On Multicasting Nested Message Sets Over Combination Networks

Shirin Saeedi Bidokhti
EPFL, Switzerland
shirin.saeedi@epfl.ch

Vinod M. Prabhakaran
TIFR, India
vinodmp@tifr.res.in

Suhas. N. Diggavi
U.C. Los Angeles, USA
suhas@ee.ucla.edu

***Abstract*—In this paper, we study delivery of two nested message sets over combination networks with an arbitrary number of receivers, where a subset of receivers (public receivers) demand only the lower priority message and a subset of receivers (private receivers) demand both the lower and the higher priority messages. We give a complete rate region characterization over combination networks with three public and any number of private receivers, where achievability is through linear coding. Our encoding scheme is general and characterizes an achievable region for arbitrary number of public and private receivers[1].**

I. Introduction

The optimal rates with which one message set could be multicast to multiple destinations was established in the original work of Ahlswede *et al*. [1] and it was shown that performing network coding is necessary to achieve the capacity. Later, [2], [3], [4] showed that linear network coding is capacity achieving and [5] demonstrated randomized construction of multicast network codes.

The problem of delivering multiple messages is unresolved in general, though there has been progress on some special cases. In particular, [6], [7], [8] consider graphs with a single source and two destinations and characterize the capacity region for a common and two individual messages sets. In [9], the capacity region of multicasting two nested message sets is derived over combination networks with three destinations.

In this paper, we study optimal encoding schemes for multicasting two nested message sets towards many destinations over a class of networks, known as combination networks.

A combination network is a three-layer single source multi-terminal directed network, first introduced in [10] by Ngai and Yeung (See Figure 1). The class of combination networks turn out to be a rich class of networks in that they capture many of the inherent difficulties of general networks, while being simple enough to explore new coding schemes. Furthermore, they are among the simplest models for broadcast channels, where the media sharing is modeled via the common resources.

In this paper, we study delivery of two nested messages, the lower priority destined to all receivers and the higher priority destined to a subset of receivers.

[1]This work was supported in part by ERC Grant NOWIRE ERC-2009-StG-240317. Vinod M. Prabhakaran was partially supported by a Ramanujan Fellowship from the Department of Science and Technology, Government of India. Suhas Diggavi was partially supported by NSF-CPS award 1136174.

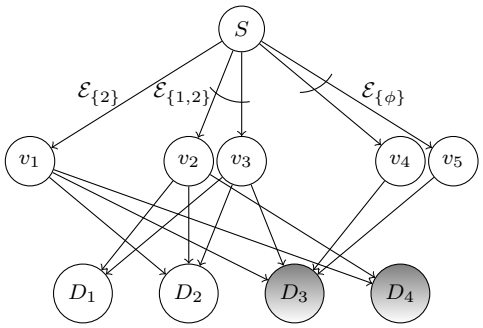

Fig. 1: A combination network with two public and two private receivers (indexed by $I_1 = \{1, 2\}$ and $I_2 = \{3, 4\}$, respectively).

II. Problem Formulation and Main Results

A source communicates a common message W_1 of rate R_1 and a private message W_2 of rate R_2 towards K destinations over a combination network and the the goal is that m (public) receivers indexed by $I_1 = \{1, 2, \ldots, m\}$ recover the common message and the rest $k - m$ (private) receivers indexed by $I_2 = \{m+1, \ldots, k\}$ recover both messages. The network over which communication takes place is a general combination network as depicted in Figure 1. All edges of the combination network are assumed to be carrying symbols from a finite field $\mathbb{F}$. The problem of interest is characterizing the ultimate rates (R_1, R_2) at which messages W_1, W_2 could be communicated reliably. We express all rates in terms of $\log_2 |\mathbb{F}|$.

Throughout this paper, we refer to the outgoing edges of the source as the *resources* of the combination network and we denote them by a set $\mathcal{E}$. We denote the set of all resources that are connected to every public receiver in $S \subseteq I_1$ and not connected to any public receiver not in S by $\mathcal{E}_S \subseteq \mathcal{E}$. Note that edges of set $\mathcal{E}_S$ may or may not be connected to the private receivers. Whenever needed, however, we identify the subset of edges in $\mathcal{E}_S$ that are also connected to a private receiver p, by $\mathcal{E}_S^p$. Figure 1 shows this notation over a combination network with two public and two private receivers. In this example, $\mathcal{E}_\phi = \{(S, v_4), (S, v_5)\}$, $\mathcal{E}_{\{1\}} = \{\}$, $\mathcal{E}_{\{2\}} = \{(S, v_1)\}$, and $\mathcal{E}_{\{1,2\}} = \{(S, v_2), (S, v_3)\}$. Also, we have $\mathcal{E}^3_{\{2\}} = \mathcal{E}^4_{\{2\}} = \{(S, v_1)\}$, $\mathcal{E}^3_{\{1,2\}} = \{(S, v_3)\}$, $\mathcal{E}^4_{\{2\}} = \{(S, v_2)\}$, $\mathcal{E}^3_\phi = \{(S, v_4), (S, v_5)\}$, and $\mathcal{E}^4_\phi = \{\}$.

