

# Coding for Errors and Erasures in Random Network Coding

**Ralf Koetter**

Institute for Communications Engineering  
TU Munich, D-80333 Munich  
ralf.koetter@tum.de

**Frank R. Kschischang**

Dept. of Electrical and Computer Engineering  
University of Toronto  
frank@comm.utoronto.ca

**Abstract**—The problem of error-control in a “noncoherent” random network coding channel is considered. Information transmission is modelled as the injection into the network of a basis for a vector space  $V$  and the collection by the receiver of a basis for a vector space  $U$ . A suitable coding metric on subspaces is defined, under which a minimum distance decoder achieves correct decoding if the dimension of the space  $V \cap U$  is large enough. When the dimension of each codeword is restricted to a fixed integer, the code forms a subset of the vertices of the Grassmann graph. Sphere-packing, sphere-covering bounds and a Singleton bound are provided for such codes. A Reed-Solomon-like code construction is provided and a decoding algorithm given.

## I. INTRODUCTION

Random network coding [1], [2] is a powerful tool for disseminating information in networks, yet it is susceptible to packet transmission errors caused by noise or intentional jamming. Indeed, in the most naive implementations, a single error in one received packet would typically render the entire transmission useless when the erroneous packet is combined with other received packets to deduce the transmitted message. It might also happen that insufficiently many packets from one generation reach the intended receivers, so that the problem of deducing the information cannot be completed.

In this paper we formulate a coding theory in the context of a “noncoherent” or “channel oblivious” transmission model for random network coding that captures the effects both of errors, i.e., erroneously received packets, and of erasures, i.e., insufficiently many received packets. We are partly motivated by the close analogy between the  $\mathbb{F}_q$ -linear channel produced in random network coding and the  $\mathbb{C}$ -linear channel produced in noncoherent multiple-antenna channels [3], where neither the transmitter nor the receiver is assumed to have knowledge of the channel transfer characteristic. In contrast with previous approaches to error control in random network coding [4]–[8], the noncoherent transmission strategy taken in this paper is oblivious to the underlying network topology and to the particular linear network coding operations performed at the various network nodes. Here, information is encoded in the choice at the transmitter of a *vector space* (not a vector), and the choice of vector space is conveyed via transmission of a generating set for the space or its orthogonal complement.

Just as codes defined over complex Grassmannians play an important role in noncoherent multiple-antenna channels [3], we find that codes defined on Grassmann graphs play an important role here. The standard, widely advocated approach

to random network coding (see, e.g., [1]) involves transmission of packet “headers” that are used to record the particular linear combination of the components of the message present in each received packet. As we will show, this “uncoded” transmission may be viewed as a particular code on the Grassmannian, but a “suboptimal” one, in the sense that the Grassmannian contains more spaces of a particular dimension than those obtained by prepending a header to the transmitted packets. Indeed, the very notion of a header or local and global encoding vectors, crucial in [4]–[8], is moot in our context. A somewhat more closely related approach is that of [9], which deals with reliable communication in networks with so-called “Byzantine adversaries.” However, in contrast with the constructions of [9], which provide probabilistic assurances of code performance, this paper concentrates on the combinatorial problem of code construction with prescribed deterministic error-correction capability.

The remainder of this paper is organized as follows. In Section II, we introduce the “operator channel” as a concise and convenient abstraction of the channel encountered in random network coding. In Section III, we define a metric on this set that is natural and suitable in the context of random network coding. The transmitter selects a space  $V$  for transmission, indicating this choice by injection into the network of a set of packets that generate  $V$  (or its orthogonal complement). The receiver collects packets that span some received space  $U$ . We show that correct decoding is possible with a minimum distance decoder if the dimension of the space  $V \cap U$  is sufficiently large. We will usually confine our attention to codes having codewords all of the same dimension, in which case the code is a subset of the vertex set of the corresponding Grassmann graph. In Section IV, we give elementary coding bounds, analogous to the sphere-packing (Hamming) upper bounds and the sphere-covering (Gilbert-Varshamov) lower bounds for such codes. We also give a Singleton bound. Asymptotic versions of these bounds are also provided. In Section V we provide a Reed-Solomon-like code construction that achieves the Singleton bound asymptotically, and we describe a decoding algorithm. This construction is closely related to the Gabidulin construction of maximum rank-distance codes [10]. The connection between (certain) codes defined over finite-field Grassmannians and rank-metric codes is explored more fully in [11].

