

Article

Subspace Coding for Networks with Different Level Messages

Feng Cai *, Ning Cai and Wangmei Guo

The State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China; E-Mails: caining@mail.xidian.edu.cn (N.C.); wangmeiguo@mail.xidian.edu.cn (W.G.)

* Author to whom correspondence should be addressed; E-Mail: fcai@mail.xidian.edu.cn.

Academic Editor: Raúl Alcaraz Martínez

Received: 06 July 2015 / Accepted: 14 September 2015 / Published: 21 September 2015

Abstract: We study the asymptotically-achievable rate region of subspace codes for wireless network coding, where receivers have different link capacities due to the access ways or the faults of the intermediate links in the network. Firstly, an outer bound of the achievable rate region in a two-receiver network is derived from a combinatorial method. Subsequently, the achievability of the outer bound is proven by code construction, which is based on superposition coding. We show that the outer bound can be achieved asymptotically by using the code presented by Koetter and Kschischang, and the outer bound can be exactly attained in some points by using a q -analog Steiner structure. Finally, the asymptotically-achievable rate region is extended to the general case when the network has m receivers with different levels.

Keywords: network coding; error correcting; achievable rate region; projective spaces; Kruskal–Katona theorem; block design

1. Introduction

Network coding, introduced in [1,2], has attracted a substantial amount of research attention. It is a technique in which the intermediate node is allowed to make a combination of its received packets before sending the combined packet out to the network. This method can effectively improve the network throughput. However, there are still many problems to be studied, such as the collection of information about the network topology [3]. As the scale of the network grows, the complexity of network code construction increases accordingly. To address this issue, random network coding was proposed by Ho *et al.* [4] without considering network topology, where the intermediate nodes select

coding coefficients at random from a finite field. It becomes an effective and robust tool when the network topology changes dynamically, especially in the case of a wireless network. Furthermore, since the characteristics of the wireless channel are time-varying in general, packets lost and errors are important factors affecting transmission performance. Therefore, error control in wireless network coding is essential [5,6].

Taking the advantage of the distance property of vector space, Koetter and Kschischang proposed the subspace metric codes for random network coding [7], where a subspace is used to represent a codeword. Even if partial changes occur in the received subspace, as long as the distance between the received subspace and the transmitted subspace satisfies a certain distance relationship, the message could still be decoded successfully. Closely relevant works about the coding bounds and the packing and covering properties of subspace codes are presented in [8–10]. However, the existing works about subspace codes are based on the multicast network model.

In this paper, we study a real-time media distribution system based on heterogeneous wireless networks, where end users are intelligent devices, such as smart TVs, mobile phones and computers. These terminals access the networks with different link capacities. There are several factors that make the link capacities different, such as the various ways that they access the networks (e.g., WLAN or mobile network), the packets lost and errors (due to the fault of the intermediate nodes or link failure) [11,12]. In this case, the terminals with high link capacity can receive more useful data, which means that some receivers are “stronger” than the others. For example, because they access the networks in a more stable way, they can always receive more than the “weaker” ones. Each end user wants to maximize the utilization of his link capacity to provide his best service. To meet the diverse requirements of the users, it is complex and a waste of resources to design the transmission approach for each user. A better solution is coding at the source node; then, the source node broadcasts the same encoded packets to the receivers, and each user collects as many packets as possible and then decodes to meet his requirement. A trivial coding method is to design a code corresponding to the “weaker” receiver. However, in this way, the “stronger” node cannot get his best service.

We assume that the media can be divided into several different priority levels according to their importance. The higher priority can ensure the basic demand of users. Meanwhile, the lower priority can guarantee the additional needs of users. To simplify the problem, we take the simplest case that there are only two receivers in the network. First, we derive an outer bound for the asymptotically-achievable rate region by a combinatorial method. Then, we prove the achievability of the outer bound by code construction with the codes that were proposed by Koetter and Kschischang (K-K codes) [7]. However, K-K codes require the dimension of ground space to be sufficiently large. We observe that the q -analog Steiner structure can be used in our construction. Our outer bound could be exactly attained in some points using a q -analog Steiner structure. We further extend our result to the general case of m receivers with different link capacities.

The rest of this paper is organized as follows. In Section 2.1, we briefly review the subspace code. Then, we observe that deletion correcting is equivalent to deletion and insertion error correcting in constant dimension codes. In Section 2.2, we extend the model to broadcast, which leads us to the definition of broadcast error correction network codes (BECNC). We state the asymptotically-achievable rate region of BECNC in Section 3. The main results are proven in Section 4. In Section 5, we present

that the outer bound can be exactly attained in some points using the q -analog Steiner structure. In Section 6, we generalize the rate region to the network with more than two receivers.

2. Preliminaries and Our Model

2.1. Previous Results: Subspace Metric Codes

We begin with previous results about subspace metric codes, which were proposed by Koetter and Kschischang [7]. It is necessary to introduce the previous results of subspace metric codes, since our works are based on them.

In the “noncoherent” model, the transmitter and receiver are assumed to have no knowledge of the channel transfer matrix. Let \mathbb{F}_q be a finite field with q elements. We use $\mathbb{F}_q^{l \times k}$ to denote the set of all $l \times k$ matrices over \mathbb{F}_q . In the error free case, the transmission model can be characterized as $\mathbf{Y} = \mathbf{F}\mathbf{X}$, where $\mathbf{F} \in \mathbb{F}_q^{l \times k}$ is a full rank random matrix (the channel transfer matrix), $\mathbf{X} \in \mathbb{F}_q^{k \times n}$ is the transmitted matrix whose rows can be considered as source packets [11] and $\mathbf{Y} \in \mathbb{F}_q^{l \times n}$ is the received matrix whose rows can be considered as received packets.

Since the receiver does not know \mathbf{F} , he only knows that the rows of \mathbf{X} and \mathbf{Y} span the same subspace. Then, he can correctly recover the transmitted space when no error occurs, if we regard space spanned by the rows of \mathbf{X} as a codeword.

However, the transmitted space will be a subspace of the received space by the receiver when an insertion error occurs, whereas the receiver will receive a subspace of the transmitted space when a deletion occurs [7].

\mathbb{F}_q^n can be regarded as an n -dimensional vector space over \mathbb{F}_q . Let $\mathcal{P}_q(n)$ denote the set of all subspaces of \mathbb{F}_q^n , forming the n -order projective space over \mathbb{F}_q [17]. A subspace metric code \mathcal{C} is a nonempty set of subspaces of \mathbb{F}_q^n , where each codeword is a vector space spanned by the rows of a message matrix. Let $U, V \in \mathcal{P}_q(n)$ be two subspaces; the subspace distance between them is defined as $d(U, V) = \dim(U) + \dim(V) - 2 \dim(U \cap V)$, where $\dim(U)$ is the dimension of U . The minimum distance of code \mathcal{C} is defined as $D(\mathcal{C}) = \min_{U, V \in \mathcal{C}: U \neq V} d(U, V)$. If:

$$D(\mathcal{C}) > 2(t + \rho), \tag{1}$$

then a minimum distance decoder will produce the transmitted space from the received space, where t and ρ denote the maximum number of deletion and insertion errors induced by the channel, respectively. Deletion is actually the packets lost, and insertion error is equivalent to malicious attack.

