Capacity Results for Multicasting Nested Message Sets over Combination Networks

Shirin Saeedi Bidokhti, Vinod M. Prabhakaran, Suhas N. Diggavi

Abstract

The problem of multicasting two nested message sets is studied over a class of wireline networks known as combination networks. A source multicasts two messages, a common and a private message, to several receivers. A subset of the receivers (called the public receivers) only demand the common message and the rest of the receivers (called the private receivers) demand both the common and the private message. Three encoding schemes are discussed which are based on linear superposition schemes.

The standard linear superposition scheme is shown to be optimal for networks with two public receivers and any number of private receivers. When the number of public receivers increases, however, this scheme stops being optimal. Two improvements are discussed: one using a pre-encoding at the source followed by a linear superposition scheme, and one using a block Markov encoding scheme. The rate-regions that are achieved by the two schemes are characterized in terms of feasibility problems. Both inner-bounds are shown to be the capacity region for networks with three (or fewer) public and any number of private receivers. Although the inner bounds are not comparable in general, it is shown through an example that the region achieved by the block Markov encoding scheme may strictly include the region achieved by the pre-encoding/linear superposition scheme.

The block Markov encoding scheme is further generalized and a new achievable scheme is derived for broadcast channels with two nested message sets. The rate-region that is obtained includes the previously known rate-regions. It remains open whether this inclusion is strict.

Index Terms

Network Coding, Combination Networks, Broadcast Channels, Superposition Coding, Linear Coding, Block Markov Encoding

I. Introduction

The problem of communicating common and individual messages over general networks has been unresolved over the past several decades, even in the two extreme cases of single-hop broadcast channels and multi-hop wireline networks. Nevertheless, several special cases have been studied where the capacity region is fully characterized (see [1] and the references therein, and [2], [3], [4], [5]). These studies have given rise to lower and upper bounds on the optimal rates of communication [6], [7], [8], [9], [10], [11], [12]. More importantly, new encoding and decoding techniques have been developed (e.g., superposition coding [13], [14], Marton's coding [15], [16], [17], network coding [2], [18], [19], joint unique and non-unique decoding [20], [21], [22], [23], etc).

Surprisingly, the problem of broadcasting nested (degraded) message sets has been completely resolved for two users. The problem was introduced and investigated for two-user broadcast channels in [17], where the capacity region was characterized and it was shown that superposition coding was optimal. The problem has also been investigated for wired networks with two users [24], [25], [26] where a scheme consisting of routing and random network coding turns out to be rate-optimal. This might suggest that the nested structure of the messages makes the problem easier in nature. Unfortunately, however, the problem has remained open for networks with more than two receivers and only some special cases are understood [22], [27], [28], [29], [30]. The state of the art is not favourable for wired networks either. Although extensions of the joint routing and network coding scheme in [24] are optimal for special classes of three-receiver networks (e.g., in [31]), they are suboptimal in general depending on the structure of the network [32, Chapter 5], [33]. It was recently shown in [34] that the problem of multicasting two nested message sets over general wired networks is as hard as the general network coding problem.

In this paper, we study nested message set broadcasting over a class of wired networks known as combination networks [35]. These networks also form a resource-based model for broadcast channels and are a special class of linear deterministic broadcast channels that were introduced in [29]. Lying at the intersection of multi-hop wired networks and single-hop broadcast channels, combination networks are an interesting class of networks to build up intuition and understanding, and develop new encoding schemes applicable to both sets of problems. We address the scenario of multicasting two nested message sets (a

S. Saeedi Bidokhti was with the School of Computer and Communication Sciences, Ecole Polytechnique Fédéral de Lausanne. She is now with the Institute for Communications Engineering, Technische Universität München (e-mail: shirin.saeedi@tum.de).

V. Prabhakaran is with the School of Technology and Computer Science, Tata Institute of Fundamental Research (e-mail: vinodmp@tifr.res.in).

S. Diggavi is with the Department of Electrical Engineering, UCLA, USA e-mail: (suhas@ee.ucla.edu).

The work of S. Saeedi Bidokhti was partially supported by the SNSF fellowship no. 146617. The work of Vinod M. Prabhakaran was partially supported by a Ramanujan Fellowship from the Department of Science and Technology, Government of India. The work of S. Diggavi was supported in part by NSF awards 1314937 and 1321120.

The material in this paper was presented in parts at the 2009 IEEE Information Theory Workshop, Taormina, Italy, 2012 IEEE Information Theory Workshop, Lausanne, Switzerland, and the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey.

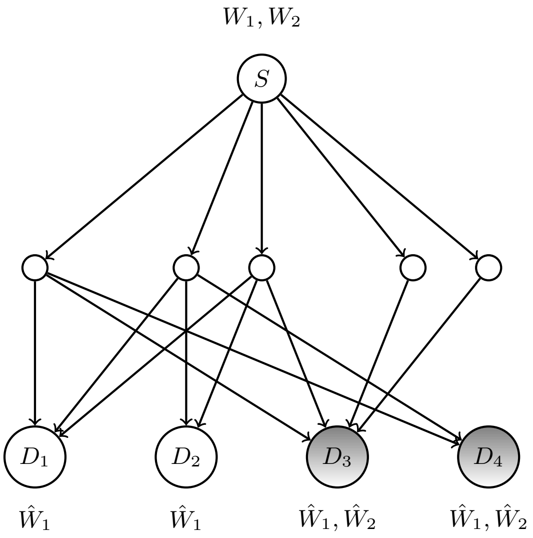


Fig. 1: A combination network with two public receivers indexed by $I_1 = \{1, 2\}$ and two private receivers indexed by $I_2 = \{3, 4\}$. All edges are of unit capacity.

common message and a private message) towards multiple users. The demands of the users are as follows: a subset of the users, which we call the public receivers, only demand the common message and the rest of the users, which we call the private receivers, demand both the common message and the private message (the term private does not imply any security criteria in this paper).

Combination networks turn out to be an interesting class of networks that allows us to discuss new encoding schemes and obtain new capacity results. We discuss three encoding schemes and prove optimality of our schemes in several cases (depending on the number of public receivers, irrespective of the number of private receivers). In particular, we propose a block Markov encoding scheme which outperforms the previous schemes that are based on rate splitting and linear superposition coding. Furthermore, for combination networks with three (or fewer) public and any number of private receivers, we characterize the capacity region in terms of a feasibility problem. Combination networks are not only a class of wired networks, but they are also a class of broadcast channels. To illustrate the implications of our study over broadcast channels, we generlize our results to propose a block Markov encoding scheme for broadcasting two nested message sets over general broadcast channels (with multiple public and private receivers). The rate-region that is obtained includes the previously known rate-regions.

A. Communication Setup

Before setting up the problem formally, we define combination networks as follows. A combination network is a three-layer directed network with one source and multiple destinations. It consists of a source node in the first layer, d intermediate nodes in the second layer and K destination nodes in the third layer. The source is connected to all intermediate nodes, and each intermediate node is connected to a subset of the destinations. We refer to the outgoing edges of the source as the *resources* of the combination network. See Fig. 1. We assume that each edge in this network carries one symbol from a finite field $\mathbb{F}_q$. We express all rates in symbols per channel use ($\log_2 q$ bits per channel use) and thus all edges are of unit capacity.

The communication setup is shown in Fig. 1. The source multicasts a common message W_1 and an a private message W_2 towards K destinations over a combination network. W_1 and W_2 are assumed to be independent. The common message is to be reliably decoded at all destinations, and the private message is to be reliably decoded at a subset of the destinations. Recall that we refer to those destinations who demand both messages as the *private receivers* and to those who demand only the common message as the *public receivers*. We denote the number of public receivers by m and, without loss of generality, we assume that they are indexed as $1, \ldots, m$. The set of all public receivers is denoted by $\mathcal{I}_1 = \{1, 2, \ldots, m\}$ and the set of all private receivers is denoted by $\mathcal{I}_2 = \{m + 1, \ldots, K\}$.

We consider encoding over blocks of length n. The source *encodes* messages W_1 (of nR_1 bits) and W_2 (of nR_2 bits) into sequences of symbols that are sent over the resources of the combination network (over n uses of the network). Based on the structure of the network, each received sequence Y_i^n consists of a certain collection of sequences that were sent by the source. From their received sequences, the public receivers $i = 1, \ldots, m$ *decode* $\hat{W}_1$ and the private receivers $p = m + 1, \ldots, K$ *decode* $\hat{W}_1, \hat{W}_2$. A rate pair (R_1, R_2) is said to be achievable if there is an encoding scheme at the source and decoding schemes at the receivers that allow the error probability $\Pr[\hat{W}_1 \neq W_1, \hat{W}_2 \neq W_2]$ approach zero (as $n \to \infty$). We call the closure of all achievable rate-pairs the capacity region of the problem. The question of main interest in this work is to find the capacity region by finding tight inner and outer bounds on the set of all achievable rates.

B. A Brief Summary of the Main Results

Our primary results are in the form of coding theorems for multicasting two nested message sets over combination networks. We characterize two inner-bounds on the capacity region and show their tightness for networks with three (or fewer) public and any number of private receivers, by proving converse theorems. We then generalize our results to propose a novel block Markov encoding scheme for broadcasting two nested message sets over general broadcast channels.

The first inner-bound is formulated in Theorem 1 (see Section IV). This inner-bound is achieved by a scheme based on pre-encoding, rate-splitting, and linear superposition coding and is characterized in terms of a feasibility problem. We show in Theorem 4 that this feasibility problem characterizes the capacity region of combination networks with three (or fewer) public and any number of private receivers. The converse proof uses sub modularity of the entropy (see Section VI). Furthermore, we show through an example that the aforementioned scheme is sub-optimal for combination networks with more than three public receivers (see Example 5).

In Section V, we propose an optimal encoding scheme for the aforementioned example (Example 5) based on a block Markov encoding scheme. Motivated by this example, we prove a second inner-bound on the capacity region which is formulated in Theorem 2. The achievability is by a block Markov encoding scheme and uses tools from the rate-splitting and superposition encoding techniques. We show that this second inner-bound is also optimal for combination networks with three (or fewer) public and any number of private receivers in Theorem 5 (see Section VI). We present an example for which the rate-region of Theorem 2 strictly includes the rate-region of Theorem 1 (see Fig. 9). Theorems 1 and 2 are not comparable in general, however, and it remains open whether this inclusion holds in general or not. We conjecture that it is true.

In Section VII, we generalize our results and propose a block Markov encoding scheme for the general broadcast channel with two nested message sets. This scheme achieves a rate-region which includes all known rate-regions (see Theorem 6). We do not know if this inclusion is strict.

C. Organization of the Paper

The paper is organized in eight sections. In Section II, we give an overview of the underlying challenges and our main ideas through several examples. Our notation is introduced in Section III. We study linear encoding schemes which are based on rate splitting, linear superposition coding, and pre-encoding in Section IV. Section V proposes a block Markov encoding scheme for multicasting nested message sets, Section VI discusses our optimality results, and Section VII generalizes the block Markov encoding scheme of Section V to general broadcast channels. We conclude in Section VIII.

II. Main Ideas at a Glance

The problem of multicasting messages to receivers which have (two) different demands over a shared medium (such as the combination network) is, in a sense, finding an optimal solution to a trade-off. This trade-off arises because, on the one hand, public receivers (which presumably have access to fewer resources) need enough information about the common message *only* so that each can decode the common message and, on the other hand, private receivers require complete information of both messages. It is, therefore, desirable from private receivers' point of view to have these messages jointly encoded (when there are multiple private receivers) and this may be in contrast with the public receivers' decodability requirement. This tension is best seen through an example.

Example 1. Consider the combination network shown in Fig. 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, it is not difficult to verify the following facts.

- Randomly and linearly combining all information symbols and sending them out on the resources of the combination network does not gaurantee decodability of W_1 at the public receivers.
- In order to achieve the rate pair $(R_1 = 1, R_2 = 2)$, it is necessary that some partial information about the private message is revealed to public receiver 2. More precisely, rate pair $(1, 2)$ is feasible only if receiver 2 decodes some partial information about W_2 in addition to its desired message W_1.

△

Example 1 suggests that an optimal encoding scheme should allow mixing of the common message with the private message, but in a restricted and controlled manner so that it reveals *partial private information* to the public receivers and allows decodability of the common message.

One standard approach for revealing partial (private) information to the public receivers is through the *rate splitting technique*. Our first encoding scheme splits the private rate into 2^m rate-split parameters $\alpha_{\mathcal{S}} \geq 0, \mathcal{S} \subseteq \mathcal{I}_1$, such that $\sum_{s \subseteq \mathcal{I}_1} \alpha_{\mathcal{S}} = R_2$, and performs a linear superposition coding. In other words, it breaks the private information into independent pieces and reveals

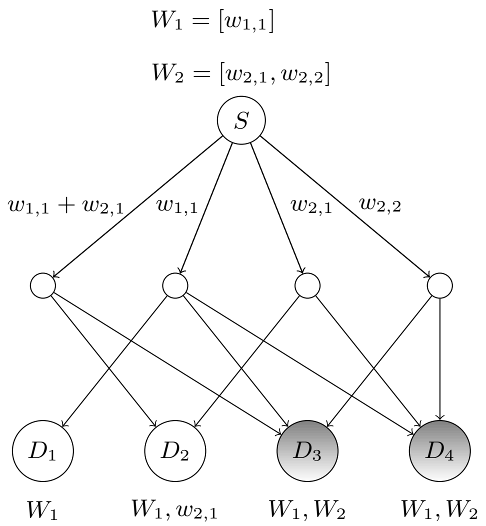


Fig. 2: In order to multicast messages $W_1 = [w_{1,1}]$ and $W_2 = [w_{2,1}, w_{2,2}]$ (of rates $R_1 = 1$ and $R_2 = 2$), the source needs to reveal partial information about the private message to public receiver 2. In this example, this partial information is $w_{2,1}$.

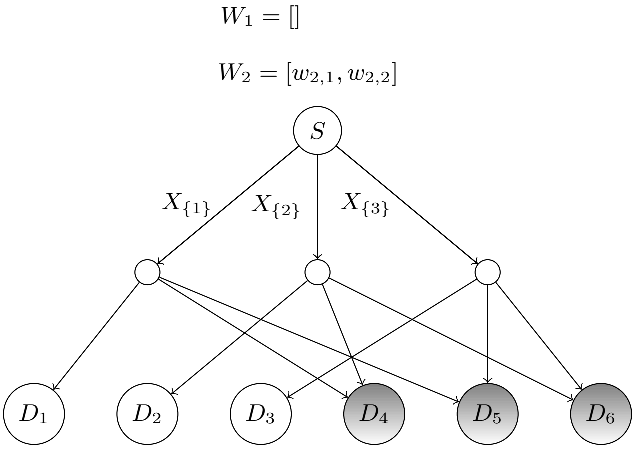


Fig. 3: The Inner-bound of Proposition 1 is not tight for $m > 2$ public receivers: while the rate pair $(0, 2)$ is not within the rate-region of Proposition 1, a multicast code such as $X_{\{1\}} = w_{2,1}$, $X_{\{2\}} = w_{2,2}$, $X_{\{3\}} = w_{2,1} + w_{2,2}$ ensures its achievability.

each piece to a subset of the public receivers. This scheme achieves the rate-region that is formulated in Proposition 1 in terms of a feasibility problem (see Section IV) and we show that it is optimal for combination networks with two public and any number of private receivers.

For networks with three or more public and any number of private receivers, the above scheme may perform sub-optimally. It turns out that one may, depending on the structure of the resources, gain by introducing some dependency among the partial (private) information that is revealed to different subsets of public receivers. This can be seen through the following example.

Example 2. Consider the combination network of Fig. 3 where destinations 1, 2, 3 are public receivers and destinations 4, 5, 6 are private receivers. The source wants to communicate a common message of rate $R_1 = 0$ (i.e., $W_1 = []$) and a private message $W_2 = [w_{2,1}, w_{2,2}]$ of rate $R_2 = 2$. One can verify that the discussed rate-splitting and linear superposition coding does not attain the desired rate pair $(0, 2)$. However, it is clear that this rate pair is achievable using the multicast code shown in Fig. 3 (or simply through a random linear network code). In order to see the insufficiency of the previous scheme, note that although the optimal scheme above reveals partial (private) information to the different subsets of the public receivers, this is not done by splitting the private message into independent pieces and there is a certain dependency structure between the symbols that are revealed to the receivers 1, 2, and 3.

