Code Construction for Multiple Sources Network Coding

Mahdi Jafari, Christina Fragouli, Suhas Diggavi
Ecole Polytechnique Fédérale de Lausanne
{mahdi.jafarisiavoshani, christina.fragouli, suhas.diggavi}@epfl.ch

ABSTRACT

In several wireless applications multiple sources transmit information to one or more receivers, many times over unknown topologies. This is especially so in mobile networks where learning the topology may have prohibitive complexity. Network coding techniques allow to achieve the min-cut capacity even when the topology is unknown. Our contribution in this paper is to develop algebraic code constructions for multiple sources network coding.

1. INTRODUCTION

In network operation with network coding, a promising technique has nodes randomly combine their incoming packets over a finite field [1, 2]. This approach is well suited to dynamically changing or large scale networks as it avoids the need for global synchronization. We consider a scenario where multiple sources transmit independent information over such a network, towards a single receiver, or towards multiple receivers all of which request all the information from the sources.

We consider a network where neither the sources nor the receiver have knowledge of the network topology or of the linear coding operations the network nodes perform. In practical networks, where such deterministic knowledge is not sustainable, the most popular approach is to append coding vectors at the headers of the packets to keep track of the linear combinations of the source packets they contain.

Recently, algebraic subspace coding constructions have been proposed as a method that allows to achieve higher information rates by dispensing of the need for the coding vector overheads [3]. We extend the work of Koetter and Kschischang [3, 4] for multisource code construction.

In this paper, we assume that time is slotted, and at each time slot the ith source inserts in total m_i source packets denoted by rows of matrix X_i while a receiver observes n packets represented by rows of matrix Y. The packets Y are related to X_i through a linear transformation, called transfer function, that is unknown to both the sources and the receiver and changes from time slot to time slot. We use the communication model introduced in [5] as our starting point and then based on that model introduce a new channel where the input and output alphabets are subspaces.

We then proceed to the associated problem of code design over the subspace channel. Designing codes using subspaces have been recently proposed for the single source case by Koetter and Kshischang [3], who use subspaces to design elegant error and erasure correction schemes. We extend their work to the multiple source case.

MobiHoc'09, May 18–21, 2009, New Orleans, Louisiana, USA.
ACM 978-1-60558-531-4/09/05.

1.1 Notation

We here introduce our notation for the following sections. In this paper we work with matrices and subspaces defined over some finite field $\mathbb{F}_q$. We use 0_n and I_n to denote the $n \times n$ zero and identity matrices respectively. For a matrix X we use $\langle X \rangle$ to represent its row span. Let us consider the T-dimensional vector space $\mathbb{F}_q^T$. Let $\mathrm{Gr}(T,d)_q$ denote all d-dimensional subspaces of $\mathbb{F}_q^T$ which in fact is a Grassmannian. Note that the cardinality of $\mathrm{Gr}(T,d)_q$ is the Gaussian number, namely[1]

$$\mathcal{G}(T,d)_q \triangleq |\mathrm{Gr}(T,d)_q| \doteq q^{d(T-d)}. \quad (1)$$

We use $\mathcal{S}(T) \triangleq \cup_{i=0}^{T} \mathrm{Gr}(T,i)_q$ to denote the set of all subspaces of $\mathbb{F}_q^T$.

We use operator "$\sqsubseteq$" to denote the subspace relationship. We write $\hat{\pi} \sqsubseteq \pi$ if $\hat{\pi}$ is a subspace of π. The sum of two subspaces $\pi_1, \pi_2 \in \mathbb{F}_q^T$ is $\pi_1 + \pi_2 = \{u + v : u \in \pi_1, v \in \pi_2\}$. Equivalently, $\pi_1 + \pi_2$ is the smallest subspace of $\mathbb{F}_q^T$ containing both π_1 and π_2. To compare the distance between two subspaces $\pi_1, \pi_2 \in \mathcal{S}(T)$ we will use the following metric (see [3])