To communicate messages W_1, W_2, each edge of the network carries symbols containing information about messages

W_1 and/or W_2. We denote the symbol carried over a resource edge e by x_e, which is a scalar from finite field $\mathbb{F}$. We denote by X_S, where $S \subseteq I_1$, the set of all symbols carried over edges in $\mathcal{E}_S$, and by X_S^p, where $S \subseteq I_1$ and $p \in I_2$, the set of all symbols carried over edges in $\mathcal{E}_S^p$. To simplify notation, we abbreviate the union sets $\bigcup_{S\in\mathcal{S}} \mathcal{E}_S$, $\bigcup_{S\in\mathcal{S}} \mathcal{E}_S^p$ and $\bigcup_{S\in\mathcal{S}} X_S$, by $\mathcal{E}_\mathcal{S}$, $\mathcal{E}_\mathcal{S}^p$ and $X_\mathcal{S}$, respectively. The vector of all received symbols at receiver i is denoted by Y_i. Finally, when working with transmission blocks of length n, we use $\bar{X}$ to denote the vector of symbols over the block of length n.

We define superset saturated subsets of 2^{I_1} as follows.

Definition 1 (Superset saturated)**.** *We say that subset $\mathcal{T} \subseteq 2^{I_1}$ is superset saturated if inclusion of a set S in $\mathcal{T}$ implies inclusion of all its supersets; e.g., over subsets of $2^{\{1,2,3\}}$, $\mathcal{T} = \{\{1\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$ is superset saturated, but not $\mathcal{T} = \{\{1\},\{1,3\},\{1,2,3\}\}$. For notational matters, we abbreviate a subset $\mathcal{T}$ by the few sets that are not implied by the other sets in $\mathcal{T}$. E.g., $\{\{1\},\{1,2\},\{1,3\},\{1,2,3\}\}$ is abbreviated by $\{\{1\}\star\}$, and $\{\{1\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$ is abbreviated by $\{\{1\}\star,\{2,3\}\star\}$.*

Our main result is summarized in the following theorem.

Theorem 1. *Consider a combination network with three public receivers (indexed by $I_1 = \{1,2,3\}$) and any number of private receivers (indexed by $I_2 = \{4,\dots,K\}$). The capacity region is characterized by all rate pairs (R_1, R_2) for which there exist real-valued variables α_S, $S \subseteq I_1$, such that*

$$\alpha_S \geq 0 \qquad \forall S\subseteq I_1,\ S\neq\phi \tag{1}$$

$$R_2 = \sum_{S\subseteq I_1} \alpha_S \tag{2}$$

$$R_1 + \sum_{S\subseteq I_1,\ S\ni i} \alpha_S \leq \sum_{S\subseteq I_1,\ S\ni i} |\mathcal{E}_S| \qquad \forall i\in I_1 \tag{3}$$

$$R_2 \leq \sum_{S\in\mathcal{T}} \alpha_S + \sum_{S\in\mathcal{T}^c} |\mathcal{E}_S^p| \qquad \substack{\forall \mathcal{T}\subseteq 2^{I_1},\ \forall p\in I_2 \\ \mathcal{T} \text{ superset saturated}} \tag{4}$$

$$R_1 + R_2 \leq \sum_{S\subseteq I_1} |\mathcal{E}_S^p| \qquad \forall p\in I_2 \tag{5}$$

We prove Theorem 1 by proposing an achievable scheme and proving a matching outer-bound. The primary difficulty in achievable code designs is how to resolve the tension between delivering the common message to the public receivers while delivering the common and private messages to the private receivers. In particular, in order for the public receivers to decode the common message, one should not provide them with too much information about the private message. One standard approach to resolve this issue is to use linear superposition coding and to reveal to public receivers partial message sets of the private message. We show in Section III that this scheme is not in general optimal. We enhance this scheme using an appropriate pre-encoder, to obtain a general inner-bound to the capacity region in Theorem 2. We prove optimality of our encoding scheme for cases with three (or fewer) public and any number of private receivers in Section IV.