$\triangle$

In our second approach, we allow this dependency by an appropriate pre-encoder which encodes the private message into a pseudo private message of a larger rate, followed by a linear superposition encoding scheme. This scheme achieves a strictly larger rate-region which is formally stated in Theorem 1 in terms of a feasibility problem (see Section IV). We further prove

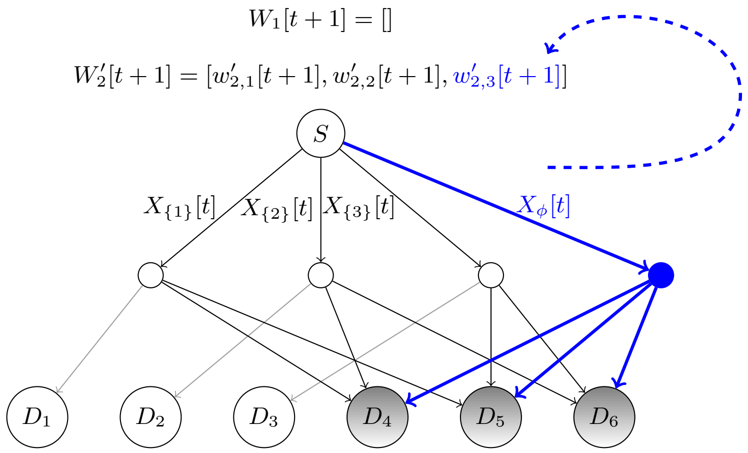


Fig. 4: The extended combination network of Example 3. A block Markov encoding scheme allows achievability of rate pair $(0, 2)$ over the original combination network. At time $t+1$, information symbol $w'_{2,3}[t+1]$ contains the information of symbol $X_{\{\phi\}}[t]$.

that this rate-region is tight for $m = 3$ (or fewer) public receivers and any number of private receivers (as opposed to 2 public receivers for Proposition 1). To prove the converse, we first write an outer-bound on the rate-region which looks *similar* to the inner-bound feasibility problem and is in terms of some entropy functions. Next, we use *sub-modularity of entropy* to write a converse for every inequality of the innerbound. In this process, we do not need to explicitly solve the feasibility problem.

Generalizing the pre/encoding scheme to networks with more than three public receivers is difficult because of the more involved dependency structure that might be needed, in an optimal code design, among the partial (private) information pieces that are to be revealed to the subsets of public receivers. Therefore, we propose an alternative encoding scheme that captures these dependencies over sequential blocks, rather than the structure of the one-time (one-block) code. This is done by devising a simple *block Markov encoding scheme*. Below, we illustrate the main idea of the block Markov scheme by revisiting the combination network of Fig. 3.

Example 3. Consider the combination network in Fig. 3 over which we want to achieve the rate pair $(R_1 = 0, R_2 = 2)$. Our first code design using rate splitting and linear superposition coding (with no pre-encoding) was not capable of achieving this rate pair. Let us add one resource to this combination network and connect it to all the private receivers. This gives an extended combination network, as shown in Fig. 4, which differs from the original network only in one edge. This “virtual” resource is shown in Fig. 4 by a bold edge. One can verify that the larger rate pair $(R_1 = 0, R'_2 = 3)$ is achievable over this extended network, using a basic linear superposition scheme!

Let the message $W'_2 = [w'_{2,1}, w'_{2,2}, w'_{2,3}]$ be a pseudo private message of larger rate ($R'_2 = 3$) which is to be communicated over the extended combination network, and let $X_{\{1\}}$, $X_{\{2\}}$, $X_{\{3\}}$, X_ϕ be the symbols that are sent over the extended combination network. One code design is given below. We will use this code to achieve our desired rate pair $(0, 2)$ over the original network.

$$\begin{aligned} X_{\{1\}} &= w'_{2,1} \\ X_{\{2\}} &= w'_{2,2} \\ X_{\{3\}} &= w'_{2,3} \\ X_\phi &= w'_{2,1} + w'_{2,2} + w'_{2,3}. \end{aligned} \tag{1}$$

Since the resource edge that carried X_ϕ is a virtual resource, we aim to emulate it through a block Markov encoding scheme. Using the code design of (1), all information symbols ($w'_{2,1}$, $w'_{2,2}$, $w'_{2,3}$) are decodable at all private receivers. One way to emulate the bold virtual resource, for example, is to send its information (the symbol carried over it) in the next time slot using one of the information symbols $w'_{2,1}$, $w'_{2,2}$, $w'_{2,4}$ that are to be communicated in the next time slot.

More precisely, consider communication over n transmission blocks, and let $(W_1[t], W'_2[t])$ be the message pair that is being encoded in block $t \in \{1, \dots, n\}$. In the t^{th} block, encoding is done as suggested by the code in (1). Nevertheless, to provide the private receivers with the information of $X_\phi[t]$ (as promised by the virtual resource), we use information symbol $w'_{2,3}[t+1]$ in the next block, to convey $X_\phi[t]$. Since this symbol is ensured to be decoded at the private receivers, it indeed emulates the virtual resource. In the n^{th} block, we simply encode $X_\phi[n-1]$ and directly communicate it with the private receivers. Upon receiving all the n blocks at the receivers, we perform backward decoding [36].

So in n transmissions, we send $n-1$ symbols of W_1 and $2(n-1)+1$ new symbols of W_2 over the original combination network; i.e., for $n \to \infty$, we achieve the rate-pair $(0, 2)$. △

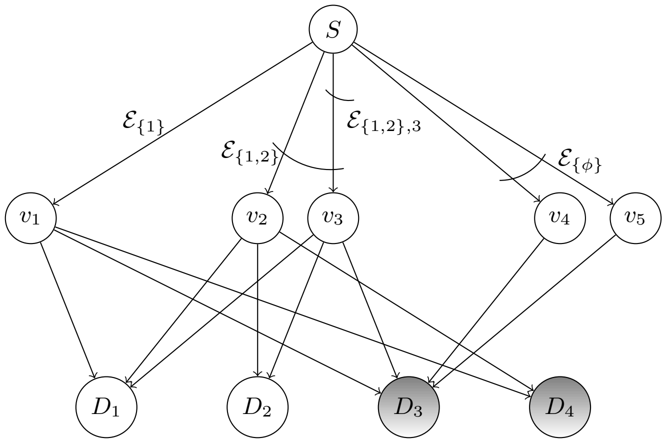


Fig. 5: A combination network with two public receivers indexed by $I_1 = \{1, 2\}$ and two private receivers indexed by $I_2 = \{3, 4\}$.

In Section V, we describe our block Markov encoding scheme and characterize its achievable rate region (see Theorem 2). We show, for three (or fewer) public and any number of private receivers, that this rate-region is equal to the capacity region and, therefore, coincides with the rate-region of Theorem 1. Furthermore, we show through an example that the block Markov encoding scheme could outperform the previously discussed linear encoding schemes when there are more than 3 public receivers.

In Section VII, we further adapt this scheme to general broadcast channels with two nested message sets and obtain a rate region that includes the previously known rate-regions. We do not know if this inclusion is strict.

III. NOTATION

We denote the set of outgoing edges from the source by $\mathcal{E}$ with cardiality $|\mathcal{E}| = d$, and we refer to those edges as the resources of the combination network. The resources are labeled according to the public receivers they are connected to; i.e., we denote the set of all resources that are connected to every public receiver in $\mathcal{S}$, $\mathcal{S} \subseteq \mathcal{I}_1$, and not connected to any other public receiver by $\mathcal{E}_{\mathcal{S}} \subseteq \mathcal{E}$. Note that the edges in $\mathcal{E}_{\mathcal{S}}$ may or may not be connected to the private receivers. We identify the subset of edges in $\mathcal{E}_{\mathcal{S}}$ that are also connected to a private receiver p by $\mathcal{E}_{\mathcal{S},p}$. Fig. 1 shows this notation over a combination network with four receivers. In this example, $d = 5$, $\mathcal{E} = \{(s, v_1), (s, v_2), (s, v_3), (s, v_4), (s, v_5)\}$, $\mathcal{E}_\phi = \{(s, v_4), (s, v_5)\}$, $\mathcal{E}_{\{1\}} = \{(s, v_1)\}$, $\mathcal{E}_{\{2\}} = \{\}$, $\mathcal{E}_{\{1,2\}} = \{(s, v_2), (s, v_3)\}$, $\mathcal{E}_{\phi,3} = \{(s, v_4), (s, v_5)\}$, $\mathcal{E}_{\phi,4} = \{\}$, $\mathcal{E}_{\{1\},3} = \mathcal{E}_{\{1\},4} = \{(s, v_1)\}$, $\mathcal{E}_{\{2\},3} = \mathcal{E}_{\{2\},4} = \{\}$, $\mathcal{E}_{\{1,2\},3} = \{(s, v_3)\}$, $\mathcal{E}_{\{1,2\},4} = \{(s, v_2)\}$.

Throughout this paper, we denote random variables by capital letters (e.g., X, Y), the sets $\{1, \ldots, m\}$ and $\{m+1, \ldots, K\}$ by $\mathcal{I}_1$ and $\mathcal{I}_2$, respectively, and subsets of $\mathcal{I}_1$ by script capital letters (e.g., $\mathcal{S} = \{1, 2, 3\}$ and $\mathcal{T} = \{1, 3, 4\}$). We denote the set of all subsets of $\mathcal{I}_1$ by $2^{\mathcal{I}_1}$ and in addition denote its subsets by Greek capital letters (e.g., $\Gamma = \{\{1\}, \{1, 2\}\}$ and $\Lambda = \{\{1\}, \{2\}, \{1, 2\}\}$).

All rates are expressed in $\log_2 |\mathbb{F}_q|$ in this work. The symbol carried over a resource of the combination network, $e \in \mathcal{E}$, is denoted by x_e which is a scalar from $\mathbb{F}_q$. Similarly, its corresponding random variable is denoted by X_e. We denote by $X_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, the vector of symbols carried over resource edges in $\mathcal{E}_{\mathcal{S}}$, and by $X_{\mathcal{S},p}$, $\mathcal{S} \subseteq \mathcal{I}_1$, $p \in \mathcal{I}_2$, the vector of symbols carried over resource edges in $\mathcal{E}_{\mathcal{S},p}$. To simplify notation, we sometimes abbreviate the union sets $\bigcup_{\mathcal{S} \in \Lambda} \mathcal{E}_{\mathcal{S}}$, $\bigcup_{\mathcal{S} \in \Lambda} \mathcal{E}_{\mathcal{S},p}$ and $\bigcup_{\mathcal{S} \in \Lambda} X_{\mathcal{S}}$, by $\mathcal{E}_\Lambda$, $\mathcal{E}_{\Lambda,p}$ and X_Λ, respectively, where Λ is a subset of $2^{\mathcal{I}_1}$. The vector of all received symbols at receiver i is denoted by Y_i, $i \in \{1, \ldots, K\}$. When communication takes place over blocks of length n, all vectors above take a superscript n; e.g., X_e^n $X_{\mathcal{S}}^n$, $X_{\mathcal{S},p}^n$, X_Λ^n, $X_{\Lambda,p}^n$, Y_i^n.

We define superset saturated subsets of $2^{\mathcal{I}_1}$ as follows. A subset $\Lambda \subseteq 2^{\mathcal{I}_1}$ is superset saturated if inclusion of any set $\mathcal{S}$ in Λ implies the inclusion of all its supersets; e.g., over subsets of $2^{\{1,2,3\}}$, $\Lambda = \{\{1\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ is superset saturated, but not $\Lambda = \{\{1\}, \{1, 3\}, \{1, 2, 3\}\}$.

Definition 1 (Superset saturated subsets)**.** *The subset $\Lambda \subseteq 2^{\mathcal{I}_1}$ is superset saturated if it is such that $\mathcal{S}$ is an element of Λ only if every $\mathcal{T} \in 2^{\mathcal{I}_1}$, where $\mathcal{T} \supseteq \mathcal{S}$, is an element of Λ.*

For notational matters, we sometimes abbreviate a superset saturated subset Λ by the few sets that are not implied by the other sets in Λ. For example, $\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$ is denoted by $\{\{1\}\star\}$, and similarly $\{\{1\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ is denoted by $\{\{1\}\star, \{2, 3\}\star\}$.

IV. Rate Splitting and Linear Encoding Schemes

Throughout this section, we confine ourselves to linear encoding at the source. For simplicity of the presentation, we describe our encoding schemes for block length $n = 1$, and we highlight cases where we need to code over longer blocks.

We assume rates R_1 and R_2 to be non-negative integer values[1]. Let $w_{1,1}, \ldots, w_{1,R_1}$ and $w_{2,1}, \ldots, w_{2,R_2}$ be variables in $\mathbb{F}_q$ for messages W_1 and W_2, respectively. We call them the information symbols of the common and the private message. Also, let vector $W \in {\mathbb{F}_q}^{R_1+R_2}$ be defined as the vector with coordinates in the standard basis $W = [w_{1,1} \ldots w_{1,R_2} w_{2,1} \ldots w_{2,R_2}]^T$. The symbol carried by each resource is a linear combination of the information symbols $w_{1,1}, \ldots, w_{1,R_1}, w_{2,1}, \ldots, w_{2,R_2}$, and after properly rearranging all vectors $X_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, we have

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

where $\mathbf{A} \in {\mathbb{F}_q}^{d \times (R_1+R_2)}$ is the encoding matrix. At each public receiver i, $i \in \mathcal{I}_1$, the received signal Y_i is given by $Y_i = \mathbf{A}_i W$, where $\mathbf{A}_i$ is a submatrix of $\mathbf{A}$ corresponding to $X_{\mathcal{S}}$, $\mathcal{S} \ni i$. Similarly, the received signal at each private receiver p, $p \in \mathcal{I}_2$, is given by $Y_p = \mathbf{A}_p W$, where $\mathbf{A}_p$ is the submatrix of the rows $\mathbf{A}$ corresponding to $X_{\mathcal{S},p}$, $\mathcal{S} \subseteq \mathcal{I}_1$.

The aim of this section is to design $\mathbf{A}$ in a manner that allows the public receivers to decode W_1 and the private receivers to decode W_1, W_2. We then characterize the rate pairs achievable by our code design.

The challenge in the optimal code design in this problem stems from the fact that destinations receive different subsets of the symbols that are sent out of the source and they have two different decodability requirements. On the one hand, private receivers require their received signal to bring information about all information symbols of the common and the private message. On the other hand, public receivers might not be able to decode the common message if their received symbols depend on "too many" private message variables. We make this statement precise in Lemma 1. In the following, we find conditions for decodability of the messages.

A. Decodability Lemmas

Lemma 1. *Let vector Y be given by* (2)*, below, where $\mathbf{B} \in {\mathbb{F}_q}^{r \times R_1}$, $\mathbf{T} \in {\mathbb{F}_q}^{r \times R_2}$, $W_1 \in {\mathbb{F}_q}^{R_1 \times 1}$, and $W_2 \in {\mathbb{F}_q}^{R_2 \times 1}$.*

$$Y = \left[\begin{array}{c|c} \mathbf{B} & \mathbf{T} \end{array}\right] \cdot \begin{bmatrix} W_1 \\ W_2 \end{bmatrix}. \tag{2}$$

Message W_1 is recoverable from Y if and only if rank$(\mathbf{B}) = R_1$ and the column space of $\mathbf{B}$ is disjoint from that of $\mathbf{T}$.