In this paper, we only consider the constant dimension codes, where the dimensions of all codewords in \mathcal{C} are the same. Let $\mathcal{P}_q(n, k)$ denote the set of all k -dimensional subspaces ($k \leq n$) of the n -dimensional vector space \mathbb{F}_q^n . This means that constant dimension code \mathcal{C} is a subset of $\mathcal{P}_q(n, k)$. The normalized weight is defined as $\lambda = k/n$, where k is the dimension of codewords. The rate of the code is defined as $R = \frac{\log_q |\mathcal{C}|}{nk}$.

In [7], Koetter and Kschischang obtained the Singleton-type bound of the subspace codes and constructed a Singleton bound-achieving code using the linearized polynomial. We refer to this code as the K-K code in the following. The Singleton-type bound is shown in the following lemma.

Lemma 1 (Corollary 10 of [7]). *Let \mathcal{C} be a collection of subspaces in $\mathcal{P}_q(n, k)$, with normalized minimum distance $\delta = \frac{D(\mathcal{C})}{2k}$. The rate of \mathcal{C} is bounded by:*

$$R \leq (1 - \delta)(1 - \lambda) + o(1), \tag{2}$$

where $\lambda = k/n$ is the normalized weight and $o(1)$ approaches zero as n grows.

They also mentioned that, for the decoder, the effects of insertion and deletion are equivalent in constant dimension codes. Furthermore, there may be an intersection between the insertion subspace and the transmitted subspace, which would possibly decrease the number of deletions seen by the receiver. In other words, the negative impact brought by simple deletion is not less than the negative impact caused by deletion and insertion simultaneously. Next, we will discuss the case of only deletions.

Observe that a subspace V_r is received at the receiver; the minimum distance decoder will decode V_r to V_s , if the distance between V_r and V_s is minimal among all of the codewords in \mathcal{C} , i.e.,

$$d(V_r, V_s) = \min_{V \in \mathcal{C}} d(V_r, V). \tag{3}$$

We define the operation of deletions as mapping \mathcal{D}_τ . For a given k -dimensional subspace V , $\mathcal{D}_\tau(V)$ produces a random $(k - \tau)$ -dimensional subspace of V , where $\tau \geq 0$. We say that a code is capable of correcting τ deletions, if it can correct τ deletions using the decoding criterion in (3). We refer to such a code as a τ -deletion-correcting code, and its minimum distance must satisfy:

$$D(\mathcal{C}) > 2\tau. \tag{4}$$

Let $V_r = \mathcal{D}_\tau(V)$ be the received subspace and $V' \neq V$ be any other codeword in \mathcal{C} , then $D(\mathcal{C}) \leq d(V', V) \leq d(V', V_r) + d(V_r, V)$; it follows that $d(V', V_r) \geq D(\mathcal{C}) - d(V_r, V)$. If the condition (4) could be satisfied, then $d(V', V_r) > d(V_r, V)$, the minimum distance decoder will produce the transmitted subspace V from the received subspace.

Remark 1. *Since Condition (4) coincides with Condition (1), a τ -deletion-correcting code can correct t deletions and ρ insertions, if $t + \rho = \tau$. Thus, it is sufficient for us to focus on deletion-correcting codes, because for this reason, all our results below for deletion hold for deletion and insertion, as well.*

An (n, k, M, τ) -deletion-correcting code \mathcal{C} over \mathbb{F}_q is a k -dimensional subspace code over \mathbb{F}_q^n with M codewords whose maximum deletion-correcting capability is τ . The rate of code \mathcal{C} is $R = \frac{\log_q M}{nk}$.

Definition 1. *A rate R is said to be (λ, μ) -asymptotically achievable if, for all $\epsilon > 0$ and sufficiently large n , there exists an (n, k, M, τ) -deletion-correcting code, such that $\frac{\log_q M}{nk} > R - \epsilon$, where $\mu = \tau/k$ and $\lambda = k/n$.*

The network model of [7] is multicast, which is actually a point-to-point communication channel with just one sender and one receiver. In next subsection, we will extend the model to broadcast, which consists of one sender and m receivers.

2.2. Network Model

We are motivated by a real-time media distribution system based on heterogeneous wireless networks, where end users are individual intelligent terminals, such as tablets, smart phones and computers. These intelligent terminals access the network with heterogeneous link capacities. The difference of link capacities may be caused by different access ways (e.g., WLAN and mobile network) or the instability of their links.

We assume that the media can be divided into different priority levels corresponding to the link capacity of receivers. The higher priority level guarantees the basic media quality, and the lower priority level corresponds to detailed information about media. Let $\{\mathcal{M}_1, \mathcal{M}_2, \dots, \mathcal{M}_m\}$ be a collection of m message sets with ordered priority, where the index $i \in \{1, \dots, m\}$ indicates the priority level, and the smaller index corresponds to the higher-priority level. Without loss of generality, we assume there are m receivers in the network, each of which has a different level of link capacity. Let $\{t_1, t_2, \dots, t_m\}$ be the ordered set of receivers, where the index $i \in \{1, \dots, m\}$ indicates the link capacity; the smaller index corresponds to the higher link capacity.

The media is encoded into packets that can be sent to the network. For arbitrary $l \in \{1, \dots, m\}$, the receiver t_l downloads the packets with its link capacity constraint. Although there exist some packets lost and errors in its link, t_l can recover the messages with priority levels $\{1, 2, \dots, m - l + 1\}$. Therefore, with respect to the receiver with lower link capacity, the receiver with higher link capacity can obtain more detailed information, and it can get clearer vision effects by decoding its received packets.

For simplicity of presentation, we focus the discussion on the network with two receivers nodes t_1, t_2 . The extension to an arbitrary number of receivers is straightforward. This model can be regarded as a combinatorial version of the asymmetric two-output broadcast channel [18] in projective space. We show it in Figure 1. The media is divided into two priority level message sets \mathcal{M}_1 and \mathcal{M}_2 . The receiver t_1 has a higher link capacity than t_2 . This means that the receiver t_1 can recover both messages $i \in \mathcal{M}_1$ and $j \in \mathcal{M}_2$; meanwhile, the receiver t_2 can only decode the message $i \in \mathcal{M}_1$ during the transmission. We assume that a message pair (i, j) is encoded into a codeword with k packets. Let τ_1 and τ_2 be the numbers of errors occurring at the link of receiver t_1 and t_2 , respectively. Receiver t_1 and t_2 can collect $(k - \tau_1)$ and $(k - \tau_2)$ independent packets with no error, respectively. We assume that $\tau_2 > \tau_1$, i.e., the receiver t_1 can receive more correct packets than t_2 .

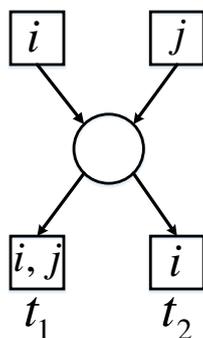


Figure 1. Asymmetric two-output broadcast channel.

