On Capacity Achieving Property of Rotational Coding for Acyclic Deterministic Wireless Networks

Mohammad A. (Amir) Khojastepour*, Alireza Keshavarz-Haddad†, Alireza Salehi Golsefidy‡
*NEC Laboratories America, 4 Independence Way, Suite 200,Princeton, NJ, 08540
†Shiraz University, School of Electrical and Computer Engineering, Shiraz, Iran
‡Princeton University, Department of Mathematics, Princeton, NJ, 08540

***Abstract*—It has been shown that the well-known cutset bounds can be achieved for deterministic wireless networks by performing random coding at each intermediate node. The complexity and forwarding overhead of random coding scheme prohibits its application in practice. Recently, a practical low complexity alternative, *rotational coding* scheme, was proposed in [1] where it was proved that the rotational coding can achieve the capacity of the layered deterministic wireless networks. In this paper, we extend the result and prove that the rotational coding is in fact capacity achieving for a general acyclic network. Our result adds to the practical property of rotational coding scheme and makes it desirable for communication networks with arbitrary topology as long as there is no directional cycle in the network.**

I. Introduction

There have been many recent works focusing on finding efficient strategies and coding schemes to achieve high throughput in a wireless network. Recent capacity results have shown coding schemes that can achieve the maximum throughput for a single multicast session in a wireless network [2]–[4]. The results are obtained for a simplified wireless network model, the deterministic channel model, where the effect of the noise is de-emphasized but the interference that is the main challenge in wireless network coding has been fully considered. The coding complexity and overhead of forward signaling prohibits these results to be employed in practice. In [1], a novel coding scheme (*rotational coding*) for layered network is proposed that has considerably lower complexity and overhead and can be implemented in practical systems. In this paper, we prove that rotational coding can be employed for any acyclic network topology and it is in fact capacity achieving.

Network coding has been an important research are in network information theory in the last decade. This was motivated by the need for more reliable and high throughput communication systems. The research on network coding has focused on improving throughput, energy consumption, delay, robustness, and some other performance metrics of communication networks. New research on network coding was also triggered by the seminal paper by Ahlswede et al. [5] in which it was proved that the maximum flow capacity of a single multicast session can be achieved using network coding in wired networks with directional links. Later, [6] and [7] show constructively that the linear (random) network codes can achieve the minimum cutset bound of a single multicast session in wired networks.

Recently, a deterministic approach to study wireless networks was introduced in [2]. This model incorporates both broadcast and interference challenges in the wireless network. However, by removing the randomness, this model makes the challenging problem of network coding for wireless network analytically tractable. For example, the problem of maximum flow capacity of a single multicast session in wireless networks was studied in [3] where it was shown that similar to the results for wired networks [5], the minimum cutset bound can be achieved. In [3], [4], a random linear network coding scheme is proposed to show the achievability of the cutset upper bound.

In this paper, we study the maximum throughput of network coding schemes for a single multicast session in general acyclic wireless networks. We adapt the deterministic channel model [2] for modeling the wireless channel. We also use the rotational coding scheme proposed in [1] for layered networks and modify it to be able to handle general acyclic network topology. We prove the optimality of rotational coding scheme for acyclic networks in a sense that it achieves the cutset bounds for the network.

This paper is organized as follows. In Section II, we describe the network model and notations. In Section III we briefly describe the rotational network coding scheme. In Section IV, we provide our main result that rotational coding scheme can achieve the capacity in acyclic networks. Finally, we conclude the paper in Section V.

II. Network Model and Notations

We consider a wireless network as a directed graph where each node can transmit the same message on *all* its outgoing links and receives the *superposition* of the signals arriving on the incoming links. We adopt the deterministic model in [2], [3] to model the gain of the links and how the superposition is performed. Notice that in this model the nodes are *full-duplex*, i.e., they can simultaneously transmit and receive data. Thus, from the standpoint of achieving the capacity, there is no need for scheduling the transmissions at the network nodes.

We assume that the network contains $1 + N$ nodes, where one of them is the source of a multicast session and the rest of the nodes are relay nodes or terminals (destinations) of the session. We use a universal index k for every node Φ_k where $k = 0, 1, \ldots, N$.