Due to space limitations, proofs have largely been omitted; however, see [12] for more details.

## II. OPERATOR CHANNELS

To capture the essence of random network coding, recall [2] that communication between transmitter and receiver occurs in a series of rounds or “generations;” during each generation, the transmitter injects a number of fixed-length packets into the network, each of which may be regarded as a vector of length  $N$  over a finite field  $\mathbb{F}_q$ . These packets propagate through the network, possibly passing through a number of intermediate nodes between transmitter and receiver. Whenever an intermediate node has an opportunity to send a packet, it creates a random  $\mathbb{F}_q$ -linear combination of the packets it has available and transmits this random combination. Finally, the receiver collects such randomly generated packets and tries to infer the set of packets injected into the network. There is *no* assumption here that the network operates synchronously or without delay or that the network is acyclic.

Let  $\{p_1, p_2, \dots, p_M\}$ ,  $p_i \in \mathbb{F}_q^N$  denote the set of injected vectors. In the error-free case, the receiver collects packets  $y_j$ ,  $j = 1, 2, \dots, L$  where each  $y_j$  is formed as  $y_j = \sum_{i=1}^M h_{j,i} p_i$  with unknown, randomly chosen coefficients  $h_{j,i} \in \mathbb{F}_q$ . We note that *a priori*  $L$  is not fixed and the receiver would normally collect as many packets as possible. However, properties of the network such as min-cut between the transmitter and the receiver may influence the joint distribution of the  $h_{i,j}$  and, at some point, there will be no benefit from collecting further redundant information.

If we choose to consider the injection of  $T$  erroneous packets, this model is enlarged to include error packets  $e_t$ ,  $t = 1, \dots, T$  to give

$$y_j = \sum_{i=1}^M h_{j,i} p_i + \sum_{t=1}^T g_{j,t} e_t$$

where again  $g_{j,t} \in \mathbb{F}_q$  are unknown random coefficients. Note that since these erroneous packets may be injected anywhere within the network, they may cause widespread error propagation; in particular, if  $g_{j,1} \neq 0$  for all  $j$ , even a single error packet  $e_1$  has the potential to corrupt each and every received packet.

In matrix form, the transmission model may be written as

$$y = Hp + Ge \quad (1)$$

where  $H$  and  $G$  are random  $L \times M$  and  $L \times T$  matrices, respectively,  $p$  is the  $M \times N$  matrix whose rows are the transmitted vectors, and  $e$  is the  $T \times N$  matrix whose rows are the error vectors.

At this point, since  $H$  is random, we may ask what property of the injected sequence of packets remains invariant in the channel described by (1), even in the absence of noise ( $e = 0$ )? Since  $H$  is a random matrix, all that is fixed by the product  $Hp$  is the particular vector space that is spanned by the rows of  $p$ . Indeed, as far as the receiver is concerned, any of the possible generating sets for this space are equivalent. We are led, therefore, to consider information transmission not via the choice of  $p$ , but rather by the choice of the vector space generated by  $p$ . This simple observation is at the heart of the

channel models and transmission strategies considered in this paper. Indeed, with regard to the vector space selected by the transmitter, the only deleterious effect that a multiplication with  $H$  may have is that  $Hp$  may have smaller rank than  $p$ , due to, e.g., an insufficient min-cut or packet erasures.

Let  $W$  be a fixed  $N$ -dimensional vector space over  $\mathbb{F}_q$ . All transmitted and received packets will be vectors of  $W$ ; however, we will describe a transmission model in terms of subspaces of  $W$  spanned by these packets. Let  $\mathcal{P}(W)$  denote the set of all sub-spaces of  $W$ , an object often called the projective geometry of  $W$ . The dimension of an element  $V \in \mathcal{P}(W)$  is denoted as  $\dim(V)$ .

We define the following “operator channel” as a concise transmission model for network coding.