$$d_S(\pi_1, \pi_2) \triangleq \dim(\pi_1 + \pi_2) - \dim(\pi_1 \cap \pi_2).$$

2. MAC CHANNEL MODEL

Consider a network where nodes perform uniform at random network coding over a finite field $\mathbb{F}_q$. We assume slotted time, and a "block" time-varying channel. At time slot t, the receiver observes

$$Y(t) = \sum_{i=1}^{s} G_i(t) X_i(t) + G_e(t) X_e(t), \quad (2)$$

where we have s sources, each source i inserting $m_i \in \mathbb{F}_q^T$ packets (vectors), corresponding to the rows of matrices $X_i(t)$, in the network. We have also one or more adversaries injecting corrupted information in the network which is represented by the rows of the matrix $X_e(t)$. Thus $X_i(t)$ is an $m_i \times T$, $G_i(t)$ is an $n \times m_i$, $X_e(t)$ is an $e \times T$, $G_e(t)$ is an $n \times e$, and $Y(t)$ is an $n \times T$ matrix over $\mathbb{F}_q$. We assume

[1]By $f \doteq g$ we mean $\lim_{q\to\infty} f = \lim_{q\to\infty} g$.

non-coherent communication where neither sources nor receiver have any knowledge about the network topology and transfer matrices.

Due to the linear structure of the channel model (2), we observe that the row span of the received packets is a subspace of the union of the row span of the transmitted packets. This fact leads us to conclude that considering the subspaces spanned by the rows of inputs and output matrices should be sufficient as far as the receiver is concerned.

Let us define the "erasure operator" $\mathcal{E}_\rho$ that operates on a subspace π of $\mathbb{F}_q^T$ and erases at most ρ dimensions from π according to some statistics[2]. Using this operator, we define the following multiple access channel which inherently describes (2).

DEFINITION 1. *The channel $C_{MAC} : [\mathcal{S}(T)]^s \to \mathcal{S}(T)$, is a multiple access channel described by*

$$\pi_y = \left[\mathcal{E}_{\rho_1}(\pi^{(1)}) + \cdots + \mathcal{E}_{\rho_s}(\pi^{(s)})\right] \oplus \pi_e, \qquad (3)$$

where $\pi^{(i)}$ is the subspace sent by ith source and π_e is an error space. Here ρ_i denotes the maximum number of erasures induced by the channel on the subspaces sent by the ith source. We also define $d_e \triangleq \dim(\pi_e)$ to be dimension of the inserted error space.

To find the achievable rate region for the channels described by (2) or (3), we need to assume a probability model for the transfer matrices and the erasure operators. For example, we can assume that the transfer matrices G_i, $i = 1, \ldots, s$, and G_e change (not necessarily independently) from time slot to time slot, according to the uniform at random linear combining performed by the network intermediate nodes. Although in general transfer matrices have some structure related to the topology of the network (see for example [6]) this is a simple enough model to be tractable, and captures well large networks where sufficient information mixing occurs. For this channel model and point-to-point communication the capacity has been calculated in [5, 7]. In [8] the capacity is calculated for a similar model that imposes the additional restriction on the transfer matrices to be full rank. In this paper we concentrate on the algebraic code design problem in $[\mathcal{S}(T)]^s$, that is independent of the probability structure of the transfer matrices.. That is, our codes have block length one and the problem we consider is a combinatorial problem rather than information theoretical.

3. CODING FOR MAC

3.1 Coding Problem

In this section we consider multiple access communication over the channel described by (3). To each source i a codebook $\mathcal{C}_i \subseteq \mathcal{S}(T)$ is assigned. The rate of each codebook is defined as $R_i \triangleq \log_2 |\mathcal{C}_i|$ and for the minimum distance we define

$$\delta_S(\mathcal{C}_i) \triangleq \min_{\pi,\pi' \in \mathcal{C}_i : \pi \neq \pi'} d_S(\pi, \pi').$$

First, let us consider the special case where there are no errors and erasures in the network, which means we can rewrite (3) as follows

$$\pi_R = \pi^{(1)} + \cdots + \pi^{(s)}, \qquad \pi^{(i)} \in \mathcal{C}_i.$$

[2]Note that there is slight difference between the definition of erasure operator here and in [3].