A. Deterministic Channel Model

In this channel model, the output signal from node Φ_k at time-slot t is considered as a column vector $\mathbf{y}_t^k = [y_{t,1}^k, y_{t,2}^k, \ldots, y_{t,q}^k]^{\rm tr}$ of size q, where each element is a value in Galois Field $\mathbb{F}(p^n)$ for some prime number p and positive integer n. Here tr is used to denote the matrix transpose operation. Each link from the node Φ_i to Φ_k in the network is denoted by its transfer function $\mathbf{G}_i^k$ which is a $q \times q$ matrix with the entries in $\mathbb{F}(p^n)$. The output of this link is equal to $\mathbf{G}_i^k \mathbf{y}_t^i$. The received vector or input at the node Φ_k is a column vector $\mathbf{x}_t^k = [x_{t,1}^k, x_{t,2}^k, \ldots, x_{t,q}^k]^{\rm tr}$ which is the superposition of the outputs of the links arriving at node Φ_k defined on component-by-component basis, i.e.,

$$\mathbf{x}_t^k = \sum_{i=0}^{n} \mathbf{G}_i^k \mathbf{y}_t^i \tag{1}$$

where $\mathbf{G}_i^k$ is the transfer function when there is an outgoing link from Φ_i to Φ_k, otherwise it is set to a $q \times q$ matrix $\mathbf{0}$ whose elements are all zeros.

If we stack together the received vectors at multiple nodes $\Phi_k, k \in \mathcal{B} = \{j_1, \ldots, j_b\}$, assuming they are characterized by the output at the nodes $\Phi_k, k \in \mathcal{A} = \{i_1, \ldots, i_a\}$ (i.e. all incoming links of $\mathcal{B}$ originated in $\mathcal{A}$), then the transfer function is given by

$$\begin{aligned}\begin{bmatrix} \mathbf{x}_t^{j_1} \\ \mathbf{x}_t^{j_2} \\ \vdots \\ \mathbf{x}_t^{j_b} \end{bmatrix} &= \begin{bmatrix} \mathbf{G}_{i_1}^{j_1} & \mathbf{G}_{i_2}^{j_1} & \ldots & \mathbf{G}_{i_a}^{j_1} \\ \mathbf{G}_{i_1}^{j_2} & \mathbf{G}_{i_2}^{j_2} & \ldots & \mathbf{G}_{i_a}^{j_2} \\ \vdots & & & \vdots \\ \mathbf{G}_{i_1}^{j_b} & \mathbf{G}_{i_2}^{j_b} & \ldots & \mathbf{G}_{i_a}^{j_b} \end{bmatrix} \begin{bmatrix} \mathbf{y}_t^{i_1} \\ \mathbf{y}_t^{i_2} \\ \vdots \\ \mathbf{y}_t^{i_a} \end{bmatrix} \\ &= \mathbf{G}_{\mathcal{A}}^{\mathcal{B}} \begin{bmatrix} \mathbf{y}_t^{i_1} \\ \mathbf{y}_t^{i_2} \\ \vdots \\ \mathbf{y}_t^{i_a} \end{bmatrix} \end{aligned} \tag{2}$$

The above notation of $\mathbf{G}_{\mathcal{A}}^{\mathcal{B}}$ will be used later in several places.

B. Time-Frame Operations for Linear Network Coding Schemes

In the proposed coding schemes in this paper, we assume that each node performs a linear operation over a time-frame of T time-slots, i.e., after receiving T vectors $\mathbf{x}_t^k$, $t = mT + 1, \ldots, mT + T$ at time-frame m, the node Φ_k linearly maps qT received symbols by a matrix $\mathbf{F}_m^k$ of size $qT \times qT$ to find qT new symbols which become the outgoing symbols. Then, these symbols are put into T column vectors $\mathbf{y}_t^k$, $t = (m+1)T+1, \ldots, (m+1)T+T$ that will be transmitted in the next T time-frames. The linear operation can be formulated as follows:

$$\begin{bmatrix} y_{(m+1)T+1,1}^k \\ \vdots \\ y_{(m+1)T+T,1}^k \\ y_{(m+1)T+1,2}^k \\ \vdots \\ y_{(m+1)T+T,2}^k \\ \vdots \\ y_{(m+1)T+T,q}^k \end{bmatrix} = \mathbf{F}_m^k \begin{bmatrix} x_{mT+1,1}^k \\ \vdots \\ x_{mT+T,1}^k \\ x_{mT+1,2}^k \\ \vdots \\ x_{mT+T,2}^k \\ \vdots \\ x_{mT+T,q}^k \end{bmatrix} \tag{3}$$