Corollary 1. *Message W_1 is recoverable from Y in equation* (2)*, only if*

$$\textit{rank}(\mathbf{T}) \leq r - R_1.$$

We defer the proof of Lemma 1 to Appendix A and instead discuss the high-level implication of the result. Let $r_{\mathbf{T}} = \text{rank}(\mathbf{T})$ where $r_{\mathbf{T}} \leq r - R_1$. Matrix $\mathbf{T}$ can thus be written as $\mathbf{L}_1\mathbf{L}_2$, where $\mathbf{L}_1$ is a full-rank matrix of dimension $r \times r_{\mathbf{T}}$ and $\mathbf{L}_2$ is a full-rank matrix of dimension $r_{\mathbf{T}} \times R_2$. $\mathbf{L}_1$ is essentially just a set of linearly independent columns of $\mathbf{B}$ spanning its column space. In other words, we can write

$$\left[\begin{array}{c|c} \mathbf{B} & \mathbf{T} \end{array}\right] W = \left[\begin{array}{c|c} \mathbf{B} & \mathbf{L}_1\mathbf{L}_2 \end{array}\right] W \tag{3}$$

$$= \left[\begin{array}{c|c} \mathbf{B} & \mathbf{L}_1 \end{array}\right] \begin{bmatrix} W_1 \\ \mathbf{L}_2 W_2 \end{bmatrix}. \tag{4}$$

Now since $r_{\mathbf{T}} + R_1 \leq r$, W_1, W_2 are decodable if $\left[\begin{array}{c|c} \mathbf{B} & \mathbf{L}_1 \end{array}\right]$ is full-rank. So if $r_{\mathbf{T}} \leq r - R_1$, then $\left[\begin{array}{c|c} \mathbf{B} & \mathbf{L}_1 \end{array}\right]$ being full rank guarantees decodability of W_1.

Defining $\left[\begin{array}{c|c} \mathbf{B} & \mathbf{T} \end{array}\right]$ as a new $\mathbf{B}'$ of dimension $r \times (R_1 + R_2)$ and defining a null matrix $\mathbf{T}'$ in Lemma 1, we get back the trivial result of the following corollary.

Corollary 2. *Messages W_1, W_2 are recoverable from Y in equation* (2)*, if and only if*

$$\textit{rank}\left(\left[\begin{array}{c|c} \mathbf{B} & \mathbf{T} \end{array}\right]\right) = R_1 + R_2.$$

Since every receiver sees a different subset of the sent symbols, it becomes clear from Corollary 1 and 2 that an admissible linear code needs to satisfy many rank constraints on its different submatrices. In this section, our primary approach to the design of such codes is through zero-structured matrices, discussed next.

[1] There is no loss of generality in this assumption. One can deal with rational values of R_1 and R_2 by coding over blocks of large enough length n and working with integer rates nR_1 and nR_2. Also, one can attain real valued rates through sequences of rational numbers that approach them.

B. Zero-structured matrices

As mentioned earlier, the goal of this section is the design of an encoding matrix $\mathbf{A}$ which allows decodability of W_1 at the public receivers and W_1, W_2 at the private receivers. This matrix is indeterminate a priori. We find conditions so that there exists an assignment of it that allows decodability of each message at its intended receivers. From Lemma 1, several rank constraints are required at different submatrices of the encoding matrix. In our first approach, we respect these requirements by setting certain entries of the encoding matrix to zero. The rest remain variables to be designed. Zero-structured matrices are a class of matrices that turn out to be useful in our code design.

Definition 2. *A zero-structured matrix $\mathbf{T}$ is an $r \times c$ matrix with entries either zero or indeterminate*[2] *(from a finite field $\mathbb{F}_q$) in a specific structure, as follows. This matrix consists of $2^t \times 2^t$ blocks, where each block is indexed on rows and columns by the subsets of $\{1, \cdots, t\}$. Block $b_{(\mathcal{S}_1, \mathcal{S}_2)}$, $\mathcal{S}_1, \mathcal{S}_2 \subseteq \{1, \cdots, t\}$, is an $r_{\mathcal{S}_1} \times c_{\mathcal{S}_2}$ matrix. Matrix $\mathbf{T}$ is structured so that all entries in block $b_{(\mathcal{S}_1, \mathcal{S}_2)}$ are set to zero if $\mathcal{S}_1 \not\subseteq \mathcal{S}_2$, and remain indeterminate otherwise. Note that $c = \sum_{\mathcal{S}} c_{\mathcal{S}}$ and $r = \sum_{\mathcal{S}} r_{\mathcal{S}}$.*

Equation (5), below, demonstrates this definition for $t = 2$.

$$\mathbf{T} = \begin{array}{c} \begin{array}{cccc} \overset{c_{\{1,2\}}}{\longleftrightarrow} & \overset{c_{\{1\}}}{\leftrightarrow} & \overset{c_{\{2\}}}{\leftrightarrow} & \overset{c_{\phi}}{\leftrightarrow} \end{array} \\ \left[\begin{array}{c|c|c|c} & 0 & 0 & 0 \\ \hline & & 0 & 0 \\ \hline & 0 & & 0 \\ \hline & & & \end{array}\right] \end{array} \begin{array}{l} \\ \updownarrow r_{\{1,2\}} \\ \updownarrow r_{\{1\}} \\ \updownarrow r_{\{2\}} \\ \updownarrow r_{\phi} \end{array} . \tag{5}$$

The idea behind using zero-structred encoding matrices is the following: the zeros are inserted in the encoding matrix such that the linear combinations that are formed for the public receivers do not depend on "too many" private information symbols (see Corollary 1).

In the rest of this subsection, we find conditions on zero-structured matrices so that they can be made full column rank. We will prove the following result.

Lemma 2. *There exists an assignment of the indeterminates in the zero-structured matrix $\mathbf{T} \in \mathbb{F}_q^{r \times c}$ (as specified in Definition 2) that makes it full column rank, provided that*

$$c \leq \sum_{\mathcal{S} \in \Lambda} c_{\mathcal{S}} + \sum_{\mathcal{S} \in \Lambda^c} r_{\mathcal{S}}, \qquad \forall \Lambda \subseteq 2^{\{1,\ldots,t\}} \text{ superset saturated.} \tag{6}$$

To illustrate the set of conditions in (6), we expand them for $t = 2$ in the following:

$$c \leq r_{\{1,2\}} + r_{\{1\}} + r_{2\}} + r_{\phi}, \tag{7}$$

$$c \leq c_{\{1,2\}} + r_{\{1\}} + r_{\{2\}} + r_{\phi}, \tag{8}$$

$$c \leq c_{\{1\}} + c_{\{1,2\}} + r_{\{2\}} + r_{\phi}, \tag{9}$$

$$c \leq c_{\{2\}} + c_{\{1,2\}} + r_{\{1\}} + r_{\phi}, \tag{10}$$

$$c \leq c_{\{1\}} + c_{\{2\}} + c_{\{1,2\}} + r_{\phi}, \tag{11}$$

$$c \leq c_{\phi} + c_{\{1\}} + c_{\{2\}} + c_{\{1,2\}}. \tag{12}$$

We briefly outline the proof of Lemma 2, because this line of argument is used again later in Section IV-D. For simplicity of notation and clarity of the proof, we give details of the proof for $t = 2$. The same proof technique proves the general case.

Let matrix $\mathbf{T} \in \mathbb{F}_q^{r \times c}$ be a zero-structured matrix given by equation (5). We first reduce the problem of matrix $\mathbf{T}$ being full column rank to an information flow problem over an equivalent unicast network (which is given in Fig. 6), and then find conditions for feasibility of the equivalent unicast problem. The former is stated in Lemma 3 and the latter is formulated in Lemma 4, both to follow.

The equivalent unicast network of Fig. 6 is formed as follows. The network is a four-layer directed network with a source node A in the first layer, four (in general 2^t) nodes $n_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1, \ldots, t\}$, in the second layer, another four (in general 2^t) nodes $n'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1, \ldots, t\}$, in the third layer, and finally a sink node B in the fourth layer. Over this network, the source wants to communicate a message of rate c to the sink. From the source A to each node $n_{\mathcal{S}}$, we have $c_{\mathcal{S}}$ (unit capacity) edges. Also, from each node $n'_{\mathcal{S}}$ to the sink B, we have $r_{\mathcal{S}}$ (unit capacity) edges. The edges from the second layer to the third layer of this equivalent unicast network are all of infinite capacity and they connect each node $n_{\mathcal{S}}$ to all nodes $n'_{\mathcal{S}'}$, where $\mathcal{S}' \subseteq \mathcal{S}$. The equivalent unicast network is tailored so that the mixing of the information which happens at each node $n'_{\mathcal{S}}$ (at the third layer) mimics the same mixing of the information that is present in the rows of matrix $\mathbf{T}$.

The aforementioned equivalence is discussed formally in Lemma 3 and its proof is deferred to Appendix B.

Lemma 3. *Given the zero-structured matrix $\mathbf{T} \in \mathbb{F}_q^{r \times c}$ of equation* (5)*, the following two statements are equivalent.*

[2] Although zero-structured matrices are defined in Definition 2 with zero or indeterminate variables, we also refer to the assignments of such matrices as zero-structured matrices.

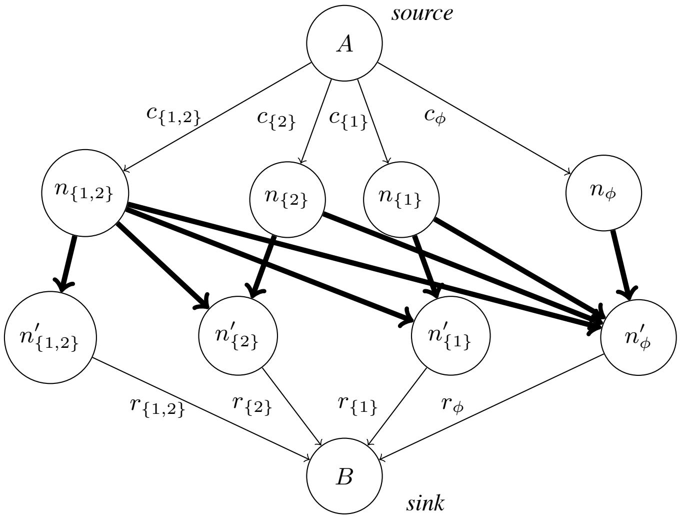


Fig. 6: The source A communicates a message of rate $c = \sum_{\mathcal{S}} c_{\mathcal{S}}$ to the sink B over a unicast network. The capacity of each edge is marked beside it. The bold edges are of infinite capacity. The network is tailored so that the mixing of the information which happens at the third layer mimics the same mixing of the information that is present in the rows of matrix $\mathbf{T}$.

(i) *There exists an assignment of variables in* $\mathbf{T}$ *that makes it full column rank.*
(ii) *A message of rate* c *could be sent over its equivalent unicast network (the network in Fig. 6).*

Using Lemma 3, we see that the conditions under which $\mathbf{T}$ could be made full-rank is given by the min-cut between nodes A and B over the equivalent unicast network. These conditions are given by Lemma 4 and the proof is delegated to Appendix C.

Lemma 4. *The min-cut separating nodes* A *and* B *over the network of Fig. 6 is given by the following expression:*

$$\min_{\substack{\Lambda \subseteq 2^{\mathcal{I}_1} \\ \Lambda \text{ superset saturated}}} \sum_{\mathcal{S} \in \Lambda} c_{\mathcal{S}} + \sum_{\mathcal{S} \in \Lambda^c} r_{\mathcal{S}}. \tag{13}$$

So Lemma 3 and Lemma 4, together, find conditions for matrix $\mathbf{T}$ to become full rank. The proof for $t > 2$ is along the same lines.

C. Zero-structured linear codes: an achievable rate-region

We saw in Example 1 that in order to allow the common message be decoded at a public receiver, the resource symbols available to that receiver should not depend on "too many" private message variables. In our initial approach, we resolve this by a zero-structured encoding matrix. Equation (14) below shows such an encoding matrix for two public and any number of private receivers. The non-zero entries are all indeterminate and to be designed appropriately. Also, parameters $\alpha_{\{1,2\}}$, $\alpha_{\{2\}}$, $\alpha_{\{1\}}$ and α_{ϕ} are non-negative structural parameters, and they satisfy $\alpha_{\{1,2\}} + \alpha_{\{2\}} + \alpha_{\{1\}} + \alpha_{\phi} = R_2$.

$$\mathbf{A} = \begin{array}{c} \begin{array}{ccccc} \overleftrightarrow{R_1} & \overleftrightarrow{\alpha_{\{1,2\}}} & \overleftrightarrow{\alpha_{\{2\}}} & \overleftrightarrow{\alpha_{\{1\}}} & \overleftrightarrow{\alpha_{\phi}} \end{array} \\ \left[\begin{array}{c|c|c|c|c} \quad & \quad & 0 & 0 & 0 \\ \hline \quad & \quad & \quad & 0 & 0 \\ \hline \quad & \quad & 0 & \quad & 0 \\ \hline \quad & \quad & \quad & \quad & \quad \end{array}\right] \end{array} \begin{array}{l} \\ \updownarrow |\mathcal{E}_{\{1,2\}}| \\ \updownarrow |\mathcal{E}_{\{2\}}| \\ \updownarrow |\mathcal{E}_{\{1\}}| \\ \updownarrow |\mathcal{E}_{\phi}| \end{array} . \tag{14}$$

In effect, matrix $\mathbf{A}$ splits message W_2 into four independent messages, $W_2^{\{1,2\}}$, $W_2^{\{2\}}$, $W_2^{\{1\}}$, W_2^{ϕ}, of rates $\alpha_{\{1,2\}}$, $\alpha_{\{2\}}$, $\alpha_{\{1\}}$, α_{ϕ}, respectively. The zero structure of $\mathbf{A}$ ensures that only messages W_1, $W_2^{\{1,2\}}$ and $W_2^{\{1\}}$ are involved in the linear combinations that are received at public receiver 1 and that only messages W_1, $W_2^{\{1,2\}}$ and $W_2^{\{2\}}$ are involved in the linear combinations that are received at public receiver 2. In general, matrix $\mathbf{A}$ splits message W_2 into independent messages $W_2^{\mathcal{S}}$ of rates $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, such that

$$\sum_{\mathcal{S} \subseteq \mathcal{I}_1} \alpha_{\mathcal{S}} = R_2. \tag{15}$$

Note that the zero structure allows messages $W_2^{\mathcal{S}}$ to be involved (only) in the linear combinations that are sent over resources in $\mathcal{E}_{\mathcal{S}'}$ where $\mathcal{S}' \subseteq \mathcal{S}$. When referring to a zero-structured encoding matrix $\mathbf{A}$, we also specify the rate-split parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$.

Remark 1. *As defined above, parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, are assumed to be integer-valued. Nonetheless, one can let these parameters be real and approximately attain them by encoding over blocks of large enough length.*

In the following, we find conditions under which all receivers can decode their messages of interest from their received signals.

- **Public receiver** $i \in \mathcal{I}_1$**:** The received signal Y_i is the vector of all the symbols carried by the resources available to receiver i. Using the zero-structured encoding matrix in (14), we have Y_2 as follows:

$$Y_2 = \left[\begin{array}{c} X_{\{1,2\}} \\ X_{\{2\}} \end{array} \right] \tag{16}$$

$$= \begin{array}{c} \begin{array}{ccccc} \overset{R_1}{\longleftrightarrow} & \overset{\alpha_{\{1,2\}}}{\longleftrightarrow} & \overset{\alpha_{\{2\}}}{\leftrightarrow} & \overset{\alpha_{\{1\}}}{\leftrightarrow} & \overset{\alpha_{\phi}}{\leftrightarrow} \end{array} \\ \left[\begin{array}{c|c|c|c|c} \quad & \quad & 0 & 0 & 0 \\ \hline \quad & \quad & & 0 & 0 \end{array} \right] \end{array} \begin{array}{l} \updownarrow |\mathcal{E}_{\{1,2\}}| \\ \updownarrow |\mathcal{E}_{\{2\}}| \end{array} . \left[\begin{array}{c} W_1 \\ W_2 \end{array} \right]. \tag{17}$$

Generally, the received signal Y_i is given by $Y_i = \mathbf{A}_i W$, where $\mathbf{A}_i$ is a submatrix of the rows of the zero-structured matrix $\mathbf{A}$ corresponding to $X_{\mathcal{S}}$, $\mathcal{S} \ni i$. It has at most $R_1 + \sum_{\mathcal{S} \subseteq \mathcal{I}_1\ \mathcal{S} \ni i} \alpha_{\mathcal{S}}$ non-zero columns.
In what follows, we relate decodability of message W_1 at receiver i to a particular submatrix of $\mathbf{A}_i$ being full column rank. Let $\mathbf{A}_i = \left[\mathbf{B}^{(i)} | \mathbf{T}^{(i)}\right]$. Choose $\mathbf{L}_1^{(i)}$ to be a largest submatrix of the columns of $\mathbf{T}^{(i)}$ that could be made full column rank (over all possible assignments). Define $\mathbf{G}^{(i)}$ to be $\mathbf{G}^{(i)} = \left[\begin{array}{c|c} \mathbf{B}^{(i)} & \mathbf{L}_1^{(i)} \end{array} \right]$. We have the following two lemmas.