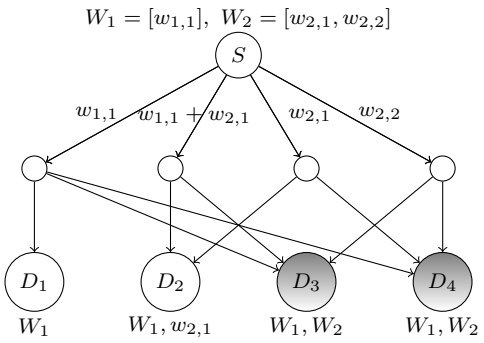

Fig. 2: To achieve rate pair $(1,2)$, the source needs to reveal partial private information to public receiver 2.

III. Achievable Schemes: Rate Splitting and Linear Encoding

Throughout this section, we confine ourselves to linear encoding at the source. For simplicity of notation, we demonstrate all the proofs in this section assuming that there are two public receivers, but our focus is on three and more public receivers. Let $w_{1,1},\dots,w_{1,R_1}$ and $w_{2,1},\dots,w_{2,R_2}$ be variables in finite field $\mathbb{F}$ for messages W_1 and W_2 respectively. We call them the information symbols of the common and the private message, respectively. Consider vector $W \in \mathbb{F}^{R_1+R_2}$ as the vector with coordinates in the standard basis $W = [w_{1,1}\dots w_{1,R_2} w_{2,1}\dots w_{2,R_2}]^T$. Within this section, we assume rates R_1 and R_2 to be non-negative integer values[2].

We use linear encoding at the source; i.e., after properly rearranging the signals that are sent over the resources of the combination network, we have

$$\begin{bmatrix} X_{\{1,2\}} \\ X_{\{2\}} \\ X_{\{1\}} \\ X_\phi \end{bmatrix} = \mathbf{A}\cdot W,$$

where $\mathbf{A}$ is the encoding matrix. Our task is to design the encoding matrix $\mathbf{A}$ such that each receiver can decode its messages of interest after receiving its incoming signals.

The challenge in the code design for this problem comes from the tension between the two different demands of receivers: On the one hand, each private receiver would like its available resources to bring information about all information symbols of the common and private messages. On the other hand, public receivers might not be able to decode the common message if their received signals contain too much information about the private message. This could be better seen through the example of Figure 2, where the source communicates a common message $W_1 = [w_{1,1}]$ and a private message $W_2 = [w_{2,1}, w_{2,2}]$ to four receivers. Receivers 1 and 2 are public receivers and receivers 3 and 4 are private receivers. In this example, one can easily verify that (i) randomly linearly

[2]There is no loss of generality in this assumption. One can deal with non-integer values R_1, R_2, by considering blocks of large enough length n, and working with (approximately) integer rates nR_1 and nR_2.

combining all information symbols and sending them out on the resources of the combination network allows neither of the public receivers decode their message of interest, and (ii) combining the information symbols across the two message sets is necessary to achieve rate pair $(1, 2)$. More precisely, rate pair $(1, 2)$ is feasible only if signal $X_{\{2\}}$ carries information about one symbol of message W_2 (or one linear combination out of the message space of W_2), in addition to common message W_1. In general, we would like the encoding scheme to allow mixing of the common message with a partial message space of the private message.

We start by a linear superposition encoding scheme, to which we refer as the *basic encoding scheme*. This code design is such that different information symbols of the private message get involved in linear combinations that are sent out towards different subsets of the public receivers. More precisely, we propose the encoding matrix $\mathbf{A}$ to have the following structure, where the un-assigned entries are to be chosen appropriately over the finite field $\mathbb{F}$.

$$\mathbf{A} = \begin{array}{c} \overset{R_1}{\longleftrightarrow}\ \overset{\alpha_{\{1,2\}}}{\longleftrightarrow}\overset{\alpha_{\{1\}}}{\leftrightarrow}\overset{\alpha_{\{2\}}}{\leftrightarrow}\overset{\alpha_\phi}{\leftrightarrow} \\ \left[\begin{array}{c|c|ccc} & & 0 & 0 & 0 \\ \hline & & & 0 & 0 \\ \hline & & 0 & & 0 \\ \hline & & & & \end{array}\right] \begin{array}{l} \updownarrow |\mathcal{E}_{\{1,2\}}| \\ \updownarrow |\mathcal{E}_{\{1\}}| \\ \updownarrow |\mathcal{E}_{\{2\}}| \\ \updownarrow |\mathcal{E}_{\phi}| \end{array} \end{array} . \tag{6}$$

In the above structure, parameters $\alpha_{\{1,2\}}, \alpha_{\{1\}}, \alpha_{\{2\}}, \alpha_\phi$ are non-negative structural parameters to be designed, and satisfy[3]

$$\sum_{S \subseteq I_1} \alpha_S = R_2. \tag{7}$$

Let us pick the un-assigned elements of matrix $\mathbf{A}$ uniformly at random over finite field $\mathbb{F}$. We now examine the received signals at each receiver and find constraints on parameters α which allow all receivers to recover their messages of interest.

