a fixed transmitted matrix \( X' \), different transfer matrices with the same rank deficiency may produce different output subspaces. (Note that this problem does not exist if the distinct transfer matrices have full rank.) As a result, for a fixed rank deficiency probability distribution the DMC is not fixed, but varies according to the realization of \( G \). In other words, a DMC for the subspace channel cannot be defined solely from rank deficiencies even if a fixed mapping \( U \to X \) with \( (X) = U \) were specified for every subspace \( U \) in the Grassmannian.

We remedy these problems by introducing a random basis selector. We show that, upon using a basis matrix \( X \) produced by this device, the resulting DMC represents RLCNs, and is both well-defined and consistent with the subspace coding approach. Given a subspace \( U \in \mathcal{X} \) at the input of the selector, it outputs a matrix \( X \) which is selected, uniformly
the transition probability distribution is given by
\[ p_{X|\langle X \rangle}(X|U) = \prod_{i=1}^{h} (q^h - q^{i-1})^{-1}, \] (3)
where the inverse of 3 is exactly the number of ordered bases that span a subspace \( U \) in \( \mathcal{P}(\mathbb{F}_q^T, h) \) \[ \mathcal{P}(\mathbb{F}_q^T, r) \]. From now on, when we refer to a DMC we mean the DMC that models RLCNs under this random basis selection.

We now prove that the distribution \( p_{\langle Y \rangle|\langle X \rangle} \) is fully characterized by the rank deficiency probability distribution only, and is conditionally independent of the network topology and the network code used.

**Theorem 3**: For the DMC
\[ (\mathcal{P}(\mathbb{F}_q^T, h), p_{\langle Y \rangle|\langle X \rangle}, \bigcup_{r=0}^{h} \mathcal{P}(\mathbb{F}_q^T, r)), \]
the transition probability distribution is given by
\[ p_{\langle Y \rangle|\langle X \rangle}(V|U) = \begin{cases} \frac{p_{\mathcal{C}}(h - \dim V)}{h}, & \text{if } V \subseteq U \\ 0, & \text{else.} \end{cases} \]

**Proof**: We begin by expanding the conditional probability distribution \( p_{\langle Y \rangle|\langle X \rangle, \tau_G} \) as follows:
\[
P_{\langle Y \rangle|\langle X \rangle, \tau_G}(V|U, \rho) = \sum_X p_{\langle X \rangle, \tau_G}(X|U, \rho) \cdot p_{\langle Y \rangle|\langle X \rangle, \tau_G}(V|X, U, \rho)
= \sum_{X:|X|=U} p_{\langle X \rangle}(X|U) \cdot p_{\langle Y \rangle|\langle X \rangle, \tau_G}(V|X, \rho)
= \prod_{i=1}^{h} (q^h - q^{i-1})^{-1} \sum_{X:|X|=U} p_{\langle X \rangle}(X|\tau_G(V|X, \rho), (4)
where we used the fact that \( X \) is conditionally independent of \( \tau_G \) given \( \langle X \rangle \) and the result in 3 for \( p_{\langle X \rangle|\langle X \rangle} \). The summation in 4 can be obtained as follows. Suppose that \( G \) is some fixed (unknown) matrix \( G \) over \( \mathbb{F}_q \) with \( |G| = \rho = h - \dim V \). Then the transmitted matrix \( X \) is mapped into some output subspace \( \langle GX \rangle = V' \) with probability one. So, the summation in 4 is either 1 (if \( V' = V \)) or zero (if \( V' \neq V \)). The resulting sum is thus the number of ordered bases \( X \) that span the subspace \( U \) in \( \mathcal{P}(\mathbb{F}_q^T, h) \) and that produce \( \langle GX \rangle = V \) as output subspace. Since the range of \( X \) is the set of all ordered bases that span the subspace \( U \), by symmetry, the summation in 4 is exactly the total number of ordered bases that span the subspace \( U \) divided by the total number of subspaces of dimension \( \dim V \) of \( U \), which is given by
\[
\prod_{i=1}^{h} (q^h - q^{i-1})^{-1} \sum_{X:|X|=U} p_{\langle X \rangle}(X|\tau_G(V|X, \rho), (4)
\]
with this result, 4 becomes
\[
P_{\langle Y \rangle|\langle X \rangle}(V|U) = \begin{cases} \frac{1}{h}, & \text{if } V \subseteq U, \rho = h - \dim V \\ 0, & \text{else.} \end{cases} \]
We now write
\[
P_{\langle Y \rangle|\langle X \rangle}(V|U) = \sum_{r=0}^{h} p_{\langle Y \rangle|\langle X \rangle, \tau_G}(V|U, r) \cdot p_{\tau_G}(r)
= p_{\langle Y \rangle|\langle X \rangle, \tau_G}(V|U, h - \dim V) \cdot p_{\tau_G}(h - \dim V),
\] which completes the proof.