**Definition 1** *An operator channel  $C$  associated with the ambient space  $W$  is a channel with input and output alphabet  $\mathcal{P}(W)$ . The channel input  $V$  and channel output  $U$  are related as*

$$U = \mathcal{H}_k(V) \oplus E$$

where  $\mathcal{H}_k$  is an erasure operator,  $E \in \mathcal{P}(W)$  is an arbitrary error space, and  $\oplus$  denotes the direct sum. If  $\dim(V) > k$ , the erasure operator  $\mathcal{H}_k$  acts to project  $V$  onto a randomly chosen  $k$ -dimensional subspace of  $V$ ; otherwise,  $\mathcal{H}_k$  leaves  $V$  unchanged. If the erasure operator  $\mathcal{H}_k$  satisfies  $\dim(V) - \dim(\mathcal{H}_k(V)) = \rho$  we say that  $\mathcal{H}_k$  corresponds to  $\rho$  erasures. The dimension of  $E$  is called the error norm  $t(E)$  of  $E$ .

## III. CODING FOR OPERATOR CHANNELS

Definition 1 concisely captures the effect of random network coding in the presence of networks with erasures, varying min-cuts and/or erroneous packets. Indeed, we will show how to construct codes for this channel that correct combinations of errors and erasures. Before we give such a construction we need to define a suitable metric.

### A. A Metric on $\mathcal{P}(W)$

Let  $\mathbb{Z}_+$  denote the set of non-negative integers. We define a function  $d : \mathcal{P}(W) \times \mathcal{P}(W) \rightarrow \mathbb{Z}_+$  by

$$d(A, B) := \dim(A + B) - \dim(A \cap B), \quad (2)$$

where  $A + B = \{a + b : a \in A, b \in B\}$  denotes the sum of spaces  $A$  and  $B$ , i.e., the smallest space containing both  $A$  and  $B$  as subspaces. It can easily be seen [12] that the function  $d(A, B)$  defined in (2) is a metric on the space  $\mathcal{P}(W)$ . This metric is the cornerstone for code design in this paper.

A *code* for an operator channel with ambient space  $W$  is simply a nonempty subset of  $\mathcal{P}(W)$ , i.e., a nonempty collection of subspaces of  $W$ . The size of a code  $\mathcal{C}$  is denoted by  $|\mathcal{C}|$ . The minimum distance of  $\mathcal{C}$  is denoted by

$$D(\mathcal{C}) := \min_{X, Y \in \mathcal{C}: X \neq Y} d(X, Y).$$

The maximum dimension of the elements of  $\mathcal{C}$  is denoted by

$$\ell(\mathcal{C}) := \max_{X \in \mathcal{C}} \dim(X).$$

## B. Error and Erasure Correction

A minimum distance decoder for a code  $\mathcal{C}$  is one that takes the output  $U$  of an operator channel and returns a nearest codeword  $V \in \mathcal{C}$ , i.e., a codeword  $V \in \mathcal{C}$  satisfying, for all  $V' \in \mathcal{C}$ ,  $d(U, V) \leq d(U, V')$ .

The importance of the minimum distance  $D(\mathcal{C})$  for a code  $\mathcal{C} \subset \mathcal{P}(W)$  is given in the following theorem, which provides the combined error-and-erasure-correction capability of  $\mathcal{C}$  under minimum distance decoding. Define  $(x)_+$  as  $(x)_+ := \max\{0, x\}$ .

**Theorem 1** Assume we use a code  $\mathcal{C}$  for transmission over an operator channel. Let  $V \in \mathcal{C}$  be transmitted, and let

$$U = \mathcal{H}_k(V) \oplus E$$

be received, where  $\dim(E) = t$ . Let  $\rho = (\ell(\mathcal{C}) - k)_+$  denote the maximum number of erasures induced by the channel. If

$$2(t + \rho) < D(\mathcal{C}), \quad (3)$$

then a minimum distance decoder for  $\mathcal{C}$  will produce the transmitted space  $V$  from the received space  $U$ .

## C. Codes in the Grassmann Graph

In the context of network coding, it is natural to consider codes in which each codeword has the same dimension, as knowledge of the codeword dimension can be exploited by the decoder to initiate decoding. Constant-dimension codes are analogous to constant-weight codes in Hamming space (in which every codeword has constant Hamming weight) or to spherical codes in Euclidean space (in which every codeword has constant energy).

Constant-dimension codes are naturally described as particular vertices of a so-called *Grassmann graph*, also called a  $q$ -Johnson scheme, where the latter name emphasizes that these objects constitute association schemes. A formal definition is given as follows.