Lemma 5. *Each public receiver i can decode W_1 from* (17) *if $\mathbf{G}^{(i)}$, as defined above, is full column rank.*

Proof: Conditions for decodability of W_1 are given in Lemma 1 (and its following argument). By the manner $\mathbf{L}_1^{(i)}$ and $\mathbf{G}^{(i)}$ are defined, whenever $\mathbf{G}^{(i)}$ is full column rank, not only $\mathbf{B}^{(i)}$ is full column rank, but also the columns of $\mathbf{L}_1^{(i)}$ span all the column space of $\mathbf{T}^{(i)}$ (for all possible assignments– otherwise a larger $\mathbf{L}^{(i)}$ would have been chosen) and the span of the column space of $\mathbf{T}^{(i)}$ is thus disjoint from that of $\mathbf{B}^{(i)}$. ■

Lemma 6. *For each public receiver i, there exists an assignment of $\mathbf{A}$ (specific to i) such that $\mathbf{G}^{(i)}$ is full column rank, provided that*

$$R_1 + \sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} \alpha_{\mathcal{S}} \leq \sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} |\mathcal{E}_{\mathcal{S}}|. \tag{18}$$

Proof: The proof is deferred to Appendix D. ■

- **Private receiver** $p \in \mathcal{I}_2$**:** The received signal Y_p is the vector of all the symbols carried by the resources in the sets $\mathcal{E}_{\mathcal{S},p}$, $\mathcal{S} \subseteq \mathcal{I}_1$. Using the zero-structured encoding matrix in (14), we have Y_p as follows:

$$Y_p = \left[\begin{array}{c} X^p_{\{1,2\}} \\ X^p_{\{2\}} \\ X^p_{\{1\}} \\ X^p_{\phi} \end{array} \right] \tag{19}$$

$$= \begin{array}{c} \begin{array}{ccccc} \overset{R_1}{\longleftrightarrow} & \overset{\alpha_{\{1,2\}}}{\longleftrightarrow} & \overset{\alpha_{\{2\}}}{\leftrightarrow} & \overset{\alpha_{\{1\}}}{\leftrightarrow} & \overset{\alpha_{\phi}}{\leftrightarrow} \end{array} \\ \left[\begin{array}{c|c|c|c|c} \quad & \quad & 0 & 0 & 0 \\ \hline \quad & \quad & & 0 & 0 \\ \hline \quad & \quad & 0 & & 0 \\ \hline \quad & \quad & & & \end{array} \right] \end{array} \begin{array}{l} \updownarrow |\mathcal{E}_{\{1,2\},p}| \\ \updownarrow |\mathcal{E}_{\{2\},p}| \\ \updownarrow |\mathcal{E}_{\{1\},p}| \\ \updownarrow |\mathcal{E}_{\phi,p}| \end{array} \cdot \left[\begin{array}{c} W_1 \\ W_2 \end{array} \right]. \tag{20}$$

Generally, the received signal Y_p is given by $Y_p = \mathbf{A}_p W$, where $\mathbf{A}_p$ is the submatrix of the rows of the zero-structured matrix $\mathbf{A}$ corresponding to $X_{\mathcal{S},p}$, $\mathcal{S} \subseteq \mathcal{I}_1$. Note that $\mathbf{A}_p$ is a zero-structured matrix. Messages W_1, W_2 are decodable at private receiver p, if and only if matrix $\mathbf{A}_p$ is full column rank. From Lemma 2, an assignment of $\mathbf{A}_p$ exists that makes it full column rank provided that the following inequalities hold:

$$R_2 \leq \sum_{\mathcal{S} \in \Lambda} \alpha_{\mathcal{S}} + \sum_{\mathcal{S} \in \Lambda^c} |\mathcal{E}_{\mathcal{S},p}|, \qquad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \text{ superset saturated,} \tag{21}$$

$$R_1 + R_2 \leq \sum_{\mathcal{S} \subseteq \mathcal{I}_1} |\mathcal{E}_{\mathcal{S},p}|. \tag{22}$$

Inequalities (18), (21) and (22) provide constraints on parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, under which W_1 is decodable at the public receivers (i.e., matrices $\mathbf{G}^{(i)}$, $i \in \mathcal{I}_1$, could be made full rank), and W_1, W_2 are decodable at private receivers (i.e., matrices

$\mathbf{A}_p$, $p \in \mathcal{I}_2$, could be made full rank). It remains to argue that there exists a universal assignment of $\mathbf{A}$ such that all receivers can decode their messages of interest. We do this by directly applying the sparse zeros lemma [37, Lemma 2.3].

Lemma 7. *If $|\mathbb{F}_q| > K$, a universal assignment of $\mathbf{A}$ exists such that all $\mathbf{G}^{(i)}$, $i \in \mathcal{I}_1$, and all $\mathbf{A}_p$, $p \in \mathcal{I}_2$, become simultaneously full column rank.*

Remark 2. *Note that operation over smaller fields is also possible by coding over blocks of larger lengths. Coding over blocks of length n is effectively done over the field $\mathbb{F}_{q^n}$. Therefore, we require $q^n > K$; i.e., we need $n > \log_q K$.*

The rate-region achievable by this scheme can be posed as a feasibility problem in terms of parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$. We summarize this region in the following proposition.

Proposition 1. *The rate pair (R_1, R_2) is achievable if there exists a set of real valued variables $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, that satisfies the following inequalities:*

Structural constraints:

$$\alpha_{\mathcal{S}} \geq 0, \qquad \forall \mathcal{S} \subseteq \mathcal{I}_1 \tag{23}$$

$$R_2 = \sum_{\mathcal{S} \subseteq \mathcal{I}_1} \alpha_{\mathcal{S}} \tag{24}$$

Decoding constraints at public receivers:

$$R_1 + \sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} \alpha_{\mathcal{S}} \leq \sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} |\mathcal{E}_{\mathcal{S}}|, \qquad \forall i \in \mathcal{I}_1 \tag{25}$$

Decoding constraints at private receivers:

$$R_2 \leq \sum_{\mathcal{S} \in \Lambda} \alpha_{\mathcal{S}} + \sum_{\mathcal{S} \in \Lambda^c} |\mathcal{E}_{\mathcal{S},p}|, \qquad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \textit{ superset saturated}, \ \forall p \in \mathcal{I}_2 \tag{26}$$

$$R_1 + R_2 \leq \sum_{\mathcal{S} \subseteq \mathcal{I}_1} |\mathcal{E}_{\mathcal{S},p}|, \qquad \forall p \in \mathcal{I}_2. \tag{27}$$

Remark 3. *Note that inequality (25) ensures decodability of only the common message (and not the superposed messages $W_2^{\mathcal{S}}$, $i \in \mathcal{S} \subseteq \mathcal{I}_1$) at the public receivers. To have public receiver i decode all superposed messages $W_2^{\mathcal{S}}$, $i \in \mathcal{S} \subseteq \mathcal{I}_1$, as well, one needs further constraints on $\alpha_{\mathcal{S}}$, as given below:*

$$\sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} \alpha_{\mathcal{S}} \leq \sum_{\mathcal{S} \in \Lambda} \alpha_{\mathcal{S}} + \sum_{\substack{\mathcal{S} \in \Lambda^c \\ \mathcal{S} \ni i}} |\mathcal{E}_{\mathcal{S}}|, \qquad \Lambda \subseteq \{\{i\}\star\} \textit{ superset saturated.} \tag{28}$$

More precisely, define $\tilde{\mathbf{A}}_i$ to be the submatrix of $\mathbf{A}_i$ which does not contain the all-zero columns. One observes that messages $W_2^{\mathcal{S}}$, $i \in \mathcal{S} \subseteq \mathcal{I}_1$, are all decodable if and only if $\tilde{\mathbf{A}}_i$ is full column rank. Since $\tilde{\mathbf{A}}_i$ is zero-structured, Lemma 2 gives the required constraints.

Remark 4. *In a similar manner, a general multicast code could be designed for the scenario where 2^K message sets are communicated and each message set is destined for a subset of the K receivers.*

Remark 5. *What the zero-structure encoding matrix does, in effect, is implement the standard techniques of rate splitting and linear superposition coding. We prove in Subsection VI-A that this encoding scheme is rate-optimal for combination networks with two public and any number of private receivers. However, this encoding scheme is not in general optimal. We discuss this sub-optimality next and modify the encoding scheme to attain a strictly larger rate region.*

D. An achievable rate-region from pre-encoding and structured linear codes

For combination networks with three or more public receivers (and any number of private receivers), the scheme outlined above turns out to be sub-optimal in general. We discussed one such example in Section II. We now elaborate on that example.

Example 4. Consider the combination network of Fig. 3 where destinations 1, 2, 3 are public receivers and destinations 4, 5, 6 are private receivers. The source wants to communicate a common message $W_1 = []$ of rate $R_1 = 0$ and a private message $W_2 = [w_{2,1}, w_{2,2}]$ of rate $R_2 = 2$. It is clear that the rate pair $(R_1 = 0, R_2 = 2)$ is achievable (just multicast the private message towards the private receivers using, say, random linear network coding). However, one can verify that there is no choice of $\alpha_{\mathcal{S}} \geq 0$, $S \subseteq \{1, 2, 3\}$, which satisfies inequalities (23)-(27) for this rate pair. △

If we were to relax the non-negativity condition on α_ϕ in Example 4, we would obtain $(R_1, R_2) = (0, 2)$ for the following set of parameters $\alpha_{\mathcal{S}}$: $\alpha_\phi = -1$, $\alpha_{\{1\}} = \alpha_{\{2\}} = \alpha_{\{3\}} = 1$, 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 set of parameters. 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, in an optimal code design, to reveal a subspace of dimension one of the private message space to each public receiver (and only that public receiver). The subtlety lies in the fact that such partial (private) information sets that are revealed to the public receiverss $\{1\}$, $\{2\}$ and $\{3\}$ are *not* mutually independent, as message W_2 is of rate 2. The previous scheme does not allow such dependency.

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

$$\begin{bmatrix} X_{\{1\}} \\ X_{\{2\}} \\ X_{\{3\}} \end{bmatrix} = \left[\begin{array}{c|c|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right] \begin{bmatrix} w_{2,1}' \\ w_{2,2}' \\ w_{2,3}' \end{bmatrix}. \tag{29}$$

Notice that this zero-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'. If the pseudo-private message is obtained from a random matrix $\mathbf{P}$, for instance, each private receiver gets to decode the (original) private message W_2 with a positive probability. Therefore, there exists such a pre-encoding/encoding scheme that achieves the rate pair $(0, 2)$.

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

Theorem 1. *The rate pair (R_1, R_2) is achievable if there exists a set of real valued variables α_S, $S \subseteq \mathcal{I}_1$, that satisfy the following inequalities:*

Structural constraints:

$$\alpha_{\mathcal{S}} \geq 0, \qquad \forall \mathcal{S} \subseteq \mathcal{I}_1,\ \mathcal{S} \neq \phi \tag{30}$$

$$R_2 = \sum_{\mathcal{S} \subseteq \mathcal{I}_1} \alpha_{\mathcal{S}}, \tag{31}$$

Decoding constraints at public receivers:

$$R_1 + \sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} \alpha_{\mathcal{S}} \leq \sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} |\mathcal{E}_{\mathcal{S}}|, \qquad \forall i \in \mathcal{I}_1 \tag{32}$$

Decoding constraints at private receivers:

$$R_2 \leq \sum_{\mathcal{S} \in \Lambda} \alpha_{\mathcal{S}} + \sum_{\mathcal{S} \in \Lambda^c} |\mathcal{E}_{\mathcal{S},p}|, \qquad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \textit{ superset saturated}, \ \forall p \in \mathcal{I}_2 \tag{33}$$

$$R_1 + R_2 \leq \sum_{\mathcal{S} \subseteq \mathcal{I}_1} |\mathcal{E}_{\mathcal{S},p}|, \qquad \forall p \in \mathcal{I}_2. \tag{34}$$

Remark 6. *Note that compared to Proposition 1, the non-negativity constraint on α_ϕ is relaxed in Theorem 1.*

Proof: Let (R_1, R_2) be in the rate region of Theorem 1; i.e., there exist parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, that satisfy inequalities (30)-(34). In the following, let $(\alpha_\phi)^- = \min(0, \alpha_\phi)$ and $(\alpha_\phi)^+ = \max(0, \alpha_\phi)$. Furthermore, without loss of generality, we assume that parameters R_1, R_2, $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, are integer valued (see Remark 1).

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 $\mathbf{P} \in {\mathbb{F}_q}^{[R_2 - (\alpha_\phi)^-] \times R_2}$; i.e., we have

$$W_2' = \mathbf{P} W_2. \tag{35}$$

Then, encode messages W_1 and W_2' using a zero-structured matrix with rate split parameters α_S, $S \subseteq \mathcal{I}_1$, omitting the columns corresponding to $S = \phi$ if $\alpha_\phi < 0$. The encoding matrix is, therefore, given as follows:

$$\mathbf{A} = \begin{array}{cl} \begin{array}{ccccc} \xleftrightarrow{R_1} & \xleftrightarrow{\alpha_{\{1,2\}}} & \xleftrightarrow{\alpha_{\{1\}}} & \xleftrightarrow{\alpha_{\{2\}}} & \xleftrightarrow{(\alpha_\phi)^+} \end{array} & \\ \left[\begin{array}{c|c|c|c|c} & & 0 & 0 & 0 \\ \hline & & & 0 & 0 \\ \hline & & 0 & & 0 \\ \hline & & & & \end{array}\right] & \begin{array}{l} \updownarrow |\mathcal{E}_{\{1,2\}}| \\ \updownarrow |\mathcal{E}_{\{1\}}| \\ \updownarrow |\mathcal{E}_{\{2\}}| \\ \updownarrow |\mathcal{E}_{\phi}| \end{array} \end{array} \cdot \ \mathbf{P}' \tag{36}$$

where

$$\mathbf{P}' = \left[\begin{array}{c|c} \mathbf{I}_{R_1\times R_1} & 0 \\ \hline 0 & \mathbf{P} \end{array}\right], \tag{37}$$

and all indeterminates are to be assigned from the finite field $\mathbb{F}_q$.

The conditions for decodability of W_1 at each public receiver $i \in \mathcal{I}_1$ are given by (32), and the conditions for decodability of W_1, W_2 at each private receiver $p \in \mathcal{I}_2$ is given by (33), (34). The proof is similar to the basic zero structured encoding scheme and is sketched in the following.

Let $\mathbf{A}_i$ be the submatrix of $\mathbf{A}$ that constitutes Y_i at receiver i. We have $\mathbf{A}_i = \left[\mathbf{B}^{(i)}|\mathbf{T}^{(i)}\right]\mathbf{P}' = \left[\mathbf{B}^{(i)}|\mathbf{T}^{(i)}\mathbf{P}\right]$. As before, define $\mathbf{L}_1^{(i)}$ to be the largest submatrix of the columns of $\mathbf{T}^{(i)}\mathbf{P}$ that could be made full column rank (over all possible assignments). Define $\mathbf{G}^{(i)}$ to be $\mathbf{G}^{(i)} = \left[\mathbf{B}^{(i)}|\mathbf{L}_1^{(i)}\right]$. From Lemma 5, each receiver i can decode W_1 from (17) if $\mathbf{G}^{(i)}$, as defined above, is full column rank.