Our aim is to design a code \mathcal{C} with which the receivers can decode their messages correctly as long as they received $(k - \tau_1)$ and $(k - \tau_2)$ independent packets with no error, respectively. Meanwhile, we are interested in the achievable rate region of the code. Although both deletion and insertion errors should be considered, it is sufficient to consider deletion error according to Remark 1.

Let $\mathcal{M}_1 = \{1, 2, \dots, M_1\}$ and $\mathcal{M}_2 = \{1, 2, \dots, M_2\}$ be two message sets, where \mathcal{M}_1 has higher level priority. The message pair $(i, j) \in (\mathcal{M}_1, \mathcal{M}_2)$ is encoded into codeword $V_{i,j}$ of \mathcal{C} by encoding mapping. Then, the codeword will be transmitted to the network. Due to the packets lost, the receiver t_1 can receive a $(k - \tau_1)$ -dimensional subspace U_1 , and the receiver t_2 can receive a $(k - \tau_2)$ -dimensional subspace U_2 . If the codewords satisfy some conditions, the messages (i, j) and i can be decoded correctly at t_1 and t_2 , respectively. The conditions will be discussed at the end of Section 4.1. In this case, the receiver t_1 can recover messages i and j . Meanwhile, the receiver t_2 can only recover message i . Next, we formally state the definition of such code.

Definition 2. Let t_1 and t_2 be the two receiver nodes of an acyclic single source network; the corresponding numbers of errors occurring at the link of receiver t_1 and t_2 are τ_1 and τ_2 , respectively, $\tau_2 > \tau_1$. A constant dimension code $\mathcal{C} \subseteq \mathcal{P}_q(n, k)$ is called an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC (broadcast error-correcting network code), if it satisfies that the two receivers can correct errors of τ_1 and τ_2 , respectively. The cardinalities of the two corresponding message sets are M_1 and M_2 .

We are interested in the maximum number of message set pairs (M_1, M_2) , when the dimension and the maximum numbers of correctable errors are given. Sometimes, the asymptotic rate pairs are also interesting.

The asymptotic rate pair is defined as (R_1, R_2) , where $R_i = \frac{\log_q M_i}{nk}, i = 1, 2$.

Definition 3. A rate pair of non-negative real numbers (R_1, R_2) is said to be (λ, μ_1, μ_2) -asymptotically achievable if, for all $\epsilon > 0$ and sufficiently large n , there exists an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC, such that $\frac{\log_q M_i}{nk} > R_i - \epsilon, i = 1, 2$, where $\tau_1/k = \mu_1, \tau_2/k = \mu_2$ and $k/n = \lambda$. The asymptotically-achievable rate region is the set of all asymptotically-achievable rate pairs.

3. Main Results

We now state the asymptotically-achievable rate region of the broadcast error-correcting network codes. The proof of the theorem will be presented in next section.

Theorem 1. The asymptotically-achievable rate region of an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC with corresponding error-correcting capability τ_1 and τ_2 over field \mathbb{F}_q consists of pairs (R_1, R_2) of non-negative numbers that satisfy the inequalities,

$$R_1 \geq 0, R_2 \geq 0 \tag{5}$$

$$R_1 \leq (1 - \mu_1)(\lambda_x - \lambda), \tag{6}$$

$$R_2 \leq (1 - \mu_2)(1 - \lambda_x), \tag{7}$$

where x is an auxiliary variable, such that $k \leq x \leq n$. The normalized weights are $\lambda_x = x/n, \lambda = k/n$, and the normalized error-correcting capabilities are $\mu_1 = \tau_1/k, \mu_2 = \tau_2/k$.

4. Proofs

Before proving the theorem, we introduce some auxiliary results in combinatorial mathematics, which are used in the proof of our results.

4.1. Combinatorial Lemmas

This part, however, is rather technical. The readers who are not interested in it can just skim the conclusion without missing the essence of this section.

The number of elements in $\mathcal{P}_q(n, k)$ is given by the Gaussian coefficient,

$$|\mathcal{P}_q(n, k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}. \tag{8}$$

The subscript q of the Gaussian coefficient will be omitted without causing ambiguity in the following text.

The asymptotic behavior of the Gaussian coefficient is given by the following lemma.

Lemma 2 ([7]). *Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$, for $0 < k < n$ satisfies:*

$$1 < q^{-k(n-k)} \begin{bmatrix} n \\ k \end{bmatrix} < 4. \tag{9}$$

We will introduce an important definition in combinatorial mathematics, which is very useful in our proof.

Let \mathcal{J} be a collection of k -subsets of an n -set S , $0 \leq k \leq n$. The collection:

$$\partial\mathcal{J} := \left\{ K \in \binom{S}{k-1} : K \subset J, \text{ for some } J \in \mathcal{J} \right\}$$

is called the shadow of \mathcal{J} , where $\binom{S}{k-1}$ denotes the set of all $(k - 1)$ -subsets of S . That is, $\partial\mathcal{J}$ consists of all subsets of S , which can be obtained by deleting an element from a set in \mathcal{J} .

The lower bound of the size of a shadow is given by the Kruskal–Katona theorem [13,14]. Additionally, Lovász [15] proposed a weaker and simpler form of the original theorem. In [16], Lovász’s theorem is extended to vector spaces.

For a given n -dimensional vector space W , we define the shadow as follows.

Definition 4. *Let \mathcal{F} be a collection of k -dimensional subspaces of an n -dimensional vector space W , where $k < n$. The shadow of \mathcal{F} is denoted by $\partial\mathcal{F}$,*

$$\partial\mathcal{F} := \left\{ E \in \begin{bmatrix} W \\ k-1 \end{bmatrix} : E \subset F, \text{ for some } F \in \mathcal{F} \right\},$$

where $\begin{bmatrix} W \\ k-1 \end{bmatrix}$ denotes the set of all $(k - 1)$ -dimensional subspaces of W .

A lower bound for the size of the shadow $\partial\mathcal{F}$ is shown in the following lemma.

Lemma 3 ([16]). Let $\mathcal{F} \subset \begin{bmatrix} W \\ k \end{bmatrix}$, and let $y \geq k$ be the positive integer, which satisfies $|\mathcal{F}| = \begin{bmatrix} y \\ k \end{bmatrix}$. Then, $|\partial\mathcal{F}| \geq \begin{bmatrix} y \\ k-1 \end{bmatrix}$. If equality holds, then $y \in \mathbb{Z}^+$ and $\mathcal{F} = \begin{bmatrix} Y \\ k \end{bmatrix}$, where Y is a y -dimensional subspace of W .

We extend Lemma 3 to the case of l -level shadow. Let $\partial^{(l)}\mathcal{F}$ denote the l -level shadow of a collection of k -dimensional subspaces of W . Namely, similarly to the definition of $\partial\mathcal{F}$, we define:

$$\partial^{(l)}\mathcal{F} := \left\{ E \in \begin{bmatrix} W \\ k-l \end{bmatrix} : E \subset F, \text{ for some } F \in \mathcal{F} \right\},$$

where $\begin{bmatrix} W \\ k-l \end{bmatrix}$ denotes the set of all $(k-l)$ -dimensional subspaces of W . For simplicity, the l -level shadow will be referred to as the l -shadow. The following lemma gives a lower bound of the size of the l -shadow.