**Definition 2** Denote by  $\mathcal{P}(W, \ell)$  the set of all subspaces of  $W$  of dimension  $\ell$ . This object is known as a *Grassmannian*. The *Grassmann graph*  $G_{W, \ell}$  has vertex set  $\mathcal{P}(W, \ell)$  with an edge joining vertices  $U$  and  $V$  if  $d(U, V) = 2$ . ■

*Remark:* It is well known that  $G_{W, \ell}$  is distance regular [13] and an association scheme with relations given by the distance between spaces. As such, practically all techniques for bounds in the Hamming association scheme apply. In particular, sphere-packing and sphere-covering concepts have a natural equivalent formulation. We explore these directions in Section IV. We also note that the distance measure between two spaces  $U, V$  in  $\mathcal{P}(W)$  introduced in (2) is equal to twice the graph distance in the Grassmann graph.<sup>1</sup> Codes (particularly the non-existence of perfect codes) in the Grassmann graph have been considered previously in [14]–[17]. ■

<sup>1</sup>Defining a distance as half of  $d(U, V)$  would give non-integer values for packings in  $\mathcal{P}(W)$ .

## D. Code Parameters

Before we study bounds and constructions of codes in  $\mathcal{P}(W)$ , we need a proper definition of rate. Let  $\mathcal{C} \subset \mathcal{P}(W)$  be a code. To transmit a space  $V \in \mathcal{C}$  would require the transmitter to inject up to  $\ell(\mathcal{C})$  (basis) vectors from  $V$  into the network. This would correspond to  $N\ell$   $q$ -ary symbols if ambient space  $W$  is a vector space over  $\mathbb{F}_q$ . This motivates the following definition.

**Definition 3** Let  $W$  be a vector space of dimension  $N$  over  $\mathbb{F}_q$ . Let  $\mathcal{C}$  be a subset of  $\mathcal{P}(W)$  such that the dimension of any  $V \in \mathcal{C}$  is at most  $\ell$  and the minimum distance of  $\mathcal{C}$  equals  $D$ . We say that  $\mathcal{C}$  is a  $q$ -ary code of type  $[N, \ell, \log_q(|\mathcal{C}|), D]$ . The normalized weight  $\lambda$ , rate  $R$  and the normalized minimum distance  $\delta$  of the code are defined as

$$\lambda = \frac{\ell}{N}, \quad R = \frac{\log_q(|\mathcal{C}|)}{N\ell} \quad \text{and} \quad \delta = \frac{D}{2\ell}. \quad \blacksquare$$

The parameters  $\lambda$ ,  $R$  and  $\delta$  are indeed natural. The normalized weight  $\lambda$  takes the role of the energy of a spherical code in Euclidean space, or the equivalent weight parameter for constant weight codes. As such  $\lambda$  is naturally limited to the range  $[0, 1]$ . Just as in constant-weight codes, the interesting range can actually be limited to  $[0, \frac{1}{2}]$  as spaces with dimension larger than  $\frac{N}{2}$  can be transmitted as the null space of a space of dimension less than  $\frac{N}{2}$ . The definition of  $\delta$  gives a natural range of  $[0, 1]$ . Indeed, a normalized distance of 1 could only be obtained by spaces having trivial intersection. The rate  $R$  of a code is restricted to the range  $[0, 1]$ , with a rate of 1 only being approachable for  $\lambda \rightarrow 0$ .

## E. Examples of Codes

We conclude this section with two examples of codes in  $\mathcal{P}(W, \ell)$ .

**Example 1** Let  $W$  be the space of vectors over  $\mathbb{F}_q$  of length  $N$ . Consider the set  $\mathcal{C} \subset \mathcal{P}(W, \ell)$  of spaces  $U_i$ ,  $i = 1, 2, \dots, |\mathcal{C}|$  with generator matrices  $G(U_i) = (I|A_i)$  where  $I$  is an  $\ell \times \ell$  identity matrix and the  $A_i$  are all possible  $\ell \times (N - \ell)$  matrices over  $\mathbb{F}_q$ . It is easy to see that all  $G(U_i)$  generate different spaces, intersecting in subspaces of dimension at most  $\ell - 1$  and that, hence, the minimum distance of the code is  $2\ell - 2(\ell - 1) = 2$ . The code is of type  $[N, \ell, \ell(N - \ell), 2]$  with normalized weight  $\lambda = \ell/N$ , rate  $R = 1 - \lambda$  and normalized distance  $\delta = \frac{1}{\lambda N}$ . ■

The first example corresponds to a trivial code that offers no error protection at all. While this code has been advocated widely for random network coding it is by no means the optimal code for a given distance  $D = 2$ , as can be seen in the following two examples.