- **Public receiver $i \in I_1$:** Received signal Y_i is the vector of all signals carried by resources available to receiver i. Using the (structured) encoding matrix of equation (6), received signal Y_i is given as follows.

$$Y_i = \underbrace{\begin{array}{c} \overset{R_1}{\longleftrightarrow}\ \overset{\alpha_{\{1,2\}}}{\longleftrightarrow}\overset{\alpha_{\{1\}}}{\leftrightarrow}\overset{\alpha_{\{2\}}}{\leftrightarrow}\overset{\alpha_\phi}{\leftrightarrow} \\ \left[\begin{array}{c|c|ccc} & & 0 & 0 & 0 \\ \hline & & & 0 & 0 \end{array}\right] \begin{array}{l} \updownarrow |\mathcal{E}_{\{1,2\}}| \\ \updownarrow |\mathcal{E}_{\{i\}}| \end{array} \end{array}}_{\mathbf{A}_i} \begin{bmatrix} W_1 \\ W_2 \end{bmatrix}$$

  To have message W_1 decodable, the first R_1 columns of $\mathbf{A}_i$ need to be linearly independent and they need to span a space which is disjoint from the column space of the rest of the columns [11, Lemma 4.2]. Lemma 1 translates this to conditions on parameters α_S.

  Lemma 1. *A random structured encoding matrix $\mathbf{A}$ lets receiver $i \in I_1$ decode its message of interest W_1 (with a probability at least $1 - \frac{1}{|\mathbb{F}|}$), if we have*

$$R_1 + \sum_{S \subseteq I_1,\ S \ni i} \alpha_S \leq \sum_{S \subseteq I_1,\ S \ni i} |\mathcal{E}_S|. \tag{8}$$

[3]Although parameters α_S are implicitly assumed integer, one can let them be real and approximately attain them by coding over blocks of larger length.

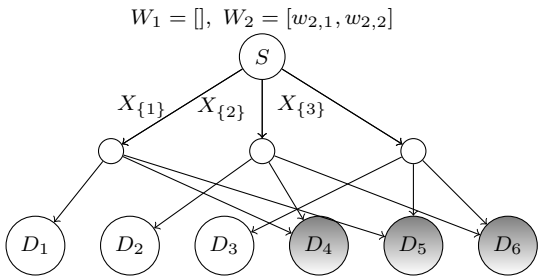

Fig. 3: Rate pair $(0, 2)$ is not achievable using the basic encoding scheme.

- **Private receivers $p \in I_2$:** Received signal Y_p is the vector of all signals carried by resources in the sets $\mathcal{E}^p_S$, $S \subseteq I_1$. Using the (structured) encoding matrix (6), received signal Y_p is given as follows.

$$Y_p = \underbrace{\begin{array}{c} \overset{R_1}{\longleftrightarrow}\ \overset{\alpha_{\{1,2\}}}{\longleftrightarrow}\overset{\alpha_{\{1\}}}{\leftrightarrow}\overset{\alpha_{\{2\}}}{\leftrightarrow}\overset{\alpha_\phi}{\leftrightarrow} \\ \left[\begin{array}{c|c|ccc} & & 0 & 0 & 0 \\ \hline & & & 0 & 0 \\ \hline & & 0 & & 0 \\ \hline & & & & \end{array}\right] \begin{array}{l} \updownarrow |\mathcal{E}^p_{\{1,2\}}| \\ \updownarrow |\mathcal{E}^p_{\{1\}}| \\ \updownarrow |\mathcal{E}^p_{\{2\}}| \\ \updownarrow |\mathcal{E}^p_{\phi}| \end{array} \end{array}}_{\mathbf{A}_p} \begin{bmatrix} W_1 \\ W_2 \end{bmatrix}$$

  One can partially extend Lemma 4.5 of [11] to find constraints on decodability of W_1, W_2 at private receiver p. We refer the reader to [12] for the proof.

  Lemma 2. *A random structured encoding matrix $\mathbf{A}$ lets receiver $p \in I_2$ decode its messages of interest W_1, W_2 (with a probability at least $1 - \frac{1}{|\mathbb{F}|}$), if we have*

$$R_2 \leq \sum_{S \in \mathcal{T}} \alpha_S + \sum_{S \in \mathcal{T}^c} |\mathcal{E}^p_S|, \qquad \overset{\forall \mathcal{T} \subseteq 2^{I_1}}{\underset{\text{superset saturated}}{}} \tag{9}$$

$$R_1 + R_2 \leq \sum_{S \in 2^{I_1}} |\mathcal{E}^p_S|. \tag{10}$$

To summarize, Lemma 1 and Lemma 2 provide constraints on the structural parameters α_S, $S \subseteq I_1$, under which a random choice of matrix $\mathbf{A}$ satisfies all decodability requirements with a probability at least $1 - \frac{K}{\mathbb{F}}$. Therefore, there exists an assignment of the encoding matrix $\mathbf{A}$ for which all receivers decode their messages of interest, provided that $\mathbb{F} > K$. Note that operation over a smaller field is also possible, by coding over blocks of large lengths.