Lemma 8. *For each public receiver i, there exists an assignment of $\mathbf{A}$ such that $\mathbf{G}^{(i)}$ is full column rank, provided that*

$$R_1 + \sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} \alpha_{\mathcal{S}} \leq \sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} |\mathcal{E}_{\mathcal{S}}|. \tag{38}$$

Proof: The proof is the same as Lemma 6. One should note that the rank of $\mathbf{T}^{(i)}\mathbf{P}$ is bounded from above by the rank of $\mathbf{T}^{(i)}$ and thus by $\sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} |\mathcal{E}_{\mathcal{S}}| - R_1$. ■

Decodability of W_1 at the private receiver $p \in \mathcal{I}_2$ is similarly guaranteed by (34). In the following, we prove that $\mathbf{T}^{(p)}\mathbf{P}$ could itself be full rank under (33) and conclude decodability of W_2 (in addition to W_1) at the private receivers. Since the variables involved in $\mathbf{B}^{(p)}$ and $\mathbf{T}^{(p)}\mathbf{P}$ are independent, we in effect show that $\mathbf{G}^{(p)}$ could be made full column rank.

Lemma 9. *For each $p \in \mathcal{I}_2$, the matrix $\mathbf{T}^{(p)}\mathbf{P}$ could be made full column rank provided that the conditions in* (33) *are satisfied.*

The proof is similar to the proof of Lemma 2 and we defer it to Appendix E. It remains to argue that for $|\mathbb{F}_q| > K$, and under (32)-(34), all matrices $\mathbf{G}^{(i)}$, $i \in \mathcal{I}$, could be made full rank simultaneously. The proof is based on the sparse zeros lemma and is deferred to Appendix F.

■

Remark 7. *It turns out that the inner-bound of Theorem 1 is tight for combination networks with $m = 3$ (or fewer) public and any number of private receivers. This is discussed in Section VI-B.*

We close this section with an example which shows that the inner-bound of Theorem 1 is not tight, in general, when the number of public receivers exceeds 3.

Example 5. Consider the combination network depicted in Fig. 7 over which a source communicates messages $W_1 = [w_{1,1}]$ and $W_2 = [w_{2,1}, w_{2,2}, w_{2,3}]$ (of rates $R_1 = 1$ and $R_2 = 3$, respectively) to four public and three private receivers. In this example, destinations $1, 2, 3, 4$ are public and destinations $5, 6, 7$ are private receivers. The encoding scheme shown in Fig. 7 proves the achievability of rate pair $(1, 3)$. However, for this rate pair, there is no set of parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq I_1 = \{1, \ldots, 4\}$, for which inequalities (30)-(34) hold, unless the non-negativity constraints in (30) are relaxed. △

Let us look at this example (see Fig. 7) more closely. Each public receiver has three resources available and needs to decode (only) the common message which is of rate $R_1 = 1$. So no more than two dimensions of the private message space could be revealed to any public receiver. For example, look at the resources that are available to public receiver 4. These three resources mimic the same structure of Fig. 3 and demand a certain dependency among their (superposed) private information symbols. More precisely, the superposed private information symbols carried over these resources come from a message space of dimension two (a condition imposed by public receiver 1), and every two out of three of these resources should carry mutually independent private information symbols (a condition imposed by the private receivers). A similar dependency structure is needed among the information symbols on $X_{\{1,2\}}$, $X_{\{1,3\}}$, $X_{\{1,4\}}$, and similarly among $X_{\{1,2\}}$, $X_{\{2,3\}}$, $X_{\{2,4\}}$ and $X_{\{1,3\}}$, $X_{\{2,3\}}$, $X_{\{3,4\}}$. This shows a more involved dependency structure among the revealed partial private information symbols, and explains why our modified encoding scheme of Theorem 1 cannot be optimal for this example. Let us look at the scheme in Fig. 7 which achieves rate $(1, 3)$. We assume $|\mathbb{F}_q| > 2$.

$$X_{\{1,2\}} = w_{1,1} + w_{2,1} \tag{39}$$

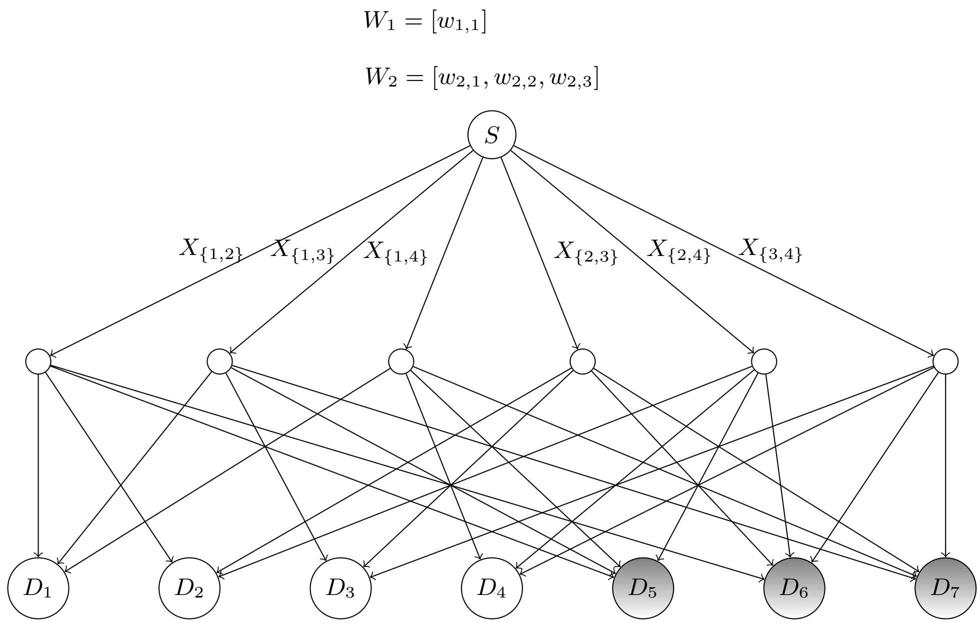


Fig. 7: The innerbound of Theorem 1 is not tight for $m > 3$ public receivers: while the rate pair $(1, 3)$ is not in the rate-region of Theorem 1, assigning $X_{\{1,2\}} = w_{1,1} + w_{2,1}$, $X_{\{1,3\}} = w_{1,1} + w_{2,2}$, $X_{\{1,4\}} = w_{1,1} + w_{2,1} + w_{2,2}$, $X_{\{2,3\}} = w_{1,1} + w_{2,3}$, $X_{\{2,4\}} = w_{1,1} + w_{2,1} + w_{2,3}$ and $X_{\{3,4\}} = w_{1,1} + w_{2,2} - w_{2,3}$ achieves the rate pair $(1, 3)$.

$$X_{\{1,3\}} = w_{1,1} + w_{2,2} \tag{40}$$
$$X_{\{1,4\}} = w_{1,1} + w_{2,1} + w_{2,2} \tag{41}$$
$$X_{\{2,3\}} = w_{1,1} + w_{2,3} \tag{42}$$
$$X_{\{2,4\}} = w_{1,1} + w_{2,1} + w_{2,3} \tag{43}$$
$$X_{\{3,4\}} = w_{1,1} + w_{2,2} - w_{2,3}. \tag{44}$$

This code ensures decodability of $W_1, w_{2,1}, w_{2,2}$ at public receiver 1, decodability of $W_1, w_{2,1}$, $w_{2,3}$ at public receiver 2, decodability of $W_1, w_{2,2}$, $w_{2,3}$ at public receiver 3, decodability of $W_1, w_{2,1} + w_{2,2}, w_{2,1} + w_{2,3}$ at public receiver 4 and decodability of W_1, W_2 at private receivers $5, 6, 7$. The (partial) private information that is revealed to the different subsets of the public receivers is also as follows: no private information is revealed to subsets $\{1, 2, 3, 4\}$, $\{1, 2, 3\}$, $\{1, 2, 4\}$, $\{1, 3, 4\}$, $\{2, 3, 4\}$, the private information revealed to $\{1, 2\}$ is $w_{2,1}$, to $\{1, 3\}$ is $w_{2,2}$, to $\{2, 3\}$ is $w_{2,3}$, to $\{1, 4\}$ is $w_{2,1} + w_{2,2}$, to $\{2, 4\}$ is $w_{2,1} + w_{2,3}$, to $\{3, 4\}$ is $w_{2,2} - w_{2,3}$, and finally no private information is revealed to $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$. Now, it becomes clearer that the dependency structure that is needed among the partial private information may, in general, be more involved than is allowed by our simple pre-encoding technique.

In the next section, we develop a simple block Markov encoding scheme to tackle Example 5, and derive a new achievable scheme for the general problem.

V. A Block Markov Encoding Scheme

A. Main idea

We saw that the difficulty in the code design stems mainly from the following tradeoff: On one hand, private receivers require all the public and private information symbols and therefore prefer to receive mutually independent information over their resources. On the other hand, each public receiver requires that its received encoded symbols do not depend on "too many" private information symbols. This imposes certain dependencies among the encoded symbols of the public receivers' resources .

The main idea in this section is to capture these dependencies over sequential blocks, rather than capturing it through the structure of the one-time (one-block) code. For this, we use a block Markov encoding scheme. We start with an examples where both previous schemes were sub-optimal and we show the optimality of the block Markov encoding scheme for it.

Example 6. Consider the combination network in Fig. 7. We saw in Example 5 that the rate pair $(R_1 = 1, R_2 = 3)$ was not achievable by the zero-structured linear code, even after employing the random pre-encoder in the the modified scheme. In this example, we achieve the rate pair $(R_1 = 1, R_2 = 3)$ through a block Markov encoding scheme, and hence, show that block Markov encoding could perform strictly better. Let us first extend the combination network by adding one extra resource to the set $\mathcal{E}_{\{4\}}$, and connecting it to all the private receivers (see Fig. 8). One can verify that a larger rate pair $(R_1 = 1, R_2' = 4)$ is

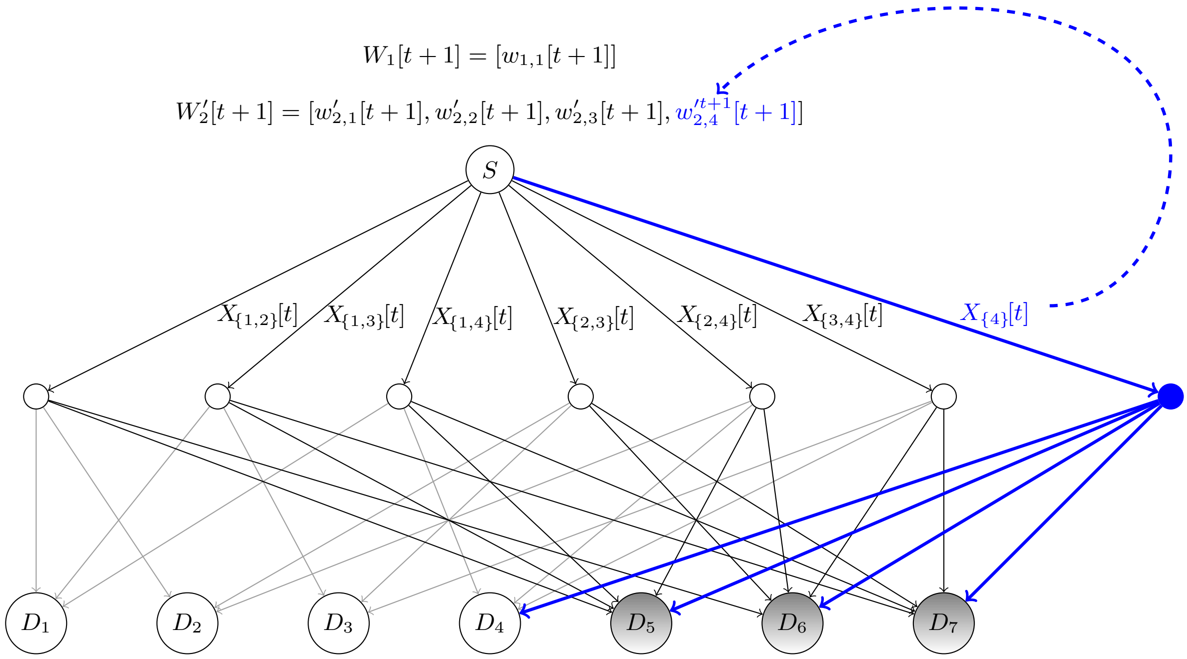


Fig. 8: The extended combination network of Example 6. A block Markov encoding scheme allows achievability of the rate pair $(1, 3)$ over the original combination network. At time $t + 1$, information symbol $w'_{2,4}[t + 1]$ contains the information of symbol $X_{\{4\}}[t]$.

achievable over this extended combination network, using a basic zero-structured linear code. One such code design is given in the following. Let message $W'_2 = [w'_{2,1}, w'_{2,2}, w'_{2,3}, w'_{2,4}]$ be the private message of the larger rate ($R'_2 = 4$) which is to be communicated over the extended combination network, and let $X_{\{1,2\}}$, $X_{\{1,3\}}$, $X_{\{1,4\}}$, $X_{\{2,3\}}$, $X_{\{2,4\}}$, $X_{\{3,4\}}$, $X_{\{4\}}$ be the symbols that are sent over the extended combination network. The encoding is described below (we assume that $\mathbb{F}_q$ has a characteristic larger than 2):

$$\begin{aligned} X_{\{1,2\}} &= w_{1,1} + w'_{2,3} & X_{\{2,3\}} &= w_{1,1} + 2w'_{2,3} \\ X_{\{1,3\}} &= 2w_{1,1} + w'_{2,3} & X_{\{2,4\}} &= w_{1,1} + w'_{2,2} \\ X_{\{1,4\}} &= w_{1,1} + w'_{2,1} & X_{\{3,4\}} &= w_{1,1} + w'_{2,4} \\ X_{\{4\}} &= w_{1,1} + w'_{2,1} + w'_{2,2} + w'_{2,4}. \end{aligned} \tag{45}$$

Since the resource edge in $\mathcal{E}_{\{4\}}$ is a virtual resource, we aim to emulate it through a block Markov encoding scheme. Using the code design of (45), receiver 4 may also decode, besides the common message, three private information symbols ($w'_{2,1}$, $w'_{2,2}$, $w'_{2,4}$). Since all these three symbols are decodable at receiver 4 and all the private receivers, any of them could be used to emulate the virtual resource in $\mathcal{E}_{\{4\}}$.

More precisely, consider communication over n transmission blocks, and let $(W_1[t], W'_2[t])$ be the message pair that is being encoded in block $t \in \{1, \ldots, n\}$. In the t^{th} block, encoding is done as suggested by the code in (45). Nevertheless, to provide receiver 4 and the private receivers with the information of $X_{\{4\}}[t]$ (as promised by the virtual resource in $\mathcal{E}_{\{4\}}$), we use information symbol $w'_{2,4}[t + 1]$ in the next block, to convey $X_{\{4\}}[t]$. Since this symbol is ensured to be decoded at receiver 4 and the private receivers, it indeed emulates $\mathcal{E}_{\{4\}}$. In the n^{th} block, we simply encode $X_{\{4\}}[n - 1]$ and directly communicate it with receiver 4 and the private receivers. Upon receiving all the n blocks, the receivers perform backward decoding [36].

So in n transmissions, we may send $n-1$ symbols of W_1 and $3(n-1)+1$ new symbols of W_2 over the original combination network; i.e., for $n \to \infty$, we can achieve the rate-pair $(1, 3)$.

Note that public receivers each have four resources available and therefore rate pair $(1, 3)$ is an optimal sum-rate point.

△

B. *Block Markov encoding scheme: an achievable region*

In both examples 3 and 6, the achievability is through a block Markov encoding scheme, and the construction of it is explained with the help of an *extended combination network*. Before further explaining this construction, let us clarify what we mean by an extended combination network.

Definition 3 (Extended combination network). *An extended combination network is formed from the original combination network by adding some extra nodes, called virtual nodes, to the intermediate layer. The source is connected to all of the* *virtual nodes through edges that we call virtual resources. Each virtual resource is connected to a subset of the receivers which we refer to as the end-destinations of that virtual resource. This subset is chosen, depending on the structure of the original combination network and the target rate pair, through an optimization problem that we will address later in this section.*

The idea behind extending the combination network is as follows. The encoding is such that in order to decode the common and private messages in block t, each receiver may need the information that it will decode in block $t+1$ (recall that receivers perform backward decoding). So, the source wants to design both its outgoing symbols in block t and the side information that the receiver will have in block $t+1$. This is captured by designing a code over an extended combination network, where the virtual resources play, in a sense, the role of the side information.