Please note the order of indices in (3); this order will be used later in Section III to describe our coding scheme. We denote the above vectors corresponding to outgoing symbols at time-frame $m+1$ and incoming symbols at time m of node k by $\mathbf{Y}_{(m+1)}^k$ and $\mathbf{X}_m^k$ respectively.

Let $\mathbf{H}_{\mathcal{A}}^{\mathcal{B}} = \mathbf{G}_{\mathcal{A}}^{\mathcal{B}} \otimes \mathbf{I}$ where $\otimes$ is the Kronecker matrix product and $\mathbf{I}$ is a $T \times T$ identity matrix. Hence,

$$\mathbf{X}_m^k = \sum_{i=0}^{n} \mathbf{H}_i^k \mathbf{Y}_m^i \tag{4}$$

C. Notations of Layered Network Model

In this subsection, we assume that the wireless network is layered, i.e., the nodes are divided into $L+1$ layers namely layer 0, 1, ..., L such that the input for any node in layer $l+1$ depends on the output of the nodes in layer l and the transfer function of the links from the nodes in layer l to the nodes in layer $l+1$. There exists exactly one node in layer 0 which is the source node of the single multicast session.

For the layered networks, we can set matrices $\mathbf{F}_m^k$ based on only the node index number k (independent from time-frame number m). The structure of layered network implies that at time-frame $m+l$ the nodes of layer l receive a linear combinations of symbols which have been sent by the source at time-frame m. In other words, the symbols which are sent at different time-frames are not mixed at any node.

Since every node performs a linear transformation there will be a linear mapping between the sent symbols from the source (Φ_0) and received symbols by an arbitrary node. We denote this linear transformation that maps input symbols of Φ_0 to an arbitrary node Φ_i in layer l by $\mathbf{S}_i$. Hence,

$$\mathbf{X}_{m+l}^i = \mathbf{S}_i \mathbf{X}_m^0 \tag{5}$$

for all time-frames m.

Assume that the source selects its input vector from a vector space $V_0 = \mathbb{F}(p^n)^{qT}$. For an arbitrary set of nodes $\mathcal{A} = \{i_1, i_2, \ldots, i_a\}$ in layer l, we define Null($\mathcal{A}$) as the subspace of $\mathbb{F}(p^n)^{qT}$ which is mapped to $\mathbf{0}$ in all nodes of $\mathcal{A}$. In other words,

$$\text{Null}(\mathcal{A}) = \{\mathbf{X} \in \mathbb{F}(p^n)^{qT} : \forall k \in \mathcal{A},\ \mathbf{S}_k \mathbf{X} = \mathbf{0}\} \tag{6}$$

We also define $V_{\mathcal{A}}$ to a subspace of $\mathbb{F}(p^n)^{qT}$ with maximal size that is complementary with subspace Null($\mathcal{A}$) (i.e. $\text{Null}(\mathcal{A}) \cap V_{\mathcal{A}} = \mathbf{0}$ and $\dim(\text{Null}(\mathcal{A})) + \dim(V_{\mathcal{A}}) = qT$). We call $V_{\mathcal{A}}$ a *decodable space* by the set $\mathcal{A}$. From the definitions, it is straightforward to show that given the received vectors of the nodes of $\mathcal{A}$ we can uniquely determine which vector in $V_{\mathcal{A}}$ is sent by the source l time-frames earlier.