It turns out that in general, the above basic encoding scheme performs optimally only when there are (at most) two public and any number of private receivers. Example 1 discusses this sub-optimality for more than two public receivers.

Example 1. *Consider the combination network of Figure 3 where receivers 1, 2, 3 are public and receivers 4, 5, 6 are private receivers. It is clear that rate pair $(0, 2)$ is achievable (just multicast the private message towards the private receivers using random linear network coding). However, there is no choice of $\alpha_S \geq 0$, $S \subseteq \{1, 2, 3\}$, which satisfies inequalities (7)-(10) for this rate pair, unless α_ϕ*

is allowed to be negative. One such set of parameters α_S is given by $\alpha_\phi = -1$, $\alpha_{\{1\}} = \alpha_{\{2\}} = \alpha_{\{3\}} = 1$, and $\alpha_{\{1,2\}} = \alpha_{\{1,3\}} = \alpha_{\{2,3\}} = \alpha_{\{1,2,3\}} = 0$.

Obviously, there is no longer a "structural" meaning to this negative parameter. Nonetheless, it still has a peculiar meaning that we try to investigate in this example. As suggested by the positive parameters $\alpha_{\{1\}}$, $\alpha_{\{2\}}$, $\alpha_{\{3\}}$, we would like to reveal a subspace of dimension one (of the private message space) to each public receiver. The subtlety comes in when one notices that such partial (private) information that is revealed to the public receiver subsets $\{1\}$, $\{2\}$ and $\{3\}$ cannot be mutually independent, as message W_2 is of rate only 2.

We use this observation to modify the encoding scheme and achieve rate pair $(0, 2)$. First, pre-encode message W_2 through a random pre-encoding matrix $\mathbf{P} \in \mathbb{F}^{3\times 2}$, into a pseudo private message W_2'. Then, encode W_2' using a structured encoding matrix, as follows.

$$\begin{bmatrix} X_{\{1\}} \\ X_{\{2\}} \\ X_{\{3\}} \end{bmatrix} = \left[\begin{array}{c|c|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right] \begin{bmatrix} w'_{2,1} \\ w'_{2,2} \\ w'_{2,3} \end{bmatrix}$$

Notice that this structured encoding matrix does reveal a subspace of dimension one (of the pseudo-private message space) to each public receiver. Furthermore, using such a pre-encoding/encoding scheme, each private receiver gets to decode two symbols out of the three symbols of W_2' and can, therefore, decode the (original) private message W_2 (w.h.p.).

Inspired by example 1, we modify the basic encoding scheme, using an appropriate pre-encoder, to obtain a strictly larger achievable region as expressed in Theorem 2.

Theorem 2. *Consider a combination network with any number of public and private receivers (indexed by I_1 and I_2, respectively). A rate pair (R_1, R_2) is achievable if there exist real-valued variables α_S, $S \subseteq I_1$, that satisfy* (1)-(5)*.*

Sketch of the proof: Let (R_1, R_2) be in the rate region of Theorem 2; i.e., there exist parameters α_S, $S \subseteq I_1$, that satisfy inequalities (1)-(5). Since we already know what to do if $\alpha \geq 0$, in this proof we assume $\alpha_\phi < 0$, and propose an achievable scheme for that. In the following we assume $(\alpha_\phi)^- = \min(0, \alpha_\phi)$ and $(\alpha_\phi)^+ = \max(0, \alpha_\phi)$.

First of all, pre-encode message W_2 into a message vector W_2' of dimension $R_2 - (\alpha_\phi)^-$, through a pre-encoding matrix $\mathbf{P}$. Then, encode messages W_1 and W_2' into the symbols that are sent out, using a matrix $\mathbf{A}$ structured as in (6) with parameters α_S, $\phi \neq S \subseteq I_1$, and with no column corresponding to $\alpha_\phi < 0$.

Choose the elements of matrix $\mathbf{P}$ and the un-assigned elements of matrix $\mathbf{A}$ uniformly at random over finite field $\mathbb{F}$. We now find the decodability requirements of the public and private receivers. Conditions for decodability of W_1 at the public receivers are given in (3) as before. Conditions for decodability of W_1, W_2 at the private receivers are found in a manner similar to Lemma 2. This is summarized in Lemma 3 (stated below) and we refer the reader to [12] for its proof.