Over the extended combination networks, we will design a *general multicast code* (as opposed to one for nested message sets). We will only consider multicast codes based on basic linear superposition coding to emulate the virtual resources (see Remark 4). We further elaborate on this in the following.

Definition 4 (Emulatable virtual resources)**.** *Given an extended combination network and a general multicast code over it, a virtual resource v is called emulatable if the multicast code allows reliable communication at a rate of at least* 1 *to all end-destinations of that virtual resource (over the extended combination network). We call a set of virtual resources emulatable if they are all simultaneously emulatable.*

We now outline the steps in devising a block Markov encoding scheme for this problem.

1) Add a set of virtual resources to the original combination network to form an extended combination network.
2) Design a general (as opposed to one for nested message sets) multicast code over the extended combination network such that all the virtual resources are emulatable.
3) Use the multicast code to make all the virtual resources emulatable. More precisely, use the information symbols in block $t+1$ to also convey the information carried on the virtual resources in block t. Use the remaining information symbols to communicate the common and private information symbols.

An achievable rate-region could then be found by optimizing over the virtual resources and the multicast code.

Formulating this problem in its full generality is not the goal of this section. We instead aim to take a simple block Markov encoding scheme, show its advantages in optimal code design, and characterize a region achievable by it. To this end, we confine ourselves to the following two assumptions: (i) the virtual resources that we introduce are connected to all private receivers and different subsets of the public receivers, and (ii) the multicast code that we design over the extended combination network is a basic linear superposition code along the lines of the codes in Section IV-C.

In order to devise our simple block Markov scheme, we first create an extended combination network by adding for every $\mathcal{S} \subseteq \mathcal{I}_1$, $\beta_{\mathcal{S}}$ many virtual resources which are connected to all the private receivers and all the public receivers in $\mathcal{S} \subseteq \mathcal{I}_1$ (and only those). We denote this subset of the virtual resources by $\mathcal{V}_{\mathcal{S}}$.

Over this extended combination network, we then design a (more general) multicast code. We say that a multicast code achieves rate tuple $(R_1, \alpha_{\{1,\ldots,m\}}, \ldots, \alpha_{\phi})$ over the extended combination network, if it reliably communicates a message of rate R_1 to all receivers, and independent messages of rates $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, to all public receivers in $\mathcal{S}$ and all private receivers. To design such a multicast code, we use a basic linear superposition code (through a zero-structured multicast code design). It turns out that the rate tuple $(R_1, \alpha_{\{1,\ldots,m\}}, \ldots, \alpha_{\phi})$ is achievable if the following inequalities are satisfied (see Remark 3):

Decodability constraints at public receivers:

$$\sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} \alpha_{\mathcal{S}} \leq \sum_{\mathcal{S}\in\Lambda} \alpha_{\mathcal{S}} + \sum_{\substack{\mathcal{S}\in\Lambda^c\\ \mathcal{S}\ni i}} \left(|\mathcal{E}_{\mathcal{S}}| + \beta_{\mathcal{S}}\right), \quad \forall \Lambda \subseteq \{\{i\}\star\} \text{ superset saturated, } \forall i \in \mathcal{I}_1 \tag{46}$$

$$R_1 + \sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} \alpha_{\mathcal{S}} \leq \sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} \left(|\mathcal{E}_{\mathcal{S}}| + \beta_{\mathcal{S}}\right), \ \forall i \in \mathcal{I}_1 \tag{47}$$

Decodability constraints at private receivers:

$$R_2' \leq \sum_{\mathcal{S}\in\Lambda} \alpha_{\mathcal{S}} + \sum_{\mathcal{S}\in\Lambda^c} \left(|\mathcal{E}_{\mathcal{S},p}| + \beta_{\mathcal{S}}\right), \quad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \text{ superset saturated, } \forall p \in \mathcal{I}_2 \tag{48}$$

$$R_1 + R_2' \leq \sum_{\mathcal{S}\subseteq\mathcal{I}_1} \left(|\mathcal{E}_{\mathcal{S},p}| + \beta_{\mathcal{S}}\right), \ \forall p \in \mathcal{I}_2. \tag{49}$$

Now, given such a multicast code, we find conditions for the virtual resources to be emulatable. The proof is relegated to Appendix G.

Lemma 10. *Given an extended combination network with $\beta_{\mathcal{S}}$ virtual resources $\mathcal{V}_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, and a multicast code design that achieves rate tuple $(R_1, \alpha_{\{1,\ldots,m\}}, \ldots, \alpha_{\phi})$, all virtual resources are emulatable provided that inequalities in* (50) *hold.*

$$\sum_{\mathcal{S}\in\Lambda} \beta_{\mathcal{S}} \leq \sum_{\mathcal{S}\in\Lambda} \alpha_{\mathcal{S}}, \quad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \textit{superset saturated.} \tag{50}$$

It remains to calculate the common and private rates that are achievable (over the original combination network) when we use our simple block Markov encoding scheme. To do so, we disregard the information symbols that are used to emulate the virtual resources, for they bring redundant information, and characterize the remaining rate of the common and private information symbols. In the above scheme, this is simply $(R_1, R_2' - \sum_{\mathcal{S}\subseteq\mathcal{I}_1} \beta_{\mathcal{S}})$, where $R_2' = \sum_{\mathcal{S}\subseteq\mathcal{I}_1} \alpha_{\mathcal{S}}$ and the real valued parameters $\alpha_{\mathcal{S}}, \beta_{\mathcal{S}}$ satisfy inequalities (46)-(50) and the following non-negativity constraints:

$$\alpha_{\mathcal{S}} \geq 0, \tag{51}$$

$$\beta_{\mathcal{S}} \geq 0. \tag{52}$$

To simplify the representation, we define $\gamma_{\mathcal{S}} = \alpha_{\mathcal{S}} - \beta_{\mathcal{S}},\ \forall \mathcal{S} \subseteq \mathcal{I}_1$, and then eliminate α's and β's from all inequalities involved. We thus have the following theorem.

Theorem 2. *The rate pair (R_1, R_2) is achievable if there exist parameters $\gamma_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, such that they satisfy the following inequalities:*

$$\sum_{\mathcal{S}\in\Lambda} \gamma_{\mathcal{S}} \geq 0, \qquad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \textit{ superset saturated} \tag{53}$$

$$R_2 = \sum_{\mathcal{S}\subseteq\mathcal{I}_1} \gamma_{\mathcal{S}}, \tag{54}$$

Decodability constraints at public receivers:

$$\sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} \gamma_{\mathcal{S}} \leq \sum_{\mathcal{S}\in\Lambda} \gamma_{\mathcal{S}} + \sum_{\substack{\mathcal{S}\in\Lambda^c\\ \mathcal{S}\ni i}} |\mathcal{E}_{\mathcal{S}}|, \quad \forall \Lambda \subseteq \{\{i\}\star\} \textit{ superset saturated}, \ \forall i \in \mathcal{I}_1 \tag{55}$$

$$R_1 + \sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} \gamma_{\mathcal{S}} \leq \sum_{\substack{\mathcal{S}\subseteq\mathcal{I}_1\\ \mathcal{S}\ni i}} |\mathcal{E}_{\mathcal{S}}|, \quad \forall i \in \mathcal{I}_1 \tag{56}$$

Decodability constraints at private receivers:

$$R_2 \leq \sum_{\mathcal{S}\in\Lambda} \gamma_{\mathcal{S}} + \sum_{\mathcal{S}\in\Lambda^c} |\mathcal{E}_{\mathcal{S},p}|, \quad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \textit{ superset saturated}, \ \forall p \in \mathcal{I}_2 \tag{57}$$

$$R_1 + R_2 \leq \sum_{\mathcal{S}\subseteq\mathcal{I}_1} |\mathcal{E}_{\mathcal{S},p}|, \quad \forall p \in \mathcal{I}_2. \tag{58}$$

Comparing the rate-regions in Theorem 1 and Theorem 2, we see that the former has a more relaxed set of inequalities in (53) while the latter is more relaxed in inequalities (55). Although the two regions are not comparable in general, it turns out that for $m \leq 3$, the two rate-regions coincide and characterize the capacity region (see Theorem 4 and Theorem 5). Furthermore, the combination network in Fig. 7 serves as an instance where the rate-region in Theorem 2 includes rate pairs that are not included in the region of Theorem 1 (see Example 5 and Example 6).

Fig. 9 plots the rate-regions of Theorem 1 and Theorem 2 for the network of Fig. 7. The grey region is the region of Theorem 1 (i.e., is achievable using pre-encoding, rate-splitting, and linear superposition coding) and the red shaded region is the region of Theorem 2 (i.e., is achievable using the above block Markov encoding scheme). Note that in this example, the proposed block Markov encoding scheme strictly outperforms our previous schemes.

Remark 8. *It remains open whether the rate-region of Theorem 2 always includes the rate-region of Theorem 1, or not. We conjecture that this is true.*

VI. Optimality Results

In this section, we prove our optimality results. More precisely, we prove optimality of the zero-structured encoding scheme of Subsection IV-C when $m = 2$, optimality of the structured linear code with pre-encoding discussed in Subsection IV-D when $m = 3$ (or fewer), and optimality of the block Markov encoding of Section V when $m = 3$ (or fewer). This is summarized in the following theorems.

Theorem 3. *Over a combination network with two public and any number of private receivers, the rate pair (R_1, R_2) is achievable if and only if it lies in the rate-region of Proposition 1.*

Theorem 4. *Over a combination network with three (or fewer) public and any number of private receivers, the rate pair (R_1, R_2) is achievable if and only if it lies in the rate-region of Theorem 1.*

Theorem 5. *Over a combination network with three (or fewer) public and any number of private receivers, the rate pair (R_1, R_2) is achievable if and only if it lies in the rate-region of Theorem 2.*

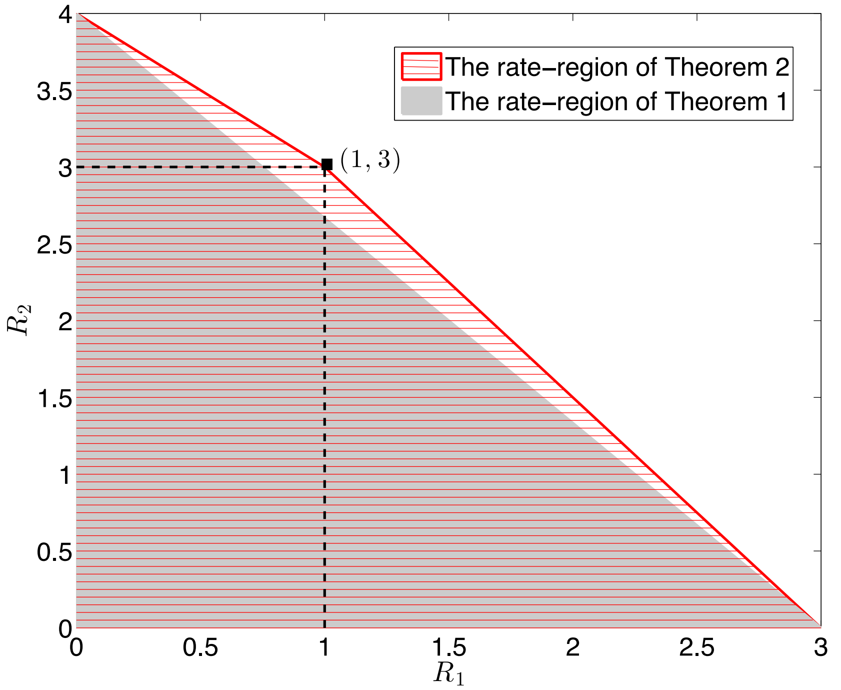


Fig. 9: The rate-regions of Theorems 1 and 2 for the combination network in Fig. 7

A. *Explicit projection of the polyhedron: proof of Theorem 3*

The achievability part of Proposition 1 was discussed in Section IV-C. We prove the converse here. Using Fourier-Motzkin elimination method, we first eliminate all parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, in the rate-region of Proposition 1 and we obtain the following region (recall that $\mathcal{I}_1 = \{1,2\}$ and $\mathcal{I}_2 = \{3,\dots,K\}$):

$$R_1 \leq \min\left(|\mathcal{E}_{\{1\}}| + |\mathcal{E}_{\{1,2\}}|, |\mathcal{E}_{\{2\}}| + |\mathcal{E}_{\{1,2\}}|\right) \tag{59}$$

$$R_1 + R_2 \leq \min_{p\in\mathcal{I}_2}\left\{|\mathcal{E}_{\phi,p}| + |\mathcal{E}_{\{1\},p}| + |\mathcal{E}_{\{2\},p}| + |\mathcal{E}_{\{1,2\},p}|\right\} \tag{60}$$

$$2R_1 + R_2 \leq \min_{p\in\mathcal{I}_2}\left\{|\mathcal{E}_{\{1\}}| + 2|\mathcal{E}_{\{1,2\}}| + |\mathcal{E}_{\{2\}}| + |\mathcal{E}_{\phi,p}|\right\}. \tag{61}$$

Note that the right hand side (RHS) of (59) is the minimum of the min-cuts to the two public receivers, and the RHS of (60) is the minimum of the min-cuts to the private receivers.

We now prove the converse; i.e., any achievable rate pair satisfies the three inequalities above. The proof is similar to [29]. Inequalities (59) and (60) are immediate (using cut-set bounds) and are easy to derive. Inequality (61) is, however, not immediate and we prove it in the following. Assume communication over blocks of length n. The rate R_2 is bounded, for each private receiver $p \in I_2$ and any $\epsilon > 0$, as follows:

$$\begin{aligned}
nR_2 =& H(W_2|W_1)\\
\leq& H(W_2|W_1) - H(W_2|W_1Y_p^n) + H(W_2|W_1Y_p^n)\\
\overset{(a)}{\leq}& I(W_2;Y_p^n|W_1) + n\epsilon\\
=& H(Y_p^n|W_1) + n\epsilon\\
\overset{(b)}{\leq}& H(X^n_{\{\phi,\{1\},\{2\}\{1,2\}\},p}X^n_{\{\{1\},\{2\},\{1,2\}\}}|W_1) + n\epsilon\\
\overset{(c)}{\leq}& H(X^n_{\{\{1\},\{1,2\}\}}|W_1) + H(X^n_{\{\{2\},\{1,2\}\}}|W_1) + H(X^n_{\{\phi,\{1\},\{2\}\{1,2\}\},p}|X^n_{\{\{1\},\{2\},\{1,2\}\}}W_1) + n\epsilon\\
\overset{(d)}{\leq}& H(X^n_{\{\{1\},\{1,2\}\}}) + H(X^n_{\{\{2\},\{1,2\}\}}) - 2nR_1 + H(X^n_{\{\phi,\{1\},\{2\}\{1,2\}\},p}|X^n_{\{\{1\},\{2\},\{1,2\}\}}W_1) + 3n\epsilon\\
\overset{(e)}{\leq}& H(X^n_{\{\{1\},\{1,2\}\}}) + H(X^n_{\{\{2\},\{1,2\}\}}) - 2nR_1 + H(X^n_{\phi,p}) + 3n\epsilon\\
\overset{(f)}{\leq}& n(|\mathcal{E}_{\{1\}}| + |\mathcal{E}_{\{1,2\}}|) + n(|\mathcal{E}_{\{2\}}| + |\mathcal{E}_{\{1,2\}}|) - 2nR_1 + n(|\mathcal{E}_{\phi,p}|) + 3n\epsilon.
\end{aligned}$$

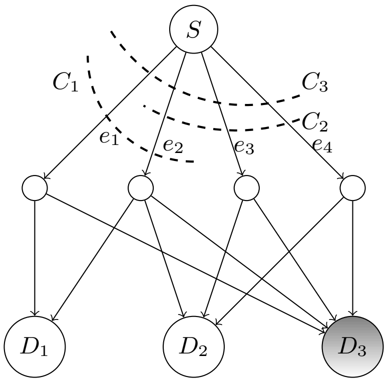


Fig. 10: The rate-region in Theorem 3 evaluates to $R_1 \leq 2$, $R_1 + R_2 \leq 4$ and $2R_1 + R_2 \leq 5$.