We denote the set theoretic difference of two sets $\mathcal{A}$ and $\mathcal{B}$, also called the relative difference of $\mathcal{A}$ from $\mathcal{B}$ by $\mathcal{A} \setminus \mathcal{B} = \mathcal{A} \cap \mathcal{B}^c$. We define a similar operator $\check{\setminus}$ on vector spaces. For two arbitrary vector spaces $V_{\mathcal{A}}$ and $V_{\mathcal{B}}$ defined on $\mathbb{F}(p^n)$, $U = V_{\mathcal{A}} \check{\setminus} V_{\mathcal{B}}$ which is defined as a subspace of $V_{\mathcal{A}}$ with maximum size that is disjoint to $V_{\mathcal{B}}$, (i.e. $U \cap V_{\mathcal{B}} = \mathbf{0}$ and $\dim(U + V_{\mathcal{B}}) = \dim(U) + \dim(V_{\mathcal{B}})$). The same operator may be applied to any two matrices, say, $\mathbf{G}_1$ and $\mathbf{G}_2$, as $\mathbf{G}_1 \check{\setminus} \mathbf{G}_2$ to denote the extended quotient space between the two vector spaces formed by the span of the *row vectors* of $\mathbf{G}_1$ and $\mathbf{G}_2$.

Here we must state that the usual vector space subtraction operation is defined only for *inner-product* vectors spaces, that defines $U = V_{\mathcal{A}} \setminus V_{\mathcal{B}}$ to be the largest subspace of $V_{\mathcal{A}}$ orthogonal to $V_{\mathcal{A}} \cap V_{\mathcal{B}}$. This definition has been used in our earlier [1], [4], while $[\mathbb{F}(p^n)]^{qT}$ is not an inner-product vector space over finite field $\mathbb{F}(p^n)$. Fortunately, if we replace $\check{\setminus}$ by the usual subspace subtraction in [1], then all mathematical arguments and results will be still valid. Therefore, we can technically use results of [1] in this paper.

D. Structure of Code-block for coding in Acyclic Networks

In a layered wireless network, the nodes are divided into $L+1$ layers namely layer 0, 1, ..., L such that the input at any node in layer $l+1$ depends on the output of the nodes in layer l and the transfer function of the links from the nodes in layer l to the nodes in layer $l+1$. Thus, we can set the encoding matrices $\mathbf{F}_m^k$ based on only the node index number k (independent from time-frame number m). The structure of a layered network implies that at time-frame $m+l$ the nodes of layer l receive a linear combinations of symbols which have been sent by the source at time-frame m. In other words, the symbols which are sent at different time-frames are not mixed at any node. However, this is not generally true for acyclic networks. Therefore, we cannot consider the coding scheme as a linear mapping of the symbols which have been sent one time-frame before. Instead, we introduce a code-block structure for handling this issue and reusing the prior result for layered networks [1]. We denote K consecutive time-frames as a *code-block*, where K is a large number.

Assume that L is the length of the longest path in the network that starts from the source of the single multicast session. In our coding schemes for acyclic networks, we set the symbols of the last L time-frames of every block equal to zero. Then, it will be straightforward to show that the information symbols which are sent at different blocks will not be mixed at any node. Arguments similar to that for layered-networks can be made about the definitions of decodable space with the difference that we use code-blocks instead of time-frames.

III. Description of Rotational Coding Scheme

In this section, we briefly review the rotational coding scheme and its properties. The encoding procedure at node Φ_k depends on the amount of rotations that are referred to as *keys*. It is important to choose the keys such that the interaction between different nodes leads to maximization of the dimension of the decodable space for any subset of nodes.

A. Rotational Coding Scheme for Layered Networks

We define *key* $f_{i,j,k,m}$ in acyclic networks to be an integer associated with the j^{th} element of the received vector and the i^{th} element of the transmitted vector by node Φ_k at m^{th} time-frame of a code-block. Thus each node has q^2 keys. The coding at node Φ_k is performed as follows. Let the rotation of a vector, say $\tilde{\mathbf{x}}_j^k$, by the integer value s be defined as $\tilde{\mathbf{x}}_j^k\{s\} = [x_{s+1,j}^k, x_{s+2,j}^k, \ldots, x_{T,j}^k, x_{1,j}^k, x_{2,j}^k, \ldots, x_{s,j}^k,]^{\text{tr}}$. Using the set of keys $f_{i,j,k,m}$, the vector $\tilde{\mathbf{y}}_i^k$ is obtained as:

$$\tilde{\mathbf{y}}_i^k = \sum_{j=1}^{q} \tilde{\mathbf{x}}_j^k \{f_{i,j,k,m}\} \tag{7}$$