Lemma 3. *A random choice of matrices $\mathbf{P}$ and $\mathbf{A}$ lets private receiver $p \in I_2$ decode messages W_1, W_2 (with a probability at least $1 - \frac{1}{|\mathbb{F}|}$), if inequalities* (4)-(5) *hold.*

So by choosing parameters α_S such that they satisfy constraints in (1)-(5), we ensure that a random choice for matrices $\mathbf{P}$ and $\mathbf{A}$ satisfies all the decodability requirements at all receivers with a probability at least $1 - \frac{K}{|\mathbb{F}|}$. This proves that for any rate pair (R_1, R_2) in Theorem 2, there exists an achievable linear encoding scheme, if $|\mathbb{F}| > K$. Operation over a smaller field is also possible, by coding over blocks of large lengths. ■

IV. Optimality Results

In this Section, we prove the converse of Theorem 1. To this end, we prove an outer-bound on the rate-region which looks *similar* to the inner-bound of Theorem 1 and then use sub-modularity to show that they coincide. We refer the reader to [12] for the detailed proofs.

Let us first give a more compact representation of the rate-region of Theorem 1, via Lemma 4 which is proved in [12].

Lemma 4. *Consider the rate region characterization of Theorem 1 (where $I_1 = \{1, 2, 3\}$ and $I_2 = \{4, \ldots, K\}$). The constraints given by inequalities* (1)-(2) *in Theorem 1 can be replaced by* (11) *given below, without affecting the rate-region.*

$$\sum_{S\in\mathcal{T}} \alpha_S \geq 0, \quad \forall \mathcal{T} \subseteq 2^I \text{ superset saturated} \tag{11}$$

By Lemma 4, the rate region of Theorem 1 is equivalently given by constraints (11), (3)-(5). Lemma 5, stated below and proved in [12], gives an outer-bound which looks *similar* to the inner-bound.

Lemma 5. *Any achievable rate pair (R_1, R_2) satisfies outer-bound constraints* (12)-(15) *for any given $\epsilon > 0$.*

$$\frac{1}{n}H(\bar{X}_\mathcal{T}|W_1) \geq 0 \quad \forall \mathcal{T}\subseteq 2^{I_1} \text{ superset saturated} \tag{12}$$

$$R_1 + \frac{1}{n}H(\bar{X}_{\{\{i\}\star\}}|W_1) \leq \sum_{S\in\{\{i\}\star\}} |\mathcal{E}_S| + \epsilon \quad \forall i\in I_1 \tag{13}$$

$$R_2 \leq \frac{1}{n}H(\bar{X}_\mathcal{T}|W_1) + \sum_{S\in\mathcal{T}^c} |\mathcal{E}_S^p| + \epsilon \quad \begin{matrix}\forall p\in I_2 \\ \forall \mathcal{T}\subseteq 2^{I_1} \text{ superset saturated}\end{matrix} \tag{14}$$

$$R_1 + R_2 \leq \sum_{S\subseteq I_1} |\mathcal{E}_S^p| + \epsilon \quad \forall p\in I_2 \tag{15}$$

Notice the similarity of inequalities (12), (13), (14), (15) with constraints (11), (3), (4), (5), respectively.

In the rest of this section, we argue that the rate-region characterized in Lemma 5 coincides with the rate-region of Theorem 1. To this end, we need the following definitions over multi-sets of subsets of 2^{I_1}, where $I_1 = \{1, 2, 3\}$.

Definition 2 (Multi-set of saturated pattern)**.** *A multi-set (of subsets of 2^{I_1}) is said to be of (superset) saturated pattern if all its elements are superset saturated. E.g., we have that multi-set $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}, \{\{2, 3\}, \{1, 2, 3\}\}]$ is of saturated pattern, but not $[\{\{2\}, \{1, 2\}, \{1, 2, 3\}\}]$.*