Lemma 4. Let $\mathcal{F} \subset \begin{bmatrix} W \\ k \end{bmatrix}$, and let $y \geq k$ be the positive integer, which satisfies $|\mathcal{F}| = \begin{bmatrix} y \\ k \end{bmatrix}$. Then, $|\partial^{(l)}\mathcal{F}| \geq \begin{bmatrix} y \\ k-l \end{bmatrix}$ for $k \geq l$. If equality holds, then $y \in \mathbb{Z}^+$ and $\mathcal{F} = \begin{bmatrix} Y \\ k \end{bmatrix}$, where Y is a y -dimensional subspace of W .

Proof. Refer to Appendix A.1.

In Lemma 4, if the equality holds, there exists a y -dimensional subspace Y , such that $\partial^{(l)}\mathcal{F}$ is the set of all $(k-l)$ -dimensional subspaces of Y , for $0 \leq l \leq k$.

Since the cardinality of the set \mathcal{F} is not exactly equal to a Gaussian coefficient in general, we extend Lemma 4 to a general case in the following corollary.

Corollary 1. Let $\mathcal{F} \subset \begin{bmatrix} W \\ k \end{bmatrix}$ be a collection of k -dimensional subspaces of W and $|\mathcal{F}| \leq \begin{bmatrix} y \\ k \end{bmatrix}$, then

$$|\partial^{(l)}\mathcal{F}| \geq \frac{\begin{bmatrix} y \\ k-l \end{bmatrix}}{\begin{bmatrix} y \\ k \end{bmatrix}} |\mathcal{F}|.$$

Proof. Refer to Appendix A.2.

Corollary 1 gives the lower bound for the size of an l -shadow of a given collection of subspaces, which will be used in the proof of our result.

Using the representation of combinatorial mathematics, we discuss the conditions for correctly decoding BECNC. Due to the packets lost, the receiver t_1 can receive a $(k - \tau_1)$ -dimensional subspace

$U_1 \in \partial^{(\tau_1)}\{V_{i,j}\}$, and the receiver t_2 can receive a $(k - \tau_2)$ -dimensional subspace $U_2 \in \partial^{(\tau_2)}\{V_{i,j}\}$. We say that the receivers can decode correctly, if for t_1 :

$$\partial^{(\tau_1)}\{V_{i,j}\} \cap \partial^{(\tau_1)}\{V_{i',j'}\} = \emptyset, \text{ if } (i, j) \neq (i', j'), \tag{10}$$

and for t_2 :

$$\partial^{(\tau_2)}\{V_{i,j}\} \cap \partial^{(\tau_2)}\{V_{i',j'}\} = \emptyset, \text{ if } i \neq i', \forall j, j'. \tag{11}$$

4.2. Outer Bound

We prove the outer bound of the achievable rate region at first. By Remark 1, it is sufficient to consider the deletion error correcting in the proof. Inspired by the analogues between the definition of shadow and the packing sphere of deletion-correcting codes, we adopt the concept of shadow in combinatorial theory. Furthermore, there is a lower bound for the size of the shadow in vector space [16]. A small generalization of the lower bound is provided in Corollary 1, which will be used in the proof of the outer bound.

Theorem 2. (Outer bound of the achievable rate region) *If (R_1, R_2) is an achievable rate pair of an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC, $\mathcal{C} \subset \mathcal{P}_q(n, k)$, for an x with $k \leq x \leq n$, then the following inequalities hold,*

$$M_1 \leq \frac{\begin{bmatrix} n \\ k - \tau_2 \end{bmatrix} \begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}}{\begin{bmatrix} x \\ k - \tau_2 \end{bmatrix} \begin{bmatrix} x - 1 \\ k - \tau_1 \end{bmatrix}} \tag{12}$$

where x is the smallest integer, such that:

$$M_2 \begin{bmatrix} k \\ k - \tau_1 \end{bmatrix} \leq \begin{bmatrix} x \\ k - \tau_1 \end{bmatrix} \tag{13}$$

In particular, if the equality of (13) holds, we have:

$$M_1 \leq \frac{\begin{bmatrix} n \\ k - \tau_2 \end{bmatrix}}{\begin{bmatrix} x \\ k - \tau_2 \end{bmatrix}} \tag{14}$$

We can obtain the asymptotic form of Theorem 2 directly.

Corollary 2. *If (R_1, R_2) is an achievable rate pair of an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC, $\mathcal{C} \subset \mathcal{P}_q(n, k)$, for an x with $k \leq x \leq n$, then the following inequalities hold,*

$$R_1 \geq 0, R_2 \geq 0 \tag{15}$$

$$R_1 \leq (1 - \mu_1)(\lambda_x - \lambda), \tag{16}$$

$$R_2 \leq (1 - \mu_2)(1 - \lambda_x), \tag{17}$$

where $\lambda_x = x/n, \lambda = k/n$ are the normalized weights and $\mu_1 = \tau_1/k, \mu_2 = \tau_2/k$ are the normalized deletion-correcting capabilities.

Proof of Theorem 2. Let $\mathcal{V} = \{V_{i,j} : i = 1, 2, \dots, M_1, j = 1, 2, \dots, M_2\}$ be the codebook of an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC that can correct τ_1 and τ_2 deletions for receivers t_1 and t_2 , respectively, where $\dim(V_{i,j}) = k, \tau_1 < \tau_2 < k$ and $\delta = \tau_2 - \tau_1$.

For fixed i , we denote the τ_1 -shadow of the codeword $V_{i,j}$ as $\partial^{(\tau_1)}\{V_{i,j}\}$; then, the τ_1 -shadows of $V_{i,j}, j = 1, 2, \dots, M_2$ are disjoint, namely:

$$\partial^{(\tau_1)}\{V_{i,j}\} \cap \partial^{(\tau_1)}\{V_{i,j'}\} = \emptyset,$$

and the cardinality of each shadow is $|\partial^{(\tau_1)}\{V_{i,j}\}| = \binom{k}{k - \tau_1}$. We denote the set of these shadows as

$$SH(i) = \{\partial^{(\tau_1)}\{V_{i,j}\} : j = 1, 2, \dots, M_2\}; \text{ then, } |SH(i)| = M_2 \binom{k}{k - \tau_1}.$$

Figure 2 illustrates the relationship of τ_1 -shadows when i is fixed. The big dotted line circle on the top level denotes the set of codewords, in which small solid circles denote the codewords. The small solid circle on the middle level denotes the τ_1 -level shadow of a codeword, while the big dotted line circle on the middle level denotes the set of the τ_1 -level shadow. Similarly, a small solid circle on the bottom level denotes the τ_2 -level shadow of a codeword, while the big dotted line circle on the bottom level denotes the set of τ_2 -level shadows.