From Theorem 3 we should note that the conditional probability \( p_{\langle Y \rangle|\langle X \rangle}(V|U) \) depends on the dimension of \( V \) (but not on \( U \) itself) and is independent of \( U \) given that \( V \subseteq U \). Since the number of subspaces of dimension \( \dim V \) of a subspace \( U \) of dimension \( h \) is independent of the specific subspace \( U \), we can clearly see that our DMC is uniformly dispersive. However, it is not strongly symmetric in general. To see this, consider the conditional probability \( p_{\langle Y \rangle|\langle X \rangle}(U|U) = p_{\tau_G}(0) \). The output subspace \( U \) of dimension \( h \) is reached by only one input subspace, namely, \( U \) itself. Consider now the conditional probability \( p_{\langle Y \rangle|\langle X \rangle}(O|U) = p_{\tau_G}(h) \). The zero-dimensional output subspace \( O \) is reached by all input subspaces. From these two situations, we can clearly see that our DMC is not uniformly focusing, so it is not strongly symmetric in general. Nevertheless, we prove next an important result.

**Lemma 1**: The DMC \( (\mathcal{P}(\mathbb{F}_q^T, h), p_{\langle Y \rangle|\langle X \rangle}, \bigcup_{r=0}^{h} \mathcal{P}(\mathbb{F}_q^T, r)) \) is symmetric.

**Proof**: There are \( h + 1 \) component channels, \( \text{DMC}_r = \langle X_r, p_r(y|x), Y_r \rangle, r = 0, \ldots, h, \) each one related to one of the possible rank deficiencies of the transfer matrix \( G \). As explained above, for \( \tau_G = 0 \) and for \( \tau_G = h \), the two component channels are \( \text{DMC}_0 = (\mathcal{P}(\mathbb{F}_q^T, h), p_0(y|x) = 1, x = y, \mathcal{P}(\mathbb{F}_q^T, h)) \) and \( \text{DMC}_h = (\mathcal{P}(\mathbb{F}_q^T, h), p_h(y|x) = 1, \{O\}) \), respectively. These channels are trivial and clearly strongly symmetric. Their capacities are
\[ C_0 = \log \mathcal{P}(\mathbb{F}_q^T, h) = \log \binom{T}{h}_q, \]
and \( C_h = 0 \). Let us then assume that \( \tau_G = \rho \), where \( 0 < \rho < h \). The input alphabet is \( X_\rho = \mathcal{P}(\mathbb{F}_q^T, h) \). In the bipartite graph representation of \( \text{DMC}_\rho \), only those sockets of the \( X \) side of DMC that are associated to the transitions to output subspaces
of dimension \( h - \rho \) are considered for the \( X_\rho \) side. From (5), we can see that the output alphabet is \( \mathcal{Y}_\rho = \mathcal{P}(\mathbb{F}_q^T, h - \rho) \), and every input (resp., output) subspace \( U \in \mathcal{X}_\rho \) (resp., \( V \in \mathcal{Y}_\rho \)) is connected with equal transition probability to the same number of output (resp., input) subspaces. (The number of input subspaces connected to an output subspace \( V \in \mathcal{Y}_\rho \) can be obtained by dividing the number of sockets on the \( \mathcal{Y}_\rho \) side, which is the same as the number of sockets on the \( X_\rho \) side, i.e.,

\[
|\mathcal{P}(\mathbb{F}_q^T, h)| \cdot \left( \frac{h}{h - \rho} \right)_q,
\]

by the number of output subspaces, namely, \( |\mathcal{P}(\mathbb{F}_q^T, h - \rho)| \). This yields a component strongly symmetric channel, with capacity given by (from Theorem 1)

\[
C_\rho = \log |\mathcal{P}(\mathbb{F}_q^T, h - \rho)| - \log |\mathcal{P}(\mathbb{F}_q^T, h)| = \log \left( \frac{T}{h - \rho} \right)_q - \log \left( \frac{h}{h - \rho} \right)_q = \log \left( \frac{h}{h - \rho} \right)_q. \tag{6}
\]

**Theorem 4:** Given its rank deficiency probability distribution \( p_{\mathcal{R}G}(r) \), a RLCN seen as a subspace channel can be modeled as the DMC \( \langle \mathcal{P}(\mathbb{F}_q^T, h), \mathcal{P}(\mathbf{Y})|\mathbf{X} \rangle, \bigcup_{r=0}^h \mathcal{P}(\mathbb{F}_q^T, r) \rangle \). The capacity of this DMC is conditionally independent of the network topology and the network code used, and is given by

\[
C = \sum_{r=0}^h p_{\mathcal{R}G}(r) \log \left( \frac{T}{h - r} \right)_q. \tag{6}
\]

**Proof:** The proof follows straightforwardly from Lemma 1 and Theorem 2 with \( L = h + 1 \), \( q_i = p_{\mathcal{R}G}(i) \), and \( C_i \) given by (5).