Multi-set $\boldsymbol{\mathcal{Q}}$	Compressed multi-set $\boldsymbol{\mathcal{Q}}'$
$[\dots, \{\{i\}\star\}, \{\{j\}\star\}, \dots]$	$[\dots, \{\{i,j\}\star\}, \{\{i\}\star,\{j\}\star\}, \dots]$
$[\dots, \{\{i\}\star\}, \{\{j,k\}\star\}, \dots]$	$[\dots, \{\{1,2,3\}\}, \{\{i,j\}\star,\{i,k\}\star\}, \dots]$
$[\dots, \{\{i,j\}\star\}, \{\{i,k\}\star\}, \dots]$	$[\dots, \{\{1,2,3\}\star\}, \{\{i,j\}\star,\{i,k\}\star,\{j,k\}\star\}, \dots]$
$[\dots, \{\{i\}\star,\{j\}\star\}, \{\{i\}\star,\{k\}\star\}, \dots]$	$[\dots, \{\{1\}\star,\{2\}\star,\{3\}\star\}, \{\{i\}\star,\{j,k\}\star\}, \dots]$
$[\dots, \{\{i\}\star\}, \{\{j\}\star,\{k\}\star\}, \dots]$	$[\dots, \{\{1\}\star,\{2\}\star,\{3\}\star\}, \{\{i,j\}\star,\{i,k\}\star\}, \dots]$
$[\dots, \{\{i\}\star,\{j\}\star\}, \{\{k\}\star,\{i,j\}\star\}, \dots]$	$[\dots, \{\{1\}\star,\{2\}\star,\{3\}\star\}, \{\{i,j\}\star,\{i,k\}\star,\{j,k\}\star\}, \dots]$

TABLE I: Each row shows the compression of a multi-set $\boldsymbol{\mathcal{Q}}$ to $\boldsymbol{\mathcal{Q}}'$. Here, (i,j,k) is a permutation of $(1,2,3)$.

Definition 3 (Multi-set of standard pattern)**.** *A multi-set (of subsets of 2^{I_1}) is said to be of standard pattern if its elements are all of the form $\{S \subseteq I_1 : S \ni i\}$, for some $i \in I_1$. E.g., $[\{\{1\},\{1,2\},\{1,3\},\{1,2,3\}\},\{\{2\},\{1,2\},\{2,3\},\{1,2,3\}\}]$ is of standard pattern, but not $[\{\{1,2\},\{1,2,3\}\}]$.*

Definition 4 (Balanced multi-sets)**.** *Multi-sets $\boldsymbol{\mathcal{A}}$ and $\boldsymbol{\mathcal{B}}$ are balanced if $\sum_{\mathcal{T}\in\boldsymbol{\mathcal{A}}} \mathbf{1}_{\mathcal{T}\ni S} = \sum_{\mathcal{T}\in\boldsymbol{\mathcal{B}}} \mathbf{1}_{\mathcal{T}\ni S}$, for all sets $S \in 2^{I_1}$.*

The sketch of the converse proof is now as follows. We perform the Fourier-Motzkin elimination over the rate-region representation of Theorem 1 (to eliminate parameters α). This way, we reach to a set of inequalities of the form $m_1R_1 + m_2R_2 \le E$, each obtained by summing potentially multiple copies of constraints (11), (3)-(5) (so that all variables α_S, $S \subseteq I_1$, get eliminated). To show a converse for each such inner-bound inequality, $m_1R_1 + m_2R_2 \le E$, we take copies of the corresponding outer-bound constraints (12)-(15) in Lemma 5 and sum them up to yield the following outer-bound inequality.

$$m_1R_1+m_2R_2+\frac{1}{n}\sum_{\mathcal{T}\in\boldsymbol{\mathcal{A}}} H(\bar{X}_{\mathcal{T}}|W_1) \le E+\frac{1}{n}\sum_{\mathcal{T}\in\boldsymbol{\mathcal{B}}} H(\bar{X}_{\mathcal{T}}|W_1)$$

Here, $\boldsymbol{\mathcal{A}}$ is a multi-set of standard pattern and $\boldsymbol{\mathcal{B}}$ is a multi-set of saturated pattern, both consisting of subsets of 2^{I_1} where $I_1 = \{1,2,3\}$. Notice that $\boldsymbol{\mathcal{A}}$ and $\boldsymbol{\mathcal{B}}$ are balanced because Fourier-Motzkin elimination ensures that all the α_S's are eliminated. Finally, we use sub-modularity of the entropy function to prove that $\sum_{\mathcal{T}\in\boldsymbol{\mathcal{A}}} H(\bar{X}_{\mathcal{T}}|W_1) \ge \sum_{\mathcal{T}\in\boldsymbol{\mathcal{B}}} H(\bar{X}_{\mathcal{T}}|W_1)$ (Lemma 6 stated below) and conclude that the converse inequality, $m_1R_1 + m_2R_2 \le E$, holds.

It remains to prove Lemma 6.

Lemma 6. *Let $\boldsymbol{\mathcal{B}}$ and $\boldsymbol{\mathcal{A}}$ be multi-sets of subsets of $2^{\{1,2,3\}}$, where $\boldsymbol{\mathcal{B}}$ is of saturated pattern and $\boldsymbol{\mathcal{A}}$ is of standard pattern. If $\boldsymbol{\mathcal{B}}$ and $\boldsymbol{\mathcal{A}}$ are balanced, then we have the following inequality.*

$$\sum_{\mathcal{T}\in\boldsymbol{\mathcal{A}}} H(\bar{X}_{\mathcal{T}}|W_1) \ge \sum_{\mathcal{T}\in\boldsymbol{\mathcal{B}}} H(\bar{X}_{\mathcal{T}}|W_1) \tag{16}$$

Sketch of the proof: The proof relies on the sub-modularity of the entropy function. We use the formulation of [13] with a slight change of notation.