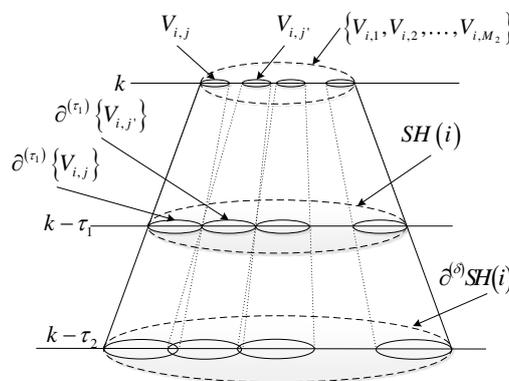


Figure 2. The relationship of τ_1 -shadows when i is fixed.

For $i \neq i'$ and any j, j' ,

$$\partial^{(\delta)}\partial^{(\tau_1)}\{V_{i,j}\} \cap \partial^{(\delta)}\partial^{(\tau_1)}\{V_{i',j'}\} = \emptyset,$$

because otherwise,

$$\partial^{(\tau_2)}\{V_{i,j}\} \cap \partial^{(\tau_2)}\{V_{i',j'}\} \neq \emptyset,$$

which is contradictory to Condition (11). That is, the δ -shadows of $SH(i)$ and $SH(i')$ are disjoint for all $i \neq i'$. From Corollary 1, we can get the minimum size of the δ -shadow of $SH(i)$, which is

bounded by $|\partial^{(\delta)}SH(i)| \geq \frac{\begin{bmatrix} x \\ k - \tau_2 \end{bmatrix}}{\begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}} |SH(i)|$, and $x \geq k - \tau_2$ is the minimum integer, such that

$$|SH(i)| \leq \begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}.$$

Then, we can get $M_2 \begin{bmatrix} k \\ k - \tau_1 \end{bmatrix} \leq \begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}$, and:

$$M_2 \leq \frac{\begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}}{\begin{bmatrix} k \\ k - \tau_1 \end{bmatrix}} \stackrel{(a)}{<} \frac{4q^{(k-\tau_1)(x-k+\tau_1)}}{q^{(k-\tau_1)(k-k+\tau_1)}} = 4q^{(k-\tau_1)(x-k)}. \tag{18}$$

The inequality (a) holds according to Lemma 2.

Now, we consider the cardinality of $\partial^{(\delta)}SH(i)$,

$$|\partial^{(\delta)}SH(i)| \geq \frac{\begin{bmatrix} x \\ k - \tau_2 \end{bmatrix}}{\begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}} |SH(i)| \stackrel{(b)}{\geq} \frac{\begin{bmatrix} x \\ k - \tau_2 \end{bmatrix}}{\begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}} \begin{bmatrix} x - 1 \\ k - \tau_1 \end{bmatrix}. \tag{19}$$

The inequality (b) holds since x is the minimum integer, such that $|SH(i)| \leq \begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}$, and the

Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ is monotone increasing with n .

By packing, M_1 is bounded by:

$$\begin{aligned} M_1 &\leq \frac{\begin{bmatrix} n \\ k - \tau_2 \end{bmatrix}}{|\partial^{(\delta)}SH(i)|} \leq \frac{\begin{bmatrix} n \\ k - \tau_2 \end{bmatrix} \begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}}{\begin{bmatrix} x \\ k - \tau_2 \end{bmatrix} \begin{bmatrix} x - 1 \\ k - \tau_1 \end{bmatrix}} \\ &\stackrel{(c)}{<} \frac{16q^{(k-\tau_2)(n-k+\tau_2)+(k-\tau_1)(x-k+\tau_1)}}{q^{(k-\tau_2)(x-k+\tau_2)+(k-\tau_1)(x-1-k+\tau_1)}} \\ &= 16q^{(k-\tau_2)(n-x)+(k-\tau_1)}. \end{aligned} \tag{20}$$

The inequality (c) holds according to Lemma 2.

Then, the rate pair of $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC, $\mathcal{C} \subset \mathcal{P}_q(n, k)$, satisfies:

$$\begin{aligned} R_1 &= \frac{\log_q M_2}{nk} \leq \frac{(k - \tau_1)(x - k)}{nk} + o(1) \\ &= (1 - \mu_1)(\lambda_x - \lambda) + o(1) \end{aligned} \tag{21}$$

and:

$$\begin{aligned} R_2 &= \frac{\log_q M_1}{nk} \leq \frac{(k - \tau_2)(n - x) + (k - \tau_1)}{nk} + o(1) \\ &= (1 - \mu_2)(1 - \lambda_x) + o(1), \end{aligned} \tag{22}$$

where $o(1)$ approaches zero as n grows, and x is an auxiliary variable, such that $k \leq x \leq n$. The normalized weights are $\lambda_x = x/n, \lambda = k/n$, and the normalized deletion-correcting capabilities are $\mu_1 = \tau_1/k, \mu_2 = \tau_2/k$.

This completes the proof of the outer bound. \square

4.3. Achievability

In this section, we propose a construction of BECNC based on superposition coding, with which the achievability of our outer bound can be proven. If the rate pair (R_1, R_2) is achievable, then the code used at each level must satisfy certain properties, which are specified below.

Construction: Let \mathbb{F}_q^n be an n -dimensional vector space over \mathbb{F}_q and x be an integer, such that $k \leq x \leq n$. We can construct an x -dimensional constant dimension subspace code \mathcal{C}_x over \mathbb{F}_q^n for t_1 and t_2 , such that it can correct deletions of $x - k + \tau_2$. The encoding mapping is \hat{f} , and the decoding mappings at t_1 and t_2 are $\hat{\varphi}$ and $\hat{\psi}$, respectively.

The codeword $\hat{f}(i)$ can be regarded as the cloud center, which will not be actually sent. For every $i \in \mathcal{M}_1$, the $(x - k + \tau_2)$ -shadows of $\{\hat{f}(i)\}$ are disjoint, namely,

$$\partial^{(x-k+\tau_2)}\{\hat{f}(i)\} \cap \partial^{(x-k+\tau_2)}\{\hat{f}(i')\} = \emptyset, \text{ for } i \neq i', \tag{23}$$

which guarantees the correctness of decoding at t_2 . The rate of \mathcal{C}_x is:

$$\frac{1}{nx} \log |\mathcal{M}_1|. \tag{24}$$

Additionally, for every $i \in \mathcal{M}_1$, the $(x - k + \tau_1)$ -shadow of $\{\hat{f}(i)\}$ must be disjoint; otherwise, the $(\tau_2 - \tau_1)$ -shadow of the $(x - k + \tau_1)$ -shadow of $\{\hat{f}(i)\}$ will have a common subset. That is,

$$\partial^{(x-k+\tau_1)}\{\hat{f}(i)\} \cap \partial^{(x-k+\tau_1)}\{\hat{f}(i')\} = \emptyset, \text{ for } i \neq i', \tag{25}$$

which guarantees the correctness of decoding at t_1 .

Let $A(i)$ be the $(x - k)$ -shadow of a codeword $\hat{f}(i)$, i.e.,

$$A(i) = \partial^{(x-k)}\{\hat{f}(i)\}, \tag{26}$$

the shadows $A(i), i \in \mathcal{M}_1$ are disjoint by construction of code \mathcal{C}_x .