In the above chain of inequalities, step (a) follows from Fano's inequality. Step (b) follows because the received signal Y_p^n is given by all symbols in $X^n_{\{\phi,\{1\},\{2\}\{1,2\}\},p}$ and we further add all symbols $X^n_{\{1,2\}}$,$X^n_{\{1\}}$,$X^n_{\{2\}}$. Step (c) follows from sub-modularity of entropy. Step (d) is a result of (62)-(64), below, where (64) is due to Fano's inequality (W_1 should be recoverable with arbitrarily small error probability from $X^n_{\{\{1\},\{1,2\}\}}$).

$$H(X^n_{\{\{1\},\{1,2\}\}}|W_1) = H(X^n_{\{\{1\},\{1,2\}\}}W_1) - nR_1 \tag{62}$$

$$= H(X^n_{\{\{1\},\{1,2\}\}}) + H(W_1|X^n_{\{\{1\},\{1,2\}\}}) - nR_1 \tag{63}$$

$$\leq H(X^n_{\{\{1\},\{1,2\}\}}) + n\epsilon - nR_1. \tag{64}$$

Similarly, $H(X^n_{\{\{2\},\{1,2\}\}}|W_1) \leq H(X^n_{\{\{2\},\{1,2\}\}}) - nR_1 + n\epsilon$. Step (e) follows by the fact that for any $\mathcal{S} \subseteq \mathcal{I}_1$, $X^n_{\mathcal{S},p}$ is contained in $X^n_{\mathcal{S}}$ (by definition) and that conditioning reduces the entropy. Finally, step (f) follows because each entropy term $H(X^n_{\mathcal{S}})$ is bounded by $n|\mathcal{S}|$ (remember that all rates are written in units of $\log_2|\mathbb{F}_q|$ bits).

We discuss an intuitive explanation of this outer-bound via the example in Fig. 10. Clearly, the common message W_1 could be reliably communicated with receiver 1 (which has a min-cut equal to 2) only if $R_1 \leq 2$. Similarly, $R_1 \leq 3$ (according to the min-cut to receiver 2) and $R_1 + R_2 \leq 4$ (according to the min-cut to receiver 3). Now, consider the three cuts C_1, C_2, C_3 shown in Fig. 10. How much information about message W_2 could be carried over edges e_1, e_2, e_3, e_4, altogether? Edges of the cut $\{e_1, e_2\}$ can carry at most $2 - R_1$ units of information about message W_2, for they have a total capacity of 2 and have to also ensure decodability of message W_1 (which is of rate R_1). Similarly, edges of the cut $\{e_2, e_3, e_4\}$ can carry at most $3 - R_1$ units of information about message W_2. So altogether, these edges cannot carry more than $2 - R_1 + 3 - R_1$ bits of information about message W_2; i.e., $R_2 \leq 5 - 2R_1$, or $2R_1 + R_2 \leq 5$.

B. Sub-modularity of the entropy function: proof of Theorem 4 and Theorem 5

While it was not difficult to eliminate all parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, from the rate-region characterization for $m = 2$, this becomes a tedious task when the number of public receivers increases. In this section, we prove Theorem 4 by showing an outer-bound on the rate-region that matches the inner-bound of Theorem 1 when $m = 3$. We bypass the issue of explicitly eliminating all parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, by first proving an outer-bound which looks *similar* to the inner-bound and then using sub-modularity of entropy to conclude the proof. The same converse technique will be used to prove Theorem 5. Together, Theorem 4 and Theorem 5 allow us to conclude that the two regions in Theorems 1 and 2 coincide for $m = 3$ public (and any number of private) receivers and characterize the capacity. We start with an example.

Example 7. Consider the combination network of Fig. 11 where receivers $1, 2, 3$ are public and receivers $4, 5$ are private receivers. We ask if the rate pair $(R_1 = 1, R_2 = 2)$ is achievable over this network. To answer this question, let us first see if this rate pair is within the inner-bound of Theorem 1. By solving the feasibility problem defined in inequalities (30)-(34), using Fourier-Motzkin elimination method, we obtain the following inner-bound inequality, and conclude that the rate pair $(1, 2)$ is not within the inner-bound of Theorem 1.

$$4R_1 + 2R_2 \leq 7. \tag{65}$$

Once this is established, we can also answer the following question: what linear combination of inequalities in (30)-(34) gave rise to the inner-bound inequality in (65)? The answer is that summing two copies of (32) (for $i = 1$), one copy of (32) (for $i = 2$), one copy of (32) (for $i = 3$), one copy of (33) (for $\Lambda = \{\{1\}\star, \{2,3\}\star\}$, $p = 4$), one copy of (33) (for $\Lambda = \{\{1\}\star, \{2\}\star, \{3\}\star\}$, $p = 5$), and finally one copy of the non-negativity constraint in (30) (for $\mathcal{S} = \{1, 2, 3\}$) gives rise to $4R_1 + 2R_2 \leq 7$.

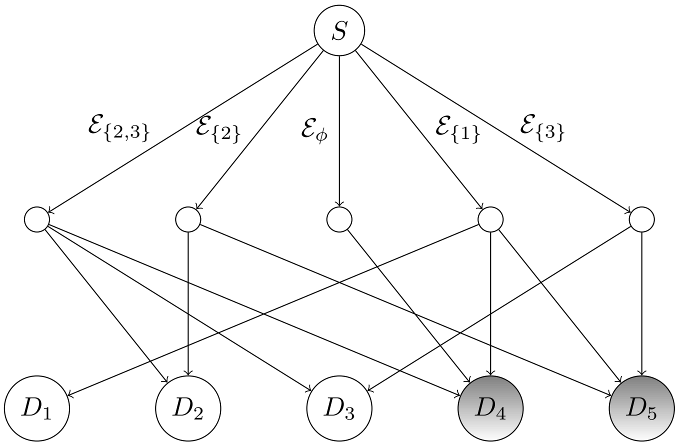


Fig. 11: Is rate pair $(1, 2)$ achievable over this combination network?

We now write the following upper-bounds on R_1 and R_2 (which we prove in detail in Section VI-B2). Notice the similarity of each outer-bound constraint in (66)-(71) to an inner-bound constraint that played a role in the derivation of $4R_1 + 2R_2 \leq 7$.

$$R_1 + \frac{1}{n}H(X^n_{\{\{1\}\star\}}|W_1) \leq 1 \tag{66}$$

$$R_1 + \frac{1}{n}H(X^n_{\{\{2\}\star\}}|W_1) \leq 2 \tag{67}$$

$$R_1 + \frac{1}{n}H(X^n_{\{\{3\}\star\}}|W_1) \leq 2 \tag{68}$$

$$R_2 \leq \frac{1}{n}H(X^n_{\{\{1\}\star,\{2,3\}\star\}}|W_1) + 1 \tag{69}$$

$$R_2 \leq \frac{1}{n}H(X^n_{\{\{1\}\star,\{2\}\star,\{3\}\star\}}|W_1) \tag{70}$$

$$0 \leq \frac{1}{n}H(X^n_{\{1,2,3\}}|W_1). \tag{71}$$

Take two copies of (66) and one copy each of (67)-(71) to yield an outer-bound inequality of the following form.

$$\begin{aligned} & 4R_1 + 2R_2 \\ \leq & 7 - \frac{1}{n}\begin{pmatrix} 2H(X^n_{\{1\}}|W_1) + H(X^n_{\{2\}}X^n_{\{2,3\}}|W_1) + H(X^n_{\{2,3\}}X^n_{\{3\}}|W_1) \\ -H(X^n_{\{1\}}X^n_{\{2,3\}}|W_1) - H(X^n_{\{1\}}X^n_{\{3\}}X^n_{\{2,3\}}X^n_{\{2\}}|W_1) \end{pmatrix} && (72) \\ \overset{(a)}{\leq} & 7 && (73) \end{aligned}$$

where (a) holds by sub-modularity of entropy. △

The intuition from Example 7 gives us a method to prove the converse of Theorem 1 (for $m = 3$). Before presenting the proof, let us introduce a few techniques, as it may not be clear how sub-modularity could be used in full generality.

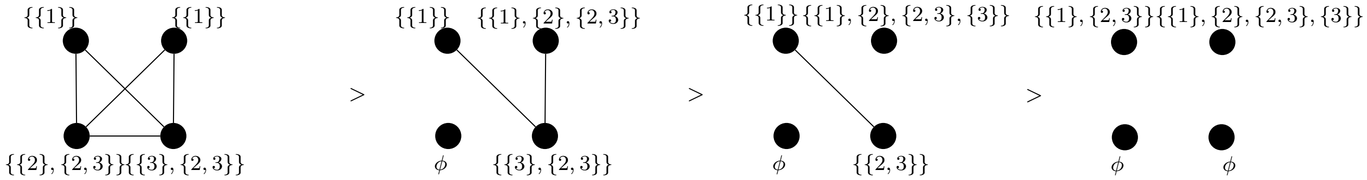
1) Sub-modularity lemmas: We adopt some definitions and results from [38] and prove a lemma that takes a central role in the converse proof in Section VI-B2.

Let $[\mathbf{F}]$ be a family of multi-sets[3] of subsets of $\{s_1, \dots, s_N\}$. Given a multi-set $\mathbf{\Gamma} = [\Gamma_1, \dots, \Gamma_l]$ (where $\Gamma_i \subseteq \{s_1, \dots, s_N\}$, $i = 1, \dots, l$), let $\mathbf{\Gamma}'$ be a multi-set obtained from $\mathbf{\Gamma}$ by replacing Γ_i and Γ_j by $\Gamma_i \cap \Gamma_j$ and $\Gamma_i \cup \Gamma_j$ for some $i, j \in \{1, \dots, l\}$, $i \neq j$. The multi-set $\mathbf{\Gamma}'$ is then said to be an *elementary compression* of $\mathbf{\Gamma}$. The elementary compression is, in particular, *non-trivial* if neither $\Gamma_i \subseteq \Gamma_j$ nor $\Gamma_j \subseteq \Gamma_i$. A sequence of elementary compressions gives a *compression*. A partial order $\geq$ is defined over $[\mathbf{F}]$ as follows. $\mathbf{\Gamma} \geq \mathbf{\Lambda}$ if $\mathbf{\Lambda}$ is a compression of $\mathbf{\Gamma}$ (equality if and only if the compression is composed of all trivial elementary compressions). A simple consequence of the sub-modularity of the entropy function is the following lemma [38, Theorem 5].

Lemma 11. *[38, Theorem 5] Let $X = (X_{s_i})_1^N$ be a sequence of random variables with $H(X)$ finite and let $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ be finite multi-sets of subsets of $\{s_1, \dots, s_N\}$ such that $\mathbf{\Gamma} \geq \mathbf{\Lambda}$. Then*

$$\sum_{\Gamma \in \mathbf{\Gamma}} H(X_\Gamma) \geq \sum_{\Lambda \in \mathbf{\Lambda}} H(X_\Lambda).$$

[3] Multi-set is a generalization of the notion of a set in which members are allowed to appear more than once.



(a) Graph $G_{\mathbf{\Gamma}}$ (b) Graph $G_{\mathbf{\Gamma}'}$ (c) Graph $G_{\mathbf{\Gamma}''}$ (d) Graph $G_{\mathbf{\Lambda}}$

Fig. 12: Graphs associated with multi-sets $\mathbf{\Gamma}$, $\mathbf{\Gamma}'$, $\mathbf{\Gamma}''$, $\mathbf{\Lambda}$ obtained through the compression that is performed in inequalities (74)-(77).

For our converse, we consider the family of multi-sets of subsets of $2^{\mathcal{I}_1}$ where $\mathcal{I}_1 = \{1, 2, 3\}$. We denote multi-sets by bold greek capital letters (e.g., $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$), subsets of $2^{\mathcal{I}_1}$ by greek capital letters (e.g., Γ_i, Σ and Λ), and elements of $2^{\mathcal{I}_1}$ by calligraphic capital letters (e.g., $\mathcal{S}$ and $\mathcal{T}$). Over a family of multi-sets of subsets of $2^{\mathcal{I}_1}$, we define *multi-sets of saturated pattern* and *multi-sets of standard pattern* as follows.

Definition 5 (Multi-sets of saturated pattern)**.** *A multi-set (of subsets of $2^{\mathcal{I}_1}$) is said to be of (superset) saturated pattern if all its elements are superset saturated. E.g., for $\mathcal{I}_1 = \{1, 2, 3\}$, we have that multi-sets $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}]$ and $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}, \{\{2, 3\}, \{1, 2, 3\}\}]$ are both of saturated pattern, but not $[\{\{2\}, \{1, 2\}, \{1, 2, 3\}\}]$ (since its only element is not superset saturated as $\{2, 3\}$ is missing from it) or $[\{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}, \{\{1\}, \{1, 2\}\}]$ (since $\{\{1\}, \{1, 2\}\}$ is not superset saturated).*

Definition 6 (Multi-sets of standard pattern)**.** *A multi-set (of subsets of $2^{\mathcal{I}_1}$) is said to be of standard pattern if its elements are all of the form $\{\mathcal{S} \subseteq \mathcal{I}_1 : \mathcal{S} \ni i\}$, for some $i \in \mathcal{I}_1$. E.g., both multi-sets $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}]$ and $[\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}, \{\{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}]$ are of standard pattern, but not multi-sets $[\{\{1, 2\}, \{1, 2, 3\}\}]$ or $[\{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}]$.*

Definition 7 (Balanced pairs of multi-sets)**.** *We say that multi-sets $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ are a balanced pair if $\sum_{\Gamma \in \mathbf{\Gamma}} \mathbf{1}_{\mathcal{S} \in \Gamma} = \sum_{\Lambda \in \mathbf{\Lambda}} \mathbf{1}_{\mathcal{S} \in \Lambda}$, for all sets $\mathcal{S} \in 2^{\mathcal{I}_1}$.*

Remark 9. *One observes that (i) multi-sets of standard pattern are also of saturated pattern, (ii) the set of all multi-sets of saturated pattern is closed under compression, (iii) if a multi-set $\mathbf{\Lambda}$ is a compression of a multi-set $\mathbf{\Gamma}$, then they are balanced, and (iv) two multi-sets of standard pattern are balanced if and only if they are equal.*

Let us look at step (a) in inequality (73) in this formulation. Consider the family of multi-sets of subsets of $2^{\{1,2,3\}}$, and in particular, the multi-set $\mathbf{\Gamma} = [\{\{1\}\}, \{\{1\}\}, \{\{2\}, \{2, 3\}\}, \{\{3\}, \{2, 3\}\}]$. After the following non-trivial elementary compressions, the multi-set $\mathbf{\Lambda} = [\{\{1\}, \{2, 3\}\}, \{\{1\}, \{2\}, \{3\}, \{2, 3\}\}]$ is obtained.

$$\begin{aligned} \mathbf{\Gamma} =& [\{\{1\}\}, \{\{1\}\}, \{\{2\}, \{2, 3\}\}, \{\{3\}, \{2, 3\}\}] && (74)\\ \geq& [\{\{1\}\}, \{\{1\}, \{2\}, \{2, 3\}\}, \{\{3\}, \{2, 3\}\}] =: \mathbf{\Gamma}' && (75)\\ \geq& [\{\{1\}\}, \{\{1\}, \{2\}, \{3\}, \{2, 3\}\}, \{\{2, 3\}\}] =: \mathbf{\Gamma}'' && (76)\\ \geq& [\{\{1\}, \{2, 3\}\}, \{\{1\}, \{2\}, \{3\}, \{2, 3\}\}] =: \mathbf{\Lambda}. && (77) \end{aligned}$$

Therefore, $\mathbf{\Gamma} \geq \mathbf{\Lambda}$ and by Lemma 11, $\sum_{\Gamma \in \mathbf{\Gamma}} H(X_\Gamma^n | W_1) \geq \sum_{\Lambda \in \mathbf{\Lambda}} H(X_\Lambda^n | W_1)$. Thus, step (a) of inequality (73) follows.

Here, we develop an alternative visual tool. Associate a graph $G_{\mathbf{\Gamma}}$ to every multi-set $\mathbf{\Gamma}$. The graph is formed as follows. Each node of the graph represents one set in $\mathbf{\Gamma}$, and is labeled by it. Two nodes are connected by an edge if and only if neither is a subset of the other. Each time an elementary compression is performed on the multi-set $\mathbf{\Gamma}$, a compressed multi-set $\mathbf{\Gamma}'$ (with a new graph associated with it) is created. E.g., graphs associated with multi-sets $\mathbf{\Gamma}$, $\mathbf{\Gamma}'$, $\mathbf{\Gamma}''$, and $\mathbf{\Lambda}$ (which are all defined in inequalities (74)-(77)) are shown in Fig. 12.