**Example 2** Again let  $W$  be the space of vectors of length  $N$ . We now choose the code  $\mathcal{C}' = \mathcal{P}(W, \ell)$ , which yields a code of type  $[N, \ell, \log_q |\mathcal{P}(W, \ell)|, 2]$  which is clearly larger than the code  $\mathcal{C}$  of Example 1. We will give a precise expression for  $|\mathcal{P}(W, \ell)|$  in Section IV. ■

#### IV. BOUNDS ON CODES

Let  $\begin{bmatrix} n \\ \ell \end{bmatrix}_q$  denote the  $q$ -ary Gaussian coefficient [18, Ch. 24], defined as the number of  $\ell$ -dimensional subspaces of an  $n$ -dimensional vector space over  $\mathbb{F}_q$ . It can be shown [12] that the Gaussian coefficient  $\begin{bmatrix} n \\ \ell \end{bmatrix}_q$  satisfies  $1 < q^{-\ell(n-\ell)} \begin{bmatrix} n \\ \ell \end{bmatrix}_q < 4$  for  $0 < \ell < n$ .

We remarked earlier that the Grassmann graph constitutes an association scheme, which lets us use simple geometric arguments to give the standard sphere-packing upper bounds and sphere-covering lower bounds. In order to establish the bounds we need the notion of a sphere.

Let  $W$  be an  $N$  dimensional vector space and let  $\mathcal{P}(W, \ell)$  be the set of  $\ell$  dimensional subspaces of  $W$ . The sphere  $S(V, \ell, t)$  of radius  $t$  centered at a space  $V$  in  $\mathcal{P}(W, \ell)$  is defined as the set of all subspaces  $U$  that satisfy  $d(U, V) \leq 2t$ , i.e.,  $S(V, \ell, t) = \{U \in \mathcal{P}(W, \ell) : d(U, V) \leq 2t\}$ . Note that we prefer to define the radius in terms of the graph distance in the Grassmann graph. The radius can therefore take on any non-negative integer value. It can be shown that the number of spaces in  $S(V, \ell, t)$  is independent of  $V$  and equals

$$|S(V, \ell, t)| = \sum_{i=0}^t q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} N - \ell \\ i \end{bmatrix}$$

for  $t \leq \ell$ .

We now can simply state the sphere-packing and sphere-covering bounds as follows:

**Theorem 2** Let  $\mathcal{C}$  be a collection of spaces in  $\mathcal{P}(W, \ell)$  such that  $D(\mathcal{C}) \geq 2t$ , and let  $s = \lfloor \frac{t-1}{2} \rfloor$ . The size of  $\mathcal{C}$  must satisfy

$$|\mathcal{C}| \leq \frac{|\mathcal{P}(W, \ell)|}{|S(V, \ell, s)|} < \frac{\begin{bmatrix} N \\ \ell \end{bmatrix}}{q^{s^2} \begin{bmatrix} \ell \\ s \end{bmatrix} \begin{bmatrix} N - \ell \\ s \end{bmatrix}} < 4q^{(\ell-s)(N-s-\ell)}$$

Conversely, there exists a code  $\mathcal{C}'$  with distance  $D(\mathcal{C}') \geq 2t$  such that  $|\mathcal{C}'|$  is lower bounded by

$$|\mathcal{C}'| \geq \frac{|\mathcal{P}(W, \ell)|}{|S(V, \ell, t-1)|} > \frac{1}{16t} q^{(\ell-t+1)(N-t-\ell+1)}.$$

In terms of normalized parameters, the bounds of Theorem 2 can be expressed as follows. The rate of any collection  $\mathcal{C}$  of spaces in  $\mathcal{P}(W, \ell)$  with normalized minimum distance  $\delta = \frac{D(\mathcal{C})}{2\ell}$  is bounded from above by

$$R \leq (1 - \delta/2)(1 - \lambda(1 + \delta/2)) + o(1),$$

where  $o(1)$  approaches zero as  $N$  grows. Conversely, there exists a code  $\mathcal{C}'$  with normalized distance  $\delta$  such that the rate of  $\mathcal{C}'$  is lower bounded as:

$$R \geq (1 - \delta)(1 - \lambda(\delta + 1)) + o(1).$$

As shown in [12], the following bound plays the role of the Singleton bound in this context.