To every $i \in \mathcal{M}_1$, by using $\hat{f}(i)$ as the ground space, we can construct a k -dimensional subspace code $\mathcal{C} \subseteq A(i)$ for t_1 , such that it can correct deletions of τ_1 . For each i , the code has the same message set \mathcal{M}_2 . The encoding mapping is f_i , and the decoding mapping is φ_i ; the rate of \mathcal{C} is:

$$\frac{1}{xk} \log |\mathcal{M}_2|. \tag{27}$$

The codewords of \mathcal{C} will be actually sent, which can be regarded as a satellite codeword. For every $i \in \mathcal{M}_1, j \in \mathcal{M}_2$, the τ_1 -shadows of $\{f_i(j)\}$ are disjoint, namely,

$$\partial^{(\tau_1)}\{f_i(j)\} \cap \partial^{(\tau_1)}\{f_{i'}(j')\} = \emptyset, \text{ for } (i, j) \neq (i', j'), \tag{28}$$

which guarantees the correctness of decoding at t_1 .

The encoding mapping:

$$f : \mathcal{M}_1 \times \mathcal{M}_2 \rightarrow \mathcal{P}(n, k),$$

and the decoding mapping:

$$\varphi : \mathcal{P}(n, k - \tau_1) \rightarrow \mathcal{M}_1 \times \mathcal{M}_2,$$

and:

$$\psi : \mathcal{P}(n, k - \tau_2) \rightarrow \mathcal{M}_1,$$

are as follows:

$$\begin{aligned} f(i, j) &= f_i(j), \text{ for every } i \in \mathcal{M}_1, j \in \mathcal{M}_2, \\ \varphi(V_{r1}) &= (i, \varphi_i(V_{r1})), \text{ where } i = \hat{\varphi}(V_{r1}), \\ \psi(V_{r2}) &= \hat{\psi}(V_{r2}), \end{aligned}$$

where $V_{r1} \in \mathcal{P}(n, k - \tau_1)$ and $V_{r2} \in \mathcal{P}(n, k - \tau_2)$ are the subspaces received by node t_1 and t_2 , respectively.

We do not specify the code \mathcal{C}_x and \mathcal{C} used at each level in the above construction. The achievability of our outer bound could be proven if the subspace code used at each level satisfies some properties.

Proposition 1. *For an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC, our outer bound could be achieved at (R_1, R_2) asymptotically by the above construction, if there exists an (n, k, M, τ) -deletion-correcting code for single-user communication, such that the code rate $R = (1 - \mu)(1 - \lambda)$ is asymptotically achievable.*

Proof. If there exists such an asymptotically-achievable code, we can substitute this code for \mathcal{C}_x and \mathcal{C} in the above construction, where the parameters are $(n, x, M_1, x - k + \tau_2)$ and (x, k, M_2, τ_1) , respectively.

The rate pair is:

$$\begin{aligned} \frac{\log_q |\mathcal{M}_2|}{nk} &\geq \frac{xk(1 - \mu_k)(1 - \lambda_k)}{nk} - \epsilon \\ &= (1 - \mu_1)(\lambda_x - \lambda) - \epsilon, \end{aligned} \tag{29}$$

$$\begin{aligned} \frac{\log_q |\mathcal{M}_1|}{nk} &\geq \frac{nx(1 - \mu_x)(1 - \lambda_x)}{nk} - \epsilon \\ &= (1 - \mu_2)(1 - \lambda_x) - \epsilon, \end{aligned} \tag{30}$$

where $\mu_k = \tau_1/k, \mu_x = \frac{x-k+\tau_2}{x}, \lambda_k = k/x, \mu_1 = \tau_1/k, \mu_2 = \tau_2/k, \lambda = k/n, \lambda_x = x/n$ and $\epsilon > 0$.

That is, the rate pair (R_1, R_2) :

$$R_1 = (1 - \mu_1)(\lambda_x - \lambda), \tag{31}$$

$$R_2 = (1 - \mu_2)(1 - \lambda_x), \tag{32}$$

is asymptotically achievable. \square

Fortunately, K-K codes satisfy the requirement in Proposition 1. From the minimum distance decoder requirements in Condition (4), we can rewrite Equation (2) in the form of deletion-correcting capability τ ,

$$R \leq (1 - \mu)(1 - \lambda) + o(1), \tag{33}$$

where $\mu = \tau/k$ is normalized deletion-correcting capability.

The achievability of outer bound can be obtained subsequently.

Theorem 3. (Achievability) *If for a rate pair (R_1, R_2) of nonnegative numbers, there exists an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC, $\mathcal{C} \subset \mathcal{P}_q(n, k)$, such that the following inequalities hold,*

$$R_1 \geq 0, R_2 \geq 0 \tag{34}$$

$$R_1 \leq (1 - \mu_1)(\lambda_x - \lambda), \tag{35}$$

$$R_2 \leq (1 - \mu_2)(1 - \lambda_x), \tag{36}$$

where x is an auxiliary variable, such that $k \leq x \leq n$. The normalized weights are $\lambda_x = x/n, \lambda = k/n$, and the normalized deletion-correcting capabilities are $\mu_1 = \tau_1/k, \mu_2 = \tau_2/k$. Then, (R_1, R_2) is an achievable rate pair for the $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC.

Proof. The theorem can be proven by specifying the K-K codes to our construction. \square

5. Exactly Attained Codes

So far, the asymptotically-achievable rate region of BECNC is obtained by using K-K codes in our construction. However, the K-K codes achieve the Singleton-type bound in Equation (33) asymptotically, which requires the dimension of ground space n sufficiently large. In this section, we study the case when our outer bound can be attained exactly.

Proposition 2. *For an $[n, k, (M_1, M_2), (\tau_1, \tau_2)]$ -BECNC, our outer bound could be achieved at (M_1, M_2) , if there exists an (n, k, M, τ) -code for single-user communication, such that:*

$$M = \frac{\begin{bmatrix} n \\ k - \tau \end{bmatrix}}{\begin{bmatrix} k \\ k - \tau \end{bmatrix}}. \tag{37}$$

The proof of this proposition will be given later.

The q -analog Steiner structure [19] could be used in the construction that was presented in Section 4.3, which does not require the size of n . We will state it in detail in the following.

A collection $\mathbb{S} \subseteq \mathcal{P}_q(n, k)$ is called a q -analog Steiner structure $\mathbb{S}[t, k, n]_q$ if the elements of \mathbb{S} are k -dimensional subspaces (called blocks), and each element from $\mathcal{P}_q(n, t)$ is contained in exactly one block from \mathbb{S} . $\mathbb{S}[t, n, n]_q$ and $\mathbb{S}[t, t, n]_q$ exist, but these are trivial. Until recently, the only known nontrivial Steiner structures $\mathbb{S}[1, k, n]_q$ exist when k divides n . The problem of the existence of a Steiner structure with various parameters is still open. We do not concentrate on the existence of the q -analog Steiner structure in this paper. The constructions and properties of the q -analog Steiner structure are further discussed in [20].