**IV. Conclusion and Final Comments**

In this paper, we have modeled random linear coding networks as a symmetric discrete memoryless channel, and we have derived the capacity of this channel. We have assumed that neither the transmitter nor the receiver has knowledge of the network transfer matrix (noncoherent scenario) or the network topology. This scenario differs from the one in (4), where the network topology is assumed known and fixed at all times. For some fixed topologies, it has been shown in (4) that the capacity of RLCNs is lower bounded by the capacity of the so-called S-networks, for which constant-dimension subspace coding is optimal.

Herein, we have tactically considered the more general situation as an attempt to complement their work, and to try to answer some of the open questions raised therein. From the results of the present paper, we have the following comments:

1. The capacity in (4) is also a lower bound for the capacity of noncoherent RLCNs with unknown topology; if constant-dimension subspace coding is used, this lower bound is achieved;

2. The capacity of noncoherent RLCNs, either with general, but fixed and known, or with unknown topology, and whether subspace coding (in contrast to matrix coding) is sufficient to achieve capacity is still unknown.

As with any DMC, the capacity of RLCNs is achieved by using the channel many times. Since subspace codes are the most promising candidates for noncoherent RLNC, **multishot** subspace codes have been investigated in [15], [16].

Finally, the case of non-constant-dimension subspace coding and the inclusion of erroneous packets to our channel model are currently being investigated.

**Acknowledgements**

The authors would like to thank CNPq (Brazil) for the financial support, and Dr. Danilo Silva for helpful discussions. The first author would like to thank Dr. Yonghui Li, Dr. Zihuai Lin, and Prof. Branka Vucetic of the Telecommunications Laboratory of the University of Sydney, Australia, where this work was performed.

**References**

[1] T. Ho, R. Koetter, M. Médard, D. Karger, and M. Effros, “The benefits of coding over routing in a randomized setting,” in Proc. 2003 IEEE Int. Symp. Information Theory (ISIT’03), Yokohama, Japan, 2003, p. 442.

[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” IEEE Trans. Inform. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[3] S.-Y. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” IEEE Trans. Inform. Theory, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[4] S. Yang and E.-H. Yang, “The worst network topology for random linear network coding,” unpublished preprint, 2009.

[5] D. Silva, F. Kschischang, and R. Koetter, “Communication over finite-field matrix channels,” Computing Research Repository (CoRR), submitted to IEEE Trans. Inform. Theory, vol. abs/0807.1372, Jul. 2008.

[6] A. Montanari and R. Urbanke, “Coding for network coding,” Computing Research Repository (CoRR), vol. abs/0711.3935, Nov. 2007.

[7] D. Silva, F. Kschischang, and R. Koetter, “A rank-metric approach to error control in random network coding,” IEEE Trans. Inform. Theory, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.

[8] M. J. Siavoshani, C. Fragouli, and S. Diggavi, “Noncoherence multisource network coding,” in Proc. 2008 IEEE Int. Symp. Information Theory (ISIT’08), Toronto, Canada, Jul. 2008, pp. 817–821.

[9] C. Fragouli, M. Jafari, S. Mohajer, and S. Diggavi, “On the capacity of non-coherent network coding,” in Proc. 2009 IEEE Int. Symp. Information Theory (ISIT’09), Seoul, Korea, 2009, pp. 273–277.

[10] R. Koetter and F. R. Kschischang, “Coding for errors and erasures in random network coding,” IEEE Trans. Inform. Theory, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[11] E. M. Gabidulin, “Theory of codes with maximum rank distance,” Probl. Inf. Transm., vol. 21, no. 1, pp. 1–12, 1985.

[12] D. Silva and F. Kschischang, “Fast encoding and decoding of Gabidulin codes,” in Proc. 2009 IEEE Int. Symp. Information Theory (ISIT’09), Seoul, Korea, 2009, pp. 2858–2862.

[13] T. Cover and J. Thomas, Elements of Information Theory. Second Edition, New York: John Wiley & Sons, 2006.

[14] J. L. Massey, Lecture Notes for Applied Digital Information Theory I. Abteilung für Elektrotechnik: ETH, Zürich, 1993.

[15] R. W. da Nóbrega and B. F. Uchoa-Filho, “Multishot codes for network coding: bounds and a multilevel construction,” in Proc. 2009 IEEE Int. Symp. Information Theory (ISIT’09), Seoul, Korea, 2009, pp. 428–432.

[16] ——, “Multishot codes for network coding using rank-metric codes,” submitted to 2010 IEEE Int. Symp. Information Theory (ISIT’10).