**Theorem 3** A  $q$ -ary code of  $\mathcal{C} \subseteq \mathcal{P}(W, \ell)$  of type  $[N, \ell, \log_q |\mathcal{C}|, D]$  must satisfy

$$|\mathcal{C}| \leq \begin{bmatrix} N - (D - 2)/2 \\ \ell - (D - 2)/2 \end{bmatrix}_q.$$

In terms of normalized parameters, the rate of any collection  $\mathcal{C}$  of spaces in  $\mathcal{P}(W, \ell)$  with normalized minimum distance  $\delta = \frac{D(\mathcal{C})}{2\ell}$  is bounded from above by

$$R \leq (1 - \delta)(1 - \lambda) + \frac{1}{\lambda N}(1 - \lambda + o(1)).$$

The three bounds are depicted in Fig. 1, for  $\lambda = 1/4$  and in the limit as  $N \rightarrow \infty$ .

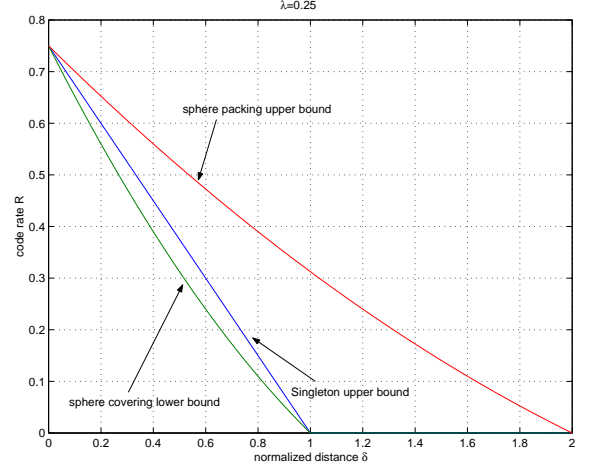


Fig. 1. Upper and lower asymptotic bounds on the largest rate of a code in the Grassmann graph  $G_{W, \ell}$  where the dimension  $N$  of ambient vector space is asymptotically large and  $\lambda = \frac{\ell}{N}$  is chosen as  $1/4$ .

#### V. A REED-SOLOMON-LIKE CODE CONSTRUCTION

We now turn to the problem of constructing a code capable of correcting errors and erasures at the output of the operator channels defined in Section II.

Let  $\mathbb{F}_q$  be a finite field and let  $\mathbb{F} = \mathbb{F}_{q^m}$  be an extension field. Recall from, e.g., [19, Sec. 3.4] that a polynomial  $L(x)$  is called a *linearized polynomial* over  $\mathbb{F}$  if it takes the form  $L(x) = \sum_{i=0}^d a_i x^{q^i}$ , with coefficients  $a_i \in \mathbb{F}$ ,  $i = 0, \dots, d$ . If  $a_d \neq 0$ , the parameter  $d$  is referred to as the associate degree of  $L(x)$ .

The sum of two linearized polynomials is again a linearized polynomial. A natural (but non-commutative) product of linearized polynomials arises via the composition  $L_1(L_2(x))$ , often written as  $L_1(x) \otimes L_2(x)$ , of two linearized polynomials, which again results in a linearized polynomial. Under addition and composition, the set of linearized polynomials forms a noncommutative ring without zero divisors and with two division algorithms (a right and left division). See [12] for further details.

Just as traditional Reed-Solomon codeword components may be obtained via the evaluation of an *ordinary* message polynomial, we obtain here a basis for the transmitted vector space via the evaluation of a *linearized* message polynomial.