Let $[\boldsymbol{\mathcal{M}}]$ be a family of multi-sets of subsets of $2^{\{1,2,3\}}$. Given a multi-set $\boldsymbol{\mathcal{Q}} = \{\mathcal{T}_1,\dots,\mathcal{T}_l\} \in [\boldsymbol{\mathcal{M}}]$, let multi-set $\boldsymbol{\mathcal{Q}}'$ be obtained from $\boldsymbol{\mathcal{Q}}$ by replacing $\mathcal{T}_i$ and $\mathcal{T}_j$ by $\mathcal{T}_i \cap \mathcal{T}_j$ and $\mathcal{T}_i \cup \mathcal{T}_j$ (where neither $\mathcal{T}_i \subseteq \mathcal{T}_j$ nor $\mathcal{T}_j \subseteq \mathcal{T}_i$). Multi-set $\boldsymbol{\mathcal{Q}}'$ is then said to be an *elementary compression* of $\boldsymbol{\mathcal{Q}}$. A sequence of elementary compressions gives a *compression*. Table I gives a list of some non-trivial elementary compressions for multi-sets of subsets of $2^{\{1,2,3\}}$.

Let $\boldsymbol{\mathcal{A}}$ and $\boldsymbol{\mathcal{B}}$ be finite multi-sets of subsets of $2^{\{1,2,3\}}$ such that $\boldsymbol{\mathcal{B}}$ is a compression of $\boldsymbol{\mathcal{A}}$. A simple consequence of the sub-modularity of the entropy function is that $\sum_{\mathcal{T}\in\boldsymbol{\mathcal{A}}} H(\bar{X}_{\boldsymbol{\mathcal{T}}}|W_1) \ge \sum_{\mathcal{T}\in\boldsymbol{\mathcal{B}}} H(\bar{X}_{\mathcal{T}}|W_1)$ [13, Theorem 5].

The core of the proof is, therefore, to show that multi-set $\boldsymbol{\mathcal{B}}$ is a compression of multi-set $\boldsymbol{\mathcal{A}}$, under the stated assumptions. We show this by proving that such a compression exists and is formed by a sequence of many elementary compressions each in the form of one of the elementary compressions in Table I. This implies inequality (16). ∎

Remark 1. *This converse proof does not generalize to $m > 3$ public receivers. More precisely, Lemma 4 and Lemma 6 are valid only for $m \le 3$.*

REFERENCES

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

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

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

[4] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *Information Theory, IEEE Transactions on*, vol. 51, no. 6, pp. 1973 – 1982, june 2005.

[5] T. Ho, R. Koetter, M. Medard, D. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Information Theory, 2003. Proceedings. IEEE International Symposium on*, july 2003, p. 442.

[6] A. Ramamoorthy and R. D. Wesel, "The single source two terminal network with network coding," *CoRR*, vol. abs/0908.2847, 2009.

[7] C. Ngai and R. Yeung, "Multisource network coding with two sinks," in *Communications, Circuits and Systems, 2004. ICCCAS 2004. 2004 International Conference on*, vol. 1, june 2004, pp. 34 – 37 Vol.1.

[8] E. Erez and M. Feder, "Capacity region and network codes for two receivers multicast with private and common data," in *Workshop on Coding, Cryptography and Combinatorics*, 2003.

[9] S. Gheorghiu, S. Saeedi Bidokhti, C. Fragouli, and A. Toledo, "Degraded multicasting with network coding over the combination network," in *IEEE International Symposium on Network Coding*, 2011.

[10] C. K. Ngai and R. Yeung, "Network coding gain of combination networks," in *Information Theory Workshop, 2004. ITW 2004. IEEE*, oct. 2004, pp. 283 – 287.

[11] S. Saeedi Bidokhti, S. Diggavi, C. Fragouli, and V. Prabhakaran, "On degraded two message set broadcasting," in *Information Theory Workshop, 2009. ITW 2009. IEEE*, oct. 2009, pp. 406 –410.

[12] S. Saeedi Bidokhti, V. M. Prabhakaran, and S. Diggavi, "Multicasting nested message sets over combination networks," EPFL, Tech. Rep., 2012. [Online]. Available: http://infoscience.epfl.ch/record/175949

[13] P. Balister and B. Bollobás, "Projections, Entropy and Sumsets," *ArXiv e-prints*, Nov. 2007.