DEFINITION 2. ***(Identifiable Code)*** *An identifiable code is a set of s codebooks $\mathcal{C}_i \subseteq \mathcal{S}(T)$ such that we have $\pi^{(1)} + \cdots + \pi^{(s)} \neq \hat{\pi}^{(1)} + \cdots + \hat{\pi}^{(s)}$ when $\pi^{(i)} \neq \hat{\pi}^{(i)}$ for at least one source i. Note that $\pi^{(i)}$ and $\hat{\pi}^{(i)}$ are the subspaces sent by source i.*

For the general case where there are errors in the network, not only the codebooks have to be identifiable, but also some distance between codewords is required to enable the receiver to decode the sent messages. Let us define the union subspace code $\mathcal{C}$ as all possible combinations of $\pi^{(1)} + \cdots + \pi^{(s)}$, namely

$$\mathcal{C} \triangleq \left\{\pi^{(1)} + \cdots + \pi^{(s)} |\ \pi^{(i)} \in \mathcal{C}_i,\ i = 1, \ldots, s\right\}. \qquad (4)$$

The following theorem relates the minimum distance of code $\mathcal{C}$ to the error and erasure correction capability of $\mathcal{C}$ under minimum distance decoding.

THEOREM 1. *Assume an identifiable code $\{\mathcal{C}_i\}$ is used for transmission over the channel in (3). Let $\pi^{(i)} \in \mathcal{C}_i$, $i = 1, \ldots, s$, be transmitted and π_R be received. If*

$$2\left(d_e + \sum_{i=1}^{s} \rho_i\right) < \delta_S(\mathcal{C}), \qquad (5)$$

then a minimum distance decoder will enable the receiver to recover the transmitted subspaces for each source.

PROOF. Let us define $\pi_S = \pi^{(1)} + \cdots + \pi^{(s)}$ and $\hat{\pi}^{(i)} = \mathcal{E}_{\rho_i}(\pi^{(i)})$ for $i = 1, \ldots, s$. So we can write

$$\begin{aligned} d_S(\pi_R, \pi_S) &\overset{(a)}{\leq} d_S(\pi^{(1)} + \cdots + \pi^{(s)}, \hat{\pi}^{(1)} + \cdots + \hat{\pi}^{(s)}) \\ &\quad + d_S(\pi_R, \hat{\pi}^{(1)} + \cdots + \hat{\pi}^{(s)}) \\ &\overset{(b)}{\leq} \sum_{i=1}^{s} d_S(\pi^{(i)}, \hat{\pi}^{(i)}) + d_S(\pi_R, \hat{\pi}^{(1)} + \cdots + \hat{\pi}^{(s)}) \\ &\leq \sum_{i=1}^{s} \rho_i + d_e, \end{aligned}$$

where (a) follows from the triangle inequality and (b) follows from Lemma 1. For another codeword $\pi'_S \neq \pi_S$ in $\mathcal{C}$ we have

$$\delta_S(C) \leq d_S(\pi_S, \pi'_S) \leq d_S(\pi_S, \pi_R) + d_S(\pi_R, \pi'_S).$$

Combining these two inequalities we can write

$$d_S(\pi_R, \pi'_S) \geq \delta_S(\mathcal{C}) - d_S(\pi_S, \pi_R) \geq \delta_S(\mathcal{C}) - \left(d_e + \sum_{i=1}^{s} \rho_i\right).$$

So if the inequality (5) holds, then $d_S(\pi_R, \pi'_S) > d_S(\pi_R, \pi_S)$ and a minimum distance decoder would choose π_R. Because $\{\mathcal{C}_i\}$ is an identifiable code, the receiver is able to decompose π_R uniquely and find the original messages. □