We assume that there exists a q -Steiner structure $\mathbb{S}[t, k, n]_q$. This structure could be considered as a k -dimensional subspace code \mathcal{C} over \mathbb{F}_q^n with deletion-correcting capability $\tau = k - t$, where each block of $\mathbb{S}[t, k, n]_q$ is a codeword of \mathcal{C} . Since a codeword V produces a random $(k - \tau)$ -dimensional subspace of V by the operation \mathcal{D}_τ , the definition of the q -Steiner structure guarantees that each $(k - \tau)$ -dimensional subspace corresponds to exactly one k -dimensional subspace in \mathcal{C} , *i.e.*, every $(k - \tau)$ -dimensional subspace can be correctly decoded into a transmitted subspace. The number of codewords of a q -Steiner structure $\mathbb{S}[t, k, n]_q$ is given by the number of blocks in \mathbb{S} .

Lemma 5 ([19]). *The total number of blocks in an $\mathbb{S}[t, k, n]_q$ is:*

$$\frac{\begin{bmatrix} n \\ t \end{bmatrix}}{\begin{bmatrix} k \\ t \end{bmatrix}}.$$

Then, the q -Steiner structure $\mathbb{S}[k - \tau, k, n]_q$ could be regarded as an (n, k, M, τ) -code, which satisfies Condition (37). Since the size of the codewords is:

$$M = |\mathbb{S}[k - \tau, k, n]_q| = \frac{\begin{bmatrix} n \\ k - \tau \end{bmatrix}}{\begin{bmatrix} k \\ k - \tau \end{bmatrix}}. \tag{38}$$

Proof of Proposition 2. Similar to the proof of Proposition 1. We could substitute the q -Steiner structure $\mathbb{S}[k - \tau_2, x, n]_q$ and $\mathbb{S}[k - \tau_1, k, x]_q$ for \mathcal{C}_x and \mathcal{C} in the construction in Section 4.3, respectively. The numbers of codewords are:

$$M_2 = |\mathbb{S}[k - \tau_1, k, x]_q| = \frac{\begin{bmatrix} x \\ k - \tau_1 \end{bmatrix}}{\begin{bmatrix} k \\ k - \tau_1 \end{bmatrix}}, \tag{39}$$

$$M_1 = |\mathbb{S}[k - \tau_2, x, n]_q| = \frac{\begin{bmatrix} n \\ k - \tau_2 \end{bmatrix}}{\begin{bmatrix} x \\ k - \tau_2 \end{bmatrix}}, \tag{40}$$

which coincide with Equations (13) and (14) when the equalities hold. That is, the rate pair (M_1, M_2) in Theorem 2 is exactly attained.

Note that, because of the number of the known q -Steiner structure is very limited, the exactly attained codes of BECNC cannot achieve all of the points in the rate region of Theorem 1. It will be of interest to study the existence of the q -Steiner structure.

6. Extension

In this section, we will extend the asymptotically-achievable rate region to more than two receivers. Consider the model depicted in Section 2.2; we can obtain the asymptotically-achievable rate region of the m -tuple coding rates (R_1, R_2, \dots, R_m) .

Theorem 4. *The asymptotically-achievable rate region of an $[n, k, (M_1, M_2, \dots, M_m), (\tau_1, \tau_2, \dots, \tau_m)]$ -BECNC with corresponding error correcting-capabilities $\tau_1, \tau_2, \dots, \tau_m$ over field \mathbb{F}_q consists of rates (R_1, R_2, \dots, R_m) of non-negative numbers that satisfy the inequalities,*

$$R_1 \geq 0, R_2 \geq 0, \dots, R_m \geq 0 \quad (41)$$

$$R_1 \leq (1 - \mu_1)(\lambda_1 - \lambda), \quad (42)$$

$$R_2 \leq (1 - \mu_2)(\lambda_2 - \lambda_1), \quad (43)$$

$$\dots \quad (44)$$

$$R_m \leq (1 - \mu_m)(1 - \lambda_{m-1}), \quad (45)$$

where x_1, \dots, x_{m-1} are auxiliary variables, such that $k \leq x_1 \leq \dots \leq x_{m-1} \leq n$. The normalized weights are $\lambda_i = x_i/n, \lambda = k/n, i = 1, \dots, m-1$, and the normalized error-correcting capabilities are $\mu_i = \tau_i/k, i = 1, \dots, m$.

The proof can refer to the steps from the proofs of Theorem 1, where we leave it for the readers as an exercise.

7. Conclusion

In this paper, we propose a network model based on a real-time media distribution system, where the receivers have different link capacities due to packets lost or a fault in intermediate nodes. To solve the transmission problem in our model, we provide the broadcast error-correcting network codes (BECNC), which are based on subspace metric codes. Then, we present the asymptotically-achievable rate region for BECNC. In the proof part, we show the outer bound of the achievable rate region, followed by a code construction. We prove that the outer bound is asymptotically achieved by specifying K-K codes in our construction. Meanwhile, the outer bound is exactly attained by using the q -analog Steiner structure in our construction. Since the number of the known q -analog Steiner structure is limited, the outer bound can be attained exactly in some points. The research on the existence and construction of q -analog Steiner structures may be interesting. Although K-K codes require the dimension of ground space n sufficiently large and the known q -analog Steiner structure is limited, the theoretical rate region given in this paper has certain practical significance. In the future, if we could find the “good” codes, this outer bound could be attained exactly at all points.

Acknowledgments

The authors thank Harout Aydinian for pointing out the existence of [16] and sending its copy. The authors are grateful for the financial support by the National Natural Science Foundation of China (Nos. 61271174 and 61301178) and Huawei Technologies Co., Ltd, China.

Author Contributions

Feng Cai performed the research with the theoretical proof and wrote the manuscript. Ning Cai guided the research and provided the idea for proving the outer bound of the asymptotically-achievable rate region. Wangmei Guo made a critical contribution to revising the manuscript, including the English correction. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

A. Appendix

A.1. Proof of Lemma 4

We prove by induction on l . Let $Y^{(l)}$ be a $y^{(l)}$ -dimensional subspace in the proof of the l -th level shadow.

From Lemma 3, we know the lemma holds in the case of $l = 1$.

We assume that the lemma holds when $l = s$, then we can get that $|\partial^{(s)}\mathcal{F}| \geq \begin{bmatrix} y^{(s)} \\ k - s \end{bmatrix}$ by assumption.

Next, we consider the case of $l = s + 1$. Let $\partial^{(s)}\mathcal{F} \subset \begin{bmatrix} W \\ k - s \end{bmatrix}$ and let $y^{(s+1)} \geq k - s$ be the positive integer represented by $|\partial^{(s)}\mathcal{F}| = \begin{bmatrix} y^{(s+1)} \\ k - s \end{bmatrix}$. By the assumption when $l = s$, we can get that $y^{(s+1)} \geq y^{(s)}$, then $|\partial^{(s)}\mathcal{F}| = \begin{bmatrix} y^{(s+1)} \\ k - s \end{bmatrix}$ is well defined since Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ is monotone increasing with n . By Lemma 3, the size of the shadow of $\partial^{(s)}\mathcal{F}$ satisfies that $|\partial^{(s+1)}\mathcal{F}| \geq \begin{bmatrix} y^{(s+1)} \\ (k - s) - 1 \end{bmatrix} = \begin{bmatrix} y^{(s+1)} \\ k - (s + 1) \end{bmatrix}$.