Let  $\mathbb{F}_q$  be a finite field, and let  $\mathbb{F} = \mathbb{F}_{q^m}$  be a (finite) extension field of  $\mathbb{F}_q$ . Let  $A = \{\alpha_1, \dots, \alpha_\ell\} \subset \mathbb{F}$  be a set of linearly independent elements in this vector space. These elements span an  $\ell$ -dimensional vector space  $\langle A \rangle \subseteq \mathbb{F}$  over

$\mathbb{F}_q$ . Clearly  $\ell \leq m$ . We will take as ambient space the direct sum  $W = \langle A \rangle \oplus \mathbb{F} = \{(\alpha, \beta) : \alpha \in \langle A \rangle, \beta \in \mathbb{F}\}$ , a vector space of dimension  $\ell + m$  over  $\mathbb{F}_q$ .

Let  $u = (u_0, u_1, \dots, u_{k-1}) \in \mathbb{F}^k$  denote a block of message symbols, consisting of  $k$  symbols over  $\mathbb{F}$  or, equivalently,  $mk$  symbols over  $\mathbb{F}_q$ . Let  $\mathbb{F}^k[x]$  denote the set of linearized polynomials over  $\mathbb{F}$  of associate degree at most  $k-1$ . Let  $f(x) \in \mathbb{F}^k[x]$ , defined as  $f(x) = \sum_{i=0}^{k-1} u_i x^{[i]}$ , be the linearized polynomial with coefficients corresponding to  $u$ . Finally, let  $\beta_i = f(\alpha_i)$ . Each pair  $(\alpha_i, \beta_i)$ ,  $i = 1, \dots, \ell$ , may be regarded as a vector in  $W$ . Since  $\{\alpha_1, \dots, \alpha_\ell\}$  is a linearly independent set, so is  $\{(\alpha_1, \beta_1), \dots, (\alpha_\ell, \beta_\ell)\}$ ; hence this set spans an  $\ell$ -dimensional subspace  $V$  of  $W$ . We denote the map that takes the message polynomial  $f(x) \in \mathbb{F}^k[x]$  to the linear space  $V \in \mathcal{P}(W, |A|)$  as  $\text{ev}_A$ . If  $|A| \geq k$  then the map  $\text{ev}_A : \mathbb{F}^k[x] \rightarrow \mathcal{P}(W, |A|)$  can be shown to be injective. Henceforth we will assume that  $\ell \geq k$ .

**Theorem 4** *Let  $\mathcal{C}$  be the image under  $\text{ev}_A$  of  $\mathbb{F}^k[x]$ , with  $\ell = |A| \geq k$ . Then  $\mathcal{C}$  is a code of type  $[\ell + m, \ell, mk, 2(\ell - k + 1)]$ .*

The Singleton bound, evaluated for the code parameters of Theorem 4, states that

$$|\mathcal{C}| \leq \begin{bmatrix} N - (D - 2)/2 \\ \ell - (D - 2)/2 \end{bmatrix}_q = \begin{bmatrix} m + k \\ k \end{bmatrix}_q < 4q^{mk}.$$

This implies that a true Singleton-bound-achieving code could have no more than 4 times as many codewords as  $\mathcal{C}$ . Thus these Reed-Solomon-like codes are nearly Singleton-bound-achieving.

This code construction involving the evaluation of linearized polynomials is clearly closely related to the rank-metric code construction of Gabidulin [10]. However, in our setup, the codewords are not arrays, but rather the vector spaces spanned by the rows of the array, and the relevant decoding metric is not the rank metric, but rather the distance measure defined in (2).

It is possible to decode these codes using a Sudan-style “list-1” minimum distance decoding algorithm as described in detail in [12]. Given a received vector space  $U$ , the main steps of the algorithm are:

- 1) Find a bivariate linearized polynomial  $Q(x, y) = Q_x(x) + Q_y(y)$  of minimal  $(1, k-1)$  weighted degree that vanishes on the vector space  $U$ .
- 2) Perform the right division  $-Q_x(x)/Q_y(x)$  to find a linearized polynomial  $f(x)$  with the property that  $-Q_x(x) \equiv Q_y(x) \otimes f(x)$ . If no such polynomial can be found declare “failure.”
- 3) Output  $f(x)$  as the information polynomial corresponding the codeword  $V \in \mathcal{C}$  if  $d(U, V) < \ell - k + 1$ .