LEMMA 1. *Suppose π_i, $i = 1, \ldots, s$, are subspaces of some vector space W. Assume $\hat{\pi}_i \sqsubseteq \pi_i$ for $i = 1, \ldots, s$. Then we have*

$$d_S(\pi_1 + \cdots + \pi_s, \hat{\pi}_1 + \cdots + \hat{\pi}_s) \leq \sum_{i=1}^{s} d_S(\pi_i, \hat{\pi}_i).$$

The following lemma relates the minimum distance of the codebook $\mathcal{C}$ to the minimum distance of each codebook $\mathcal{C}_i$.

LEMMA 2. *For the minimum distance of code $\mathcal{C}$ we have*

$$\delta_S(\mathcal{C}) \leq \min_{i:\ 1\leq i\leq s} \delta_S(\mathcal{C}_i). \tag{6}$$

PROOF. Consider two subspaces $\pi, \hat{\pi} \in \mathcal{C}$ where $\pi = \pi^{(1)}+\cdots+\pi^{(s)}$ and $\hat{\pi} = \hat{\pi}^{(1)}+\cdots+\hat{\pi}^{(s)}$ such that $\pi^{(j)} = \hat{\pi}^{(j)}$ for all sources except source i. Then take the minimum value over i. □

3.2 Code Construction

We here give our code construction which is a simplified version of the codes introduced in [5]. Let us assign to ith user the codebook $\mathcal{C}_i$ which is constructed as follows

$$\mathcal{C}_i = \{\pi_i |\ \pi_i = \langle H_i \rangle\}, \tag{7}$$

where H_i is a $d_i \times T$ matrix of the form

$$H_i = \left[0_{d_1}|\cdots|0_{d_{i-1}}|I_{d_i}|0_{d_{i+1}}|\cdots|0_{d_s}|m_i\right], \tag{8}$$

and we define $d \triangleq \sum_{i=1}^{s} d_i$. In the definition of H_i we choose $m_i \in C_{M_i}$, where C_{M_i} is a matrix code over $\mathbb{F}_q^{d_i\times(T-d)}$. Let $\delta_R(C_{M_i})$ be the minimum distance of C_{M_i} calculated using rank metric which is defined as follows

$$\delta_R(C_{M_i}) \triangleq \min_{x,y\in C_{M_i},\ x\neq y} \text{Rank}(x-y).$$

The codes C_{M_i} are called rank metric codes and were largely developed by Gabidulin [9]. However, the rank metric was first used in coding theory by Delsarte [10].

Obviously, the above construction results in an identifiable code since for every $\pi_i \in \mathcal{C}_i$ and $\pi_j \in \mathcal{C}_j$ we have $\dim(\pi_i \cap \pi_j) = 0$. The following lemma relates the minimum distance of subspace code $\mathcal{C}_i$ to the minimum distance of C_{M_i}.

LEMMA 3. *If a subspace code $\mathcal{C}_i$ is constructed from a rank metric code C_{M_i} using (7) and (8), for their minimum distance we have*

$$\delta(\mathcal{C}_i) = 2\delta_R(C_{M_i}).$$

PROOF. See Proposition 4 in [4]. □

Also, the minimum distance of the union code $\mathcal{C}$ defined by (4) satisfies Lemma 2 with equality as it is shown in the following theorem.