The linear operation matrix $\mathbf{F}_m^k$ of node Φ_k can be obtained from (7) as

$$\begin{bmatrix} \tilde{\mathbf{y}}_1^k \\ \tilde{\mathbf{y}}_2^k \\ \vdots \\ \tilde{\mathbf{y}}_q^k \end{bmatrix} = \begin{bmatrix} \mathbf{I}\{f_{1,1,k,m}\} & \mathbf{I}\{f_{1,2,k,m}\} & \ldots & \mathbf{I}\{f_{1,q,k,m}\} \\ \mathbf{I}\{f_{2,1,k,m}\} & \mathbf{I}\{f_{2,2,k,m}\} & \ldots & \mathbf{I}\{f_{2,q,k,m}\} \\ \vdots & & & \vdots \\ \mathbf{I}\{f_{q,1,k,m}\} & \mathbf{I}\{f_{q,2,k,m}\} & \ldots & \mathbf{I}\{f_{q,q,k,m}\} \end{bmatrix} \cdot \begin{bmatrix} \tilde{\mathbf{x}}_1^k \\ \tilde{\mathbf{x}}_2^k \\ \vdots \\ \tilde{\mathbf{x}}_q^k \end{bmatrix} = \mathbf{F}_m^k \begin{bmatrix} \tilde{\mathbf{x}}_1^k \\ \tilde{\mathbf{x}}_2^k \\ \vdots \\ \tilde{\mathbf{x}}_q^k \end{bmatrix} \tag{8}$$

where $\mathbf{I}\{f_{.,.,.,.}\}$ denotes the rotation of rows of the matrix $\mathbf{I}$ by the amount $f_{.,.,.,.}$.

One proper choice of the keys is as follows. Enumerate all possible choices of the keys and assign each pair (i,j,k,m) a unique number $e_{i,j,k,m}$ between 1 and $q^2(N+1)K$. Define $f_{i,j,k,m} = (q+1)^{e_{i,j,k,m}}$ where $e_{i,j,k,m}$ is a unique natural number for $i,j = 1,2,\ldots,q$ and $k = 1,2,\ldots,N$, and $m = 1,2,\ldots,K$. The keys for the nodes based on rotational coding scheme at each node transform the received frame of size T to the output frame. It can be verified that for any two disjoint subset of $(i,j,k,m) \in \Xi_1$ and $(i,j,k,m) \in \Xi_2$, we have

$$\sum_{(i,j,k,m)\in\Xi_1} \alpha_{i,j,k,m} \cdot f_{i,j,k,m} \neq \sum_{(i,j,k,m)\in\Xi_2} \alpha_{i,j,k,m} \cdot f_{i,j,k,m} \tag{9}$$

where $\alpha(.,.,.,.) \in \{1,2,\ldots,q\}$. We choose T very large compare to the values of $f_{i,j,k,m}$.

IV. Rotational Coding Scheme for Acyclic Networks

In this section, we explain how to use the rotational coding scheme to achieve the minimum cutset bound in acyclic networks, i.e., the rate of information that can be sent from the source to any arbitrary destination is (almost) equal to the minimum cutset bound between the source and the destination. Note that by 'almost' we mean that the rate can be achieved in the limit of large codeword size T; for finite T there would be a negligible loss in the rate in comparison to the cutset bound.

We denote the set of cutsets between the source and a terminal node k_i by $\Lambda_{k_i} = \{\Omega : \Omega \subset \{0, 1, \dots, N\}, 0 \in \Omega, N \in \Omega^c\}$ and define the minimum cutset rank between the source and the destination as

$$r_{\min} = \min_{k_i \in \text{terminals}} \min_{\Omega \in \Lambda_{k_i}} \{|\mathbf{G}_{\Omega}^{\Omega^c}|\} \tag{10}$$

If the multicast session contains more than one terminal, then we define $r_{\min}$ as the minimum value among the minimum cutset ranks of different terminals. The following result was proved in [1] that for the layered network the cutset bound can be achieved in the limit of large T.