We now focus on the equality. Again the proof proceeds by induction on l .

In case of $l = 1$, from Lemma 3, if the equality holds, then $y^{(1)} \in \mathbb{Z}^+$ and $\mathcal{F} = \begin{bmatrix} Y^{(1)} \\ k \end{bmatrix}$, where $Y^{(1)}$ is a $y^{(1)}$ -dimensional subspace of W .

We assume that the equality holds when $l = s$, then we can get that

$$|\partial^{(s)}\mathcal{F}| = \begin{bmatrix} y^{(s)} \\ k - s \end{bmatrix}, \tag{46}$$

then $y^{(s)} \in \mathbb{Z}^+$ and $\mathcal{F} = \begin{bmatrix} Y^{(s)} \\ k \end{bmatrix}$, where $Y^{(s)}$ is a $y^{(s)}$ -dimensional subspace of W .

In the case of $l = s + 1$, from Lemma 3, if equality holds, $|\partial\partial^{(s)}\mathcal{F}| = |\partial^{(s+1)}\mathcal{F}| = \begin{bmatrix} y^{(s+1)} \\ k - s - 1 \end{bmatrix}$, then $y^{(s+1)} \in \mathbb{Z}^+$ and $\partial^{(s)}\mathcal{F} = \begin{bmatrix} Y^{(s+1)} \\ k - s \end{bmatrix}$, where $Y^{(s+1)}$ is a $y^{(s+1)}$ -dimensional subspace of W . We know that $\partial^{(s)}\mathcal{F}$ is consisted of all $(k - s)$ -dimensional subspaces of $Y^{(s+1)}$, and $|\partial^{(s)}\mathcal{F}| = \begin{bmatrix} y^{(s+1)} \\ k - s \end{bmatrix}$. Comparing with Equation (46), we get $\begin{bmatrix} y^{(s)} \\ k - s \end{bmatrix} = \begin{bmatrix} y^{(s+1)} \\ k - s \end{bmatrix}$, hence $y^{(s)} = y^{(s+1)}$. By induction, $y^{(1)} = \dots = y^{(s)} = y^{(s+1)} = \dots = y$ is constant.

This completes the proof.

A.2. Proof of Corollary 1

Let $|\mathcal{F}| = \begin{bmatrix} x \\ k \end{bmatrix}$, $x \leq y$. Then by Lemma 4, $|\partial^{(l)}\mathcal{F}| \geq \begin{bmatrix} x \\ k - l \end{bmatrix} = \frac{\begin{bmatrix} x \\ k - l \end{bmatrix}}{\begin{bmatrix} x \\ k \end{bmatrix}} |\mathcal{F}| \geq \frac{\begin{bmatrix} y \\ k - l \end{bmatrix}}{\begin{bmatrix} y \\ k \end{bmatrix}} |\mathcal{F}|$, since

$$\frac{\begin{bmatrix} x \\ k - l \end{bmatrix}}{\begin{bmatrix} x \\ k \end{bmatrix}} = \frac{(q^k - 1)(q^{k-1} - 1) \dots (q^{k-l+1} - 1)}{(q^{x-(k-l)} - 1)(q^{x-(k-l)-1} - 1) \dots (q^{x-k+1} - 1)}$$

is a decreasing function of x .

References

1. Ahlswede, R.; Cai, N.; Li, S.-Y.R.; Yeung, R.W. Network information flow. *IEEE Trans. Inf. Theory* **2000**, *46*, 1204–1216.
2. Li, S.-Y.R.; Yeung, R.W.; Cai, N. Linear network coding. *IEEE Trans. Inf. Theory* **2003**, *49*, 371–381.
3. Jaggi, S.; Sanders, P.; Chou, P.A.; Effros, M.; Egner, S.; Jain, K.; Tolhuizen, L.M.G.M. Polynomial time algorithms for multicast network code construction. *IEEE Trans. Inf. Theory* **2005**, *51*, 1973–1982.
4. Ho, T.; Médard, M.; Koetter, R.; Karger, D.R.; Effros, M.; Shi, J.; Leong, B. A random linear network coding approach to multicast. *IEEE Trans. Inf. Theory* **2006**, *52*, 4413–4430.
5. Yeung, R.W.; Cai, N. Network error correction, I: Basic concepts and upper bounds. *Commun. Inf. Syst.* **2006**, *6*, 19–35.

6. Cai, N.; Yeung, R.W. Network error correction, II: Lower bounds. *Commun. Inf. Syst.* **2006**, *6*, 37–54.
7. Koetter, R.; Kschischang, F.R. Coding for errors and erasures in random network coding. *IEEE Trans. Inf. Theory* **2008**, *54*, 3579–3591.
8. Etzion, T.; Vardy, A. Error-Correcting codes in projective space. *IEEE Trans. Inf. Theory* **2011**, *57*, 1165–1173.
9. Xia, S.-T.; Fu, F.-W. Johnson type bounds on constant dimension codes. *Des. Codes Cryptogr.* **2009**, *50*, 163–172.
10. Gadouleau, M.; Yan, Z. Packing and covering properties of subspace codes for error control in random linear network coding. *IEEE Trans. Inf. Theory* **2010**, *56*, 2097–2108.
11. Chou, P.A.; Wu, Y.; Chou, P.; Jain, K. Practical network coding. In Proceedings of 41st Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, 1–3 October 2003.
12. Wang, M.; Li, B. How Practical is Network Coding? In Proceedings of 14th IEEE International Workshop on Quality of Service, New Haven, CT, USA, 19–21 June 2006; pp. 274–278.
13. Kruskal, J.B. The number of simplices in a complex. In *Mathematical Optimization Techniques*; Bellman, R., Ed.; Birkhäuser: Boston, MA, USA, 1963; p. 251.
14. Katona, G. A theorem of finite sets. In *Classic Papers in Combinatorics*; Birkhäuser: Boston, MA, USA, 1987; pp. 381–401.
15. Lovász, L. *Combinatorial Problems and Exercises*, 2nd ed.; American Mathematical Society: Providence, RI, USA, 1993.
16. Chowdhury, A.; Patkós, B. Shadows and intersections in vector spaces. *J. Combin. Theory Ser. A* **2010**, *117*, 1095–1106.
17. Van Lint, J.H.; Wilson, R.M. *A Course in Combinatorics*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2001.
18. Csiszár, I.; Körner, J. *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2011.
19. Schwartz, M.; Etzion, T. Codes and anticodes in the Grassman graph. *J. Combin. Theory Ser. A* **2002**, *97*, 27–42.
20. Etzion, T.; Vardy, A. On q -Analogues of Steiner systems and covering designs. *Adv. Math. Commun.* **2011**, *5*, 161–176.