THEOREM 2. *For the minimum distance of the union code $\mathcal{C}$ of codes $\mathcal{C}_i$ constructed as above, we have*

$$\delta_S(\mathcal{C}) = \min_{i:\ 1\leq i\leq s} \delta_S(\mathcal{C}_i) = 2\times \min_{i:\ 1\leq i\leq s} \delta_R(C_{M_i}).$$

PROOF. Let $\pi, \hat{\pi} \in \mathcal{C}$. From the code construction, we know that π and $\hat{\pi}$ have the following structure

$$\pi = \left\langle \left[\begin{array}{c|c} & m_1 \\ I & \vdots \\ & m_s \end{array}\right] \right\rangle, \quad \hat{\pi} = \left\langle \left[\begin{array}{c|c} & \hat{m}_1 \\ I & \vdots \\ & \hat{m}_s \end{array}\right] \right\rangle.$$

Now let us assume π and $\hat{\pi}$ are two subspaces that achieve the minimum distance of the code $\mathcal{C}$. Using the definition of minimum distance, we have

$$\begin{aligned}
\delta_S(\mathcal{C}) &= d_S(\pi,\hat{\pi}) = 2\dim(\pi+\hat{\pi}) - \dim(\pi) - \dim(\hat{\pi}) \\
&= 2\text{Rank}\begin{bmatrix} \hat{m}_1 - m_1 \\ \vdots \\ \hat{m}_s - m_s \end{bmatrix} \\
&\geq 2\times \min_{i:\ 1\leq i\leq s} \delta_R(C_{M_i}) \\
&= \min_{i:\ 1\leq i\leq s} \delta_S(\mathcal{C}_i).
\end{aligned}$$

From the previous equation and by Lemma 2 we are done. □

EXAMPLE 1. ***Error free case**: For the special case where there are no errors and erasures in the network, for each source i we can assign all possible $d_i \times (T-d)$ matrices to C_{M_i}. For the rate of each user we have $R_i = d_i(T-d)\log_2 q$, where $d = \sum_{i=1}^{s} d_i$. For their sum rate we can also write $\sum_{i=1}^{s} R_i = d(T-d)\log_2 q$.* □

Preliminary results indicate that these code constructions for the channel (2), if (i) there are no errors in the network ($X_e(t) = 0$), (ii) the elements of the transfer matrices $G_i(t)$ are chosen independently and uniformly at random from $\mathbb{F}_q$ and (iii) $G_i(t)$ are independent from block to block, then the subspace codes introduced in Example 1 can achieve the rate region of (2). Verifying this is part of our future work.

4. REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow", *IEEE Transactions on Information Theory*, Volume 46, Issue 4, Page(s) 1204–1216, 2000.

[2] T. Ho, R. Koetter, M. Medard, M. Effros, J. Shi, and D. Karger, "A random linear network coding approach to multicast", *IEEE Transactions on Information Theory*, Volume 52, Issue 10, Page(s) 4413–4430, October 2006.

[3] R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding", *IEEE Transactions on Information Theory*, Volume 54, Issue 8, Page(s) 3579–3591, August 2008.

[4] D. Silva, F. R. Kschischang, and R. Kotter, "A Rank-Metric approach to error control in random network coding", *IEEE Transactions on Information Theory*, Volume 54, Issue 9, Page(s) 3951–3967, 2008.

[5] M. Jafari Siavoshani, C. Fragouli, and S. Diggavi, "Noncoherent multisource network coding", *IEEE International Symposium on Information Theory (ISIT)*, Page(s) 817–821, Canada, Toronto, July 2008.

[6] M. Jafari Siavoshani, C. Fragouli and S. Diggavi, "Passive topology discovery for network coded systems", *Information Theory Workshop(ITW)*, Bergen, Norway, Page(s) 17–21, July 2007.

[7] M. Jafari, S. Mohajer, C. Fragouli and S. Diggavi, "Capacity of non-coherent network coding", to appear in ISIT 2009, also available as EPFL technical report.

[8] D. Silva, F. R. Kschischang, and R. Koetter, "Capacity of random network coding under a probabilistic error model", July 2008, *available online at http://arxiv.org/pdf/0807.1372/*.

[9] E. M. Gabidulin, "Theory of codes with maximal rank distance", *Problems of Information Transmission*, Volume 21, Page(s) 1–12, July 1985.

[10] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory", *Journal of Combinatorial Theory, Series A*, Volume 25, Page(s) 226–241, 1978.