Theorem 1 (Achievability Theorem in Layered Networks [1]): Assume a single multicast session in a layered wireless network and define $r_{\min}$ as (10). The rate of $R = n \log_2(p) r_{\min}(1 - o(T)/T)$ can be achieved using rotational coding scheme. Clearly, the achievable rate becomes equal to the minimum cutset bound of the multicast session as $T \to \infty$.

We are extending this result and show that the minimum cutset bound can be achieved for any acyclic network. We have the following Theorem.

Theorem 2 (Achievability Theorem in Acyclic Networks): Assume a single multicast session in a acyclic wireless network and define $r_{\min}$ as (10). The rate of $R = n \log_2(p)[(K - L)r_{\min}T - qT - o(T)]/(KT)$ can be achieved using the rotational coding scheme with proper key setting algorithm defined in Section III. Clearly, the achievable rate is equal to the minimum cutset bound of the multicast session when $K, T \to \infty$.

Proof of Theorem 2: Denote Φ_k as an arbitrary destination in the network. We unfold the network graph over the K time-frames to demonstrate the information flow in a block. We first claim that the minimum cutset size in the unfolded graph is at least $r_{\min}^{\text{block}} \geq (K - L)r_{\min}T - qT$. If we apply Theorem 1 for the unfolded graph which is a layered network, then we can conclude that the linear mapping which maps inputs of Φ_0 to inputs of Φ_k has rank of $r_{\min}^{\text{block}}$. Therefore, the destination can decode information sent by the source at rate of $R = \frac{(K-L)r_{\min}T - qT - o(T)}{KT} \cdot n \log_2(p)$. Clearly, $R \to n \log_2(p) \cdot r_{\min}$ as $K, T \to \infty$.

For proving the claim, we consider a cutset of the unfolded graph. For example please see Figure 1. Since frames $m = K - L + 1, \dots, K$ are not used by the source for sending information, we only consider the part of cutset which is located between $m = 1, \dots, K - L$. Note that the cutset of the unfolded graph consists of $K - L$ cutsets over different frames which separate the source from the destination in all frames. In other words, the cutset in the unfolded graph can be written as $(\Omega_1, \dots, \Omega_{K-L})$ where Ω_m is an arbitrary subset of nodes which includes the source. Now we have

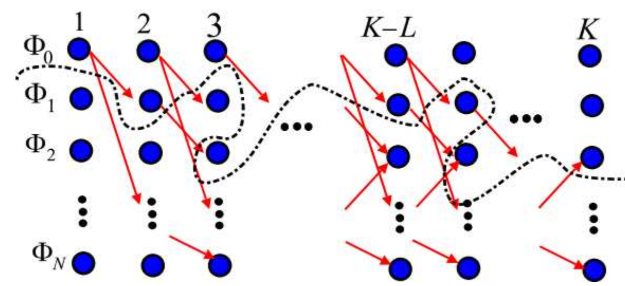

Fig. 1. The unfolded network graph is over time-frames of a block. The arrows represent the transmissions at different time-frames. The dotted line show an arbitrary cutset in the unfolded graph which separates the source (Φ_0) from a terminal. Ω_m is the set of nodes which belong to the top area of the dotted line at time-frame m.

$$\begin{aligned}
r_{\min}^{\text{block}} &\geq \sum_{m=1}^{K-L-1} |\mathbf{H}_{\Omega_m}^{(\Omega_{m+1})^c}| \\
&= |\mathbf{H}_{\Omega_{K-L}}^{(\Omega_1)^c}| - |\mathbf{H}_{\Omega_{K-L}}^{(\Omega_1)^c}| + \sum_{m=1}^{K-L-1} |\mathbf{H}_{\Omega_m}^{(\Omega_{m+1})^c}| \\
&\geq |\mathbf{H}_{\Omega_{K-L}}^{(\Omega_1)^c}| - qT + \sum_{m=1}^{K-L-1} |\mathbf{H}_{\Omega_m}^{(\Omega_{m+1})^c}| \\
&\stackrel{(a)}{\geq} -qT + \sum_{i=1}^{K-L} |\mathbf{H}_{[\Omega_1,\dots,\Omega_{K-L}]_i}^{[\Omega_1^c,\dots,\Omega_{K-L}^c]_{K-L-i+1}}| \\
&= -qT + \sum_{i=1}^{K-L} |\mathbf{H}_{[\Omega_1,\dots,\Omega_{K-L}]_i}^{([\Omega_1,\dots,\Omega_{K-L}]_i)^c}| \\
&\geq (K - L)r_{\min}T - qT
\end{aligned} \tag{11}$$

In above formulas $|.|$ is used to represent the matrix rank. The latter inequality (a) is obtained by applying Lemma 1 explained in the following.