## VI. CONCLUSIONS

In this paper we have defined a class of operator channels as the natural transmission models in “noncoherent” random network coding. The inputs and outputs of operator channels are subspaces of some given ambient vector space. We have

defined a coding metric on these subspaces which gives rise to notions of erasures (dimension reduction) and errors (dimension enlargement). In defining codes, it is natural to restrict each codeword to have some fixed dimension; in this case, the code forms a subset of a finite-field Grassmannian. Sphere-packing and sphere-covering bounds as well as a Singleton-type bound are obtained in this context. Finally, a Reed-Solomon-like code construction is given, resulting in codes that are capable of correcting various combinations of errors and erasures.

## ACKNOWLEDGMENT

The authors thank Danilo Silva for useful discussions.

## REFERENCES

- [1] P. A. Chou, Y. Wu, and K. Jain, “Practical network coding,” in *Proc. 2003 Allerton Conf. on Commun., Control and Computing*, (Monticello, IL), Oct. 2003.
- [2] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” *IEEE Trans. on Inform. Theory*, vol. 52, pp. 4413–4430, Oct. 2006.
- [3] L. Zheng and D. N. C. Tse, “Communication on the Grassmannian manifold: A geometric approach to the noncoherent multiple-antenna channel,” *IEEE Trans. on Inform. Theory*, vol. 48, pp. 359–383, Feb. 2002.
- [4] N. Cai and R. W. Yeung, “Network coding and error correction,” in *Proc. 2002 IEEE Inform. Theory Workshop*, pp. 119–122, Oct. 20–25, 2002.
- [5] L. Song, R. W. Yeung, and N. Cai, “Zero-error network coding for acyclic networks,” *IEEE Trans. on Inform. Theory*, vol. 49, pp. 3129–3139, Dec. 2003.
- [6] R. W. Yeung and N. Cai, “Network error correction, part I: Basic concepts and upper bounds,” *Comm. in Inform. and Systems*, vol. 6, no. 1, pp. 19–36, 2006.
- [7] R. W. Yeung and N. Cai, “Network error correction, part II: Lower bounds,” *Comm. in Inform. and Systems*, vol. 6, no. 1, pp. 37–54, 2006.
- [8] Z. Zhang, “Network error correction coding in packetized networks,” in *Proc. 2006 IEEE Inform. Theory Workshop*, Oct. 22–26, 2006.
- [9] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, “Resilient network coding in the presence of Byzantine adversaries,” in *Proc. 26th Annual IEEE Conf. on Computer Commun., INFOCOM*, (Anchorage, AK), May 6–12, 2007. (To appear.)
- [10] E. M. Gabidulin, “Theory of codes with maximal rank distance,” *Problems of Information Transmission*, vol. 21, pp. 1–12, July 1985.
- [11] D. Silva and F. R. Kschischang, “Using rank-metric codes for error correction in random network coding,” in *Proc. 2007 IEEE Int. Symp. on Inform. Theory*, (Nice), June, 2007.
- [12] R. Koetter and F. R. Kschischang, “Coding for errors and erasures in random network coding.” Submitted to *IEEE Trans. on Inform. Theory*, Mar. 2007. Available online at [arxiv.org/abs/cs/0703061v1](http://arxiv.org/abs/cs/0703061v1), 2007.
- [13] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*. New York, NY: Springer Verlag, 1989.
- [14] L. Chihara, “On the zeros of the Askey-Wilson polynomials, with applications to coding theory,” *SIAM J. Math. Anal.*, vol. 18, no. 1, pp. 191–207, 1987.
- [15] W. J. Martin and X. J. Zhu, “Anticodes for the Grassmann and bilinear forms graphs,” *Designs, Codes and Cryptography*, vol. 6, pp. 73–79, 1995.
- [16] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, “On perfect codes and related concepts,” *Designs, Codes and Cryptography*, vol. 22, pp. 221–237, 2001.
- [17] M. Schwartz and T. Etzion, “Codes and anticodes in the Grassmann graph,” *J. of Combin. Theory Series A*, vol. 97, pp. 27–42, 2002.
- [18] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*. Cambridge, UK: Cambridge University Press, second ed., 2001.
- [19] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983. Vol. 20 of *The Encyclopedia of Mathematics*, G.-C. Rota, Ed.