■

Here, two notes are in order. First, the loss due to the acyclic nature of the network is exactly L/K. Therefore, if the maximum length of the path from source to any destination, i.e., L, is known, then by controlling the number of codewords in the code block, i.e., K, we can precisely control the loss in performance. The factor $(K - L)/L$ comes from the fact that in the last L blocks the source has to be quiet and cannot send new information. This can be interpreted as flushing out the information from the nodes in the network and getting prepared for transmission of the next code block.

It is obvious that the proof of Theorem 2 is mainly based on Lemma 1. For proving the Lemma, we generalizing the statement by arguing about two linear transformations of two arbitrary subsets of a given vector space under certain condition in the following lemma and corollaries.

Lemma 1: Let $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ be four subsets of the nodes in the network. Then,

$$|\mathbf{G}_{\mathcal{A}}^{\mathcal{B}}| + |\mathbf{G}_{\mathcal{C}}^{\mathcal{D}}| \geq |\mathbf{G}_{\mathcal{A}\cap\mathcal{C}}^{\mathcal{B}\cup\mathcal{D}}| + |\mathbf{G}_{\mathcal{A}\cup\mathcal{C}}^{\mathcal{B}\cap\mathcal{D}}|$$

This property can be generalized as follows. Let $\{\Omega_1, \Omega_2, \ldots, \Omega_l\}$ and $\{\Theta_1, \Theta_2, \ldots, \Theta_l\}$ be two sets where each of them contain l subsets of the nodes in the network. Then,

$$\sum_{i=1}^{l} |\mathbf{G}_{\Omega_i}^{\Theta_i}| \geq \sum_{i=1}^{l} |\mathbf{G}_{[\Omega_1,\ldots,\Omega_l]_i}^{[\Theta_1,\ldots,\Theta_l]_{l-i+1}}| \tag{12}$$

Lemma 2: Let V be a vector space, W_1 and W_2 two subspaces of V. Furthermore let $\mathbf{G}_1$ and $\mathbf{G}_2$ be two linear transformations from V to V such that:

1- $\mathbf{G} := \mathbf{G}_1\mathbf{G}_2 = \mathbf{G}_2\mathbf{G}_1$.

2- $\ker \mathbf{G}_1 \cap \ker \mathbf{G}_2 = \{0\}$.

Then we have

$$\begin{aligned} \dim(\mathbf{G}_1(W_1)) + \dim(\mathbf{G}_2(W_2)) \quad \geq \quad & \dim(W_1 \cap W_2) + \\ & \dim(\mathbf{G}(W_1 + W_2)) \end{aligned}$$

Proof of Lemma 2: On the one hand, we know that

$$\dim(\mathbf{G}_i(W_i)) = \dim(W_i) - \dim(W_i \cap \ker \mathbf{G}_i)$$

for $i = 1, 2$, and similarly

$$\dim(\mathbf{G}(W_1+W_2)) = \dim(W_1+W_2) - \dim((W_1+W_2) \cap \ker \mathbf{G})$$

On the other hand, we have

$$\dim(W_1 + W_2) = \dim(W_1) + \dim(W_2) - \dim(W_1 \cap W_2)$$

Altogether we have to prove the following inequality:

$$\begin{aligned} \dim((W_1 + W_2) \cap \ker \mathbf{G}) \quad \geq \quad & \dim(W_1 \cap \ker \mathbf{G}_1) + \\ & \dim(W_2 \cap \ker \mathbf{G}_2) \end{aligned}$$

To show this inequality, it is enough to notice that

$$\ker \mathbf{G}_1 + \ker \mathbf{G}_2 \subseteq \ker \mathbf{G}$$

because $\mathbf{G}_1\mathbf{G}_2 = \mathbf{G}_2\mathbf{G}_1$,

$$\begin{aligned} & \dim(W_1 \cap \ker \mathbf{G}_1) + \dim(W_2 \cap \ker \mathbf{G}_2) \\ & = \dim((W_1 + \ker \mathbf{G}_1) + (W_2 + \ker \mathbf{G}_2)) \end{aligned}$$

because $\ker \mathbf{G}_1 \cap \ker \mathbf{G}_2 = \{0\}$, and

$$(W_1 + \ker \mathbf{G}_1) + (W_2 + \ker \mathbf{G}_2) \subseteq (W_1 + W_2) \cap (\ker \mathbf{G}_1 + \ker \mathbf{G}_2).$$

■

Corollary 1: Let $\mathbb{F}$ be a field, V' a vector space over $\mathbb{F}$, $\mathbf{T} : V' \to V = \mathbb{F}^m$ a linear transformation, $\mathbf{G}_1$ the projection onto the first k_1 components, and $\mathbf{G}_2$ the projection onto the last k_2 components, where $k_1 + k_2 \geq m$. Furthermore let V_1 and V_2 be two subspaces of V' and $\mathbf{G}$ the projection onto the "middle" $k_1 + k_2 - m$ components. Then we have

$$\begin{aligned} \dim \mathbf{G}_1(\mathbf{T}(V_1)) + \dim \mathbf{G}_2(\mathbf{T}(V_2)) \quad \geq \quad & \dim \mathbf{T}(V_1 \cap V_2) + \\ & \dim \mathbf{G}(\mathbf{T}(V_1 + V_2)) \end{aligned}$$

Proof of Corollary 1: It is a direct consequence of Lemma 2, for $W_i = \mathbf{T}(V_i)$. (Notice that $\dim \mathbf{T}(V_1) \cap \mathbf{T}(V_2) \geq \dim \mathbf{T}(V_1 \cap V_2)$.) ■

Corollary 2: Let $\mathbb{F}$ be a field, $\mathbf{T} : \mathbb{F}^n \to \mathbb{F}^m$ be a linear transformation. Then

$$\dim \mathbf{G}_1(\mathbf{T}(\mathbb{F}^{l_1} \oplus \{0\}^{n-l_1})) + \dim \mathbf{G}_2(\mathbf{T}(\{0\}^{n-l_2} \oplus \mathbb{F}^{l_2}))$$

is at least

$$\dim \mathbf{T}(\{0\}^{n-l_2} \oplus \mathbb{F}^{l_1+l_2-n} \oplus \{0\}^{n-l_1}) + \dim \mathbf{G}(\mathbf{T}(\mathbb{F}^n)),$$

where $l_1 + l_2 \geq n$, $\mathbf{G}_1$, $\mathbf{G}_2$, and $\mathbf{G}$ are as in Corollary 1.

Proof of Lemma 1: We can prove the lemma by setting $A = \{1, \cdots, l_1\}$ and $C = \{n - l_2 + 1, \cdots, n\}$ for the domain space and $B = \{1, \cdots, k_1\}$ and $D = \{m - k_2 + 1, \cdots, m\}$ for the co-domain space in Corollary .

The second part of the lemma can be proved easily by induction on the number of sets (l) and using the first part. ■

V. Conclusion

In this paper, we considered a network coding scheme called *rotational coding* for wireless networks modeled by deterministic channel model [2], [3]. We proved that this coding scheme can achieve the minimum cutset bound for a single multicast session in acyclic wireless networks. Our result extends the current capacity achieving property of the rotational coding scheme for the layered networks to general acyclic networks.

References

[1] M. A. Khojastepour and A. Keshavarz-Haddad, "Rotational coding achieves multicast capacity of deterministic wireless networks," in *Allerton*, 2009.

[2] S. Avestimehr, S. Diggavi, and D. Tse, "A deterministic approach to wireless relay networks," in *ISIT*, 2007.

[3] ——, "Wireless network information flow," in *Allerton*, 2007.

[4] M. A. Khojastepour and A. Keshavarz-Haddad, "On capacity of deterministic relay networks," in *Allerton*, 2008.

[5] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.

[6] S. Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003.

[7] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Network*, vol. 11, no. 5, pp. 782–795, 2003.