For such (associated) graphs, we prove that compression reduces the total number of edges in the graphs.

Lemma 12. *Let $G_{\mathbf{\Gamma}}$ denote the graph associated with a multi-set $\mathbf{\Gamma}$ and $G_{\mathbf{\Lambda}}$ denote the graph associated with a multi-set $\mathbf{\Lambda}$. Provided that $\mathbf{\Lambda} < \mathbf{\Gamma}$, the total number of edges in $G_{\mathbf{\Lambda}}$ is strictly smaller than that of $G_{\mathbf{\Gamma}}$.*

Proof: We prove that a non-trivial elementary compression over $\mathbf{\Gamma}$ strictly reduces the total number of edges in its associated graph. Assume that a non-trivial elementary compression over $\mathbf{\Gamma}$ yields a compressed multi-set $\mathbf{\Gamma}'$, and the compression is performed using two sets Γ_i and Γ_j. Consider the nodes associated with these two sets and track, throughout the compression, all edges that connect them to the other nodes of the associated graph. Let Γ_k $(\neq \Gamma_j, \Gamma_j)$ be an arbitrary node of the associated graph. We first show that for any such node, the total number of edges connecting it to Γ_i and Γ_j does not increase after the compression. This is summarized in the following.

Multi-set $\mathbf{\Lambda}$	Multi-set $\mathbf{\Sigma} > \mathbf{\Lambda}$
$[\ldots,\ \{\{i,j\}\star\},\ \{\{i\}\star,\{j\}\star\},\ \ldots]$	$[\ldots,\ \{\{i\}\star\},\ \{\{j\}\star\},\ \ldots]$
$[\ldots,\ \{\{1,2,3\}\},\ \{\{i\}\star,\{j,k\}\star\},\ \ldots]$	$[\ldots,\ \{\{i\}\star\},\ \{\{j,k\}\star\},\ \ldots]$
$[\ldots,\ \{\{1,2,3\}\},\ \{\{i,j\}\star,\{i,k\}\star\},\ \ldots]$	$[\ldots,\ \{\{i,j\}\star\},\ \{\{i,k\}\star\},\ \ldots]$
$[\ldots,\ \{\{1,2,3\}\},\ \{\{i,j\}\star,\{i,k\}\star,\{j,k\}\star\},\ \ldots]$	$[\ldots,\ \{\{i,j\}\star\},\ \{\{i,k\}\star,\{j,k\}\star\},\ \ldots]$
$[\ldots,\ \{\{1\}\star,\{2\}\star,\{3\}\star\},\ \{\{i\}\star,\{j,k\}\star\},\ \ldots]$	$[\ldots,\ \{\{i\}\star,\{j\}\star\},\ \{\{i\}\star,\{k\}\star\},\ \ldots]$
$[\ldots,\ \{\{1\}\star,\{2\}\star,\{3\}\star\},\ \{\{i,j\}\star,\{i,k\}\star\},\ \ldots]$	$[\ldots,\ \{\{i\}\star\},\ \{\{j\}\star,\{k\}\star\},\ \ldots]$
$[\ldots,\ \{\{1\}\star,\{2\}\star,\{3\}\star\},\ \{\{i,j\}\star,\{i,k\}\star,\{j,k\}\star\},\ \ldots]$	$[\ldots,\ \{\{i\}\star,\{j\}\star\},\ \{\{k\}\star,\{i,j\}\star\},\ \ldots]$

Fig. 13: Non-trivial elementary decompressions for multi-sets of subsets of $2^{\{1,2,3\}}$. Here, (i,j,k) is a permutation of $(1,2,3)$.

- There is an edge (Γ_i,Γ_k) and an edge (Γ_j,Γ_k): In this case, no matter what the resulting graph $G_{\mathbf{\Gamma}'}$ is after the compression, there cannot be more than two edges connecting Γ_k to Γ_i and Γ_j.
- There is an edge (Γ_i,Γ_k) but there is no edge (Γ_j,Γ_k): Since there is no edge between Γ_j and Γ_k, one of them is a subset of the other.
  1) If $\Gamma_j \subseteq \Gamma_k$, then $\Gamma_i \cap \Gamma_j \subseteq \Gamma_k$ and there is, therefore, no edge between Γ_k and $\Gamma_i \cap \Gamma_j$ after the compression.
  2) If otherwise $\Gamma_j \supseteq \Gamma_k$, then $\Gamma_i \cup \Gamma_j \supseteq \Gamma_k$ and there is, therefore, no edge between Γ_k and $\Gamma_i \cup \Gamma_j$ after the compression.
- There is no edge (Γ_i,Γ_k) but an edge (Γ_j,Γ_k): This case is similar to the previous case.
- There is neither an edge (Γ_i,Γ_k) nor an edge (Γ_j,Γ_k): In this case, we have either of the following possibilities.
  1) If $\Gamma_i \subseteq \Gamma_k$ and $\Gamma_j \subseteq \Gamma_k$, then both $\Gamma_i \cup \Gamma_j$ and $\Gamma_i \cap \Gamma_j$ are subsets of Γ_k and there is no edge connecting Γ_k to $\Gamma_i \cap \Gamma_j$ or $\Gamma_i \cup \Gamma_j$ over $G_{\mathbf{\Gamma}'}$.
  2) If $\Gamma_i \subseteq \Gamma_k$ and $\Gamma_j \supseteq \Gamma_k$, then $\Gamma_i \cup \Gamma_j \supseteq \Gamma_k$ and $\Gamma_i \cap \Gamma_j \subseteq \Gamma_k$ and there is, therefore, no edge connecting Γ_k to $\Gamma_i \cap \Gamma_j$ or $\Gamma_i \cup \Gamma_j$ over $G_{\mathbf{\Gamma}'}$.
  3) If $\Gamma_i \supseteq \Gamma_k$ and $\Gamma_j \subseteq \Gamma_k$, then similar to the previous case one concludes that there is no edge connecting Γ_k to $\Gamma_i \cap \Gamma_j$ or $\Gamma_i \cup \Gamma_j$ over $G_{\mathbf{\Gamma}'}$.
  4) If $\Gamma_i \supseteq \Gamma_k$ and $\Gamma_j \supseteq \Gamma_k$, then both $\Gamma_i \cup \Gamma_j$ and $\Gamma_i \cap \Gamma_j$ are supersets of Γ_k and there is, therefore, no edge connecting Γ_k to their replacements $\Gamma_i \cap \Gamma_j$ or $\Gamma_i \cup \Gamma_j$ over $G_{\mathbf{\Gamma}'}$.

Besides, edges between Γ_k and $\Gamma_{k'}$, where $k,k' \notin \{i,j\}$, remain unaffected. Since the compression is non-trivial, nodes Γ_i and Γ_j have been connected over $G_{\mathbf{\Gamma}}$ and are no longer connected over $G_{\mathbf{\Gamma}'}$. So, the total number of edges in $G_{\mathbf{\Gamma}}$ is strictly smaller than $G_{\mathbf{\Gamma}}$, and this concludes the proof. ■

Define a *(non-trivial) decompression* as the inverse act of a (non-trivial) compression. As opposed to compression, a non-trivial decompression is not always possible using every two elements of a multi-set $\mathbf{\Lambda}$. It is, indeed, not clear whether a multi-set $\mathbf{\Lambda}$ is decompressible at all. For example, the multi-set $[\{\{2,3\},\{1,2,3\}\},\{\{1\},\{2\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}]$ cannot be non-trivially decompressed; i.e., there exists no multi-set $\mathbf{\Gamma}$ such that

$$\mathbf{\Gamma} > [\{\{2,3\},\{1,2,3\}\},\{\{1\},\{2\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}]. \tag{78}$$

The table in Fig. 13 gives a list of some non-trivial elementary decompressions for multi-sets of subsets of $2^{\{1,2,3\}}$.

Although not all multi-sets are decompressible, Lemma 13 below identifies a class of multi-sets of subsets of $2^{\{1,2,3\}}$ that are decompressible.

Lemma 13. *Let $\mathbf{\Lambda}$ and $\mathbf{\Gamma}$ be multi-sets of subsets of $2^{\{1,2,3\}}$. Suppose $\mathbf{\Lambda}$ is of saturated pattern and $\mathbf{\Gamma}$ is of standard pattern. If $\mathbf{\Lambda}$ and $\mathbf{\Gamma}$ are a pair of balanced multi-sets, then a non-trivial elementary decompression could be performed over $\mathbf{\Lambda}$, unless $\mathbf{\Lambda} = \mathbf{\Gamma}$.*

Proof: The proof is by showing that for any multi-set $\mathbf{\Lambda}$ with the stated assumptions, at least one of the non-trivial elementary decompressions in Fig. 13 is doable. This is done by double counting (once in $\mathbf{\Lambda}$ and once in $\mathbf{\Gamma}$) the number of times each subset $\mathcal{S} \in 2^{\{1,2,3\}}$ appears in the multi-set $\mathbf{\Lambda}$, and showing that no matter what $\mathbf{\Lambda}$ and $\mathbf{\Gamma}$ are, at least one of the cases of Fig. 13 occurs. We defer details of this proof to Appendix H. ■

Lemma 13 shows that a multi-set $\mathbf{\Lambda}$ of saturated pattern, which is balanced with a multi-set $\mathbf{\Gamma}$ of standard pattern, can be non-trivially decompressed. Let the result of this non-trivial elementary decompression be a multi-set $\mathbf{\Sigma}$. Since the decompressed multi-set $\mathbf{\Sigma}$ is, itself, of saturated pattern and remains balanced with multi-set $\mathbf{\Gamma}$ (see Remark 9), one can continue decompressing it using Lemma 13 as long as $\mathbf{\Sigma} \neq \mathbf{\Gamma}$. This, either ends in an infinite loop, or ends in $\mathbf{\Sigma} = \mathbf{\Gamma}$ (Note that there cannot be two different multi sets $\mathbf{\Gamma} \geq \mathbf{\Lambda}$ and $\mathbf{\Gamma}' \geq \mathbf{\Lambda}$ such that $\mathbf{\Gamma}$, $\mathbf{\Gamma}'$, and $\mathbf{\Lambda}$ are all balanced); the former is ensured not to happen, for the total number of edges in the associated graph strictly decreases after each decompression (see Lemma 12). Thus, we arrive at the following lemma.

Lemma 14. *Let* $\mathbf{\Lambda}$ *and* $\mathbf{\Gamma}$ *be multi-sets of subsets of* $2^{\{1,2,3\}}$ *where* $\mathbf{\Lambda}$ *is of saturated pattern and* $\mathbf{\Gamma}$ *is of standard pattern. If* $\mathbf{\Lambda}$ *and* $\mathbf{\Gamma}$ *are balanced, then* $\mathbf{\Lambda}$ *can be decompressed to* $\mathbf{\Gamma}$*; i.e.,* $\mathbf{\Gamma} \geq \mathbf{\Lambda}$*.*

2) The converse proof in Theorem 4: With these tools in hand, we are now ready to prove the converse part of Theorem 4. The key to proving the converse is the following lemma which we only state here and prove in Appendix I.

Lemma 15. *Consider the rate-region characterization in Theorem 1 (where* $\mathcal{I}_1 = \{1,2,3\}$ *and* $\mathcal{I}_2 = \{4,\ldots,K\}$*). The constraints given by inequality* (30) *in Theorem 1 can be replaced by* (79)*,below, without affecting the rate-region.*

$$\sum_{\mathcal{S}\in\Lambda} \alpha_{\mathcal{S}} \geq 0, \quad \forall\Lambda \subseteq 2^{\mathcal{I}_1} \textit{ superset saturated.} \tag{79}$$

By Lemma 15, the rate-region of Theorem 1 is equivalently given by constraints (31)-(34), (79). We start with finding an outer-bound which looks *similar* to this inner-bound.

Lemma 16. *Any achievable rate pair* (R_1, R_2) *satisfies outer-bound constraints* (80)-(83) *for any given* $\epsilon > 0$*.*

$$\frac{1}{n}H(X^n_{\Lambda}|W_1) \geq 0, \qquad \forall\Lambda \subseteq 2^{\mathcal{I}_1} \textit{ superset saturated} \tag{80}$$

$$R_1 + \frac{1}{n}H(X^n_{\{\{i\}\star\}}|W_1) \leq \sum_{\mathcal{S}\in\{\{i\}\star\}} |\mathcal{E}_{\mathcal{S}}| + \epsilon, \qquad \forall i \in \mathcal{I}_1 \tag{81}$$

$$R_2 \leq \frac{1}{n}H(X^n_{\Lambda}|W_1) + \sum_{\mathcal{S}\in\Lambda^c} |\mathcal{E}_{\mathcal{S},p}| + \epsilon, \qquad \forall\Lambda \subseteq 2^{\mathcal{I}_1} \textit{ superset saturated}, \ \forall p \in \mathcal{I}_2 \tag{82}$$

$$R_1 + R_2 \leq \sum_{\mathcal{S}\subseteq\mathcal{I}_1} |\mathcal{E}_{\mathcal{S},p}| + \epsilon, \qquad \forall p \in \mathcal{I}_2. \tag{83}$$

Remark 10. *Notice the similarity of inequalities* (80), (81), (82), (83) *with constraints* (79), (32), (33), (34)*, respectively. We provide no similar outer-bound for the inner-bound constraint* (31) *because it is redundant*[4]*.*

Proof: Inequalities in (80) hold by the positivity of entropy. To show inequalities in (81), we bound R_1 for each public receiver $i \in \mathcal{I}_1$ as follows:

$$\begin{aligned} nR_1 =& H(W_1) & (84)\\ =& H(W_1) - H(W_1|Y_i^n) + H(W_1|Y_i^n) & (85)\\ \overset{(a)}{\leq}& I(W_1;Y_i^n) + n\epsilon & (86)\\ =& I(W_1;X^n_{\{\{i\}\star\}}) + n\epsilon & (87)\\ =& H(X^n_{\{\{i\}\star\}}) - H(X^n_{\{\{i\}\star\}}|W_1) + n\epsilon & (88)\\ \overset{(b)}{\leq}& n\left(\sum_{\mathcal{S}\in\{\{i\}\star\}} |\mathcal{E}_{\mathcal{S}}|\right) - H(X^n_{\{\{i\}\star\}}|W_1) + n\epsilon. & (89) \end{aligned}$$

In the above chain of inequalities, (a) follows from Fano's inequality and (b) follows by bounding the cardinality of the alphabet set of $X^n_{\{\{i\}\star\}}$ and using $H(X) \leq \log|\mathcal{X}|$, where $\mathcal{X}$ is the alphabet set of X. In a similar manner, we have the following bound on $nR_1 + nR_2$ for each private receiver p which proves inequality (83).

$$\begin{aligned} nR_1 + nR_2 =& H(W_1W_2) & (90)\\ \leq& I(W_1W_2;Y_p^n) + n\epsilon & (91)\\ =& I(W_1W_2;X^n_{\{\phi\star\},p}) + n\epsilon & (92)\\ =& H(X^n_{\{\phi\star\},p}) + n\epsilon & (93)\\ \leq& n\left(\sum_{\mathcal{S}\in\{\phi\star\}} |\mathcal{E}_{\mathcal{S},p}|\right) + n\epsilon. & (94) \end{aligned}$$

Finally, we bound R_2 to obtain the inequalities in (82). In the following, we have $p \in \mathcal{I}_2$, $\Lambda \subseteq 2^{\mathcal{I}_1}$, and $\epsilon > 0$.

$$nR_2 = H(W_2|W_1) \tag{95}$$

[4] This inequality is redundant because it is the only inequality that contains the free variable α_{ϕ}.

$$
\begin{aligned}
&= H(W_2|W_1) - H(W_2|W_1 Y_p^n) + H(W_2|W_1 Y_p^n) && (96)\\
&\overset{(a)}{\leq} I(W_2; Y_p^n|W_1) + n\epsilon && (97)\\
&= I(W_2; X_{\{\phi\star\},p}^n|W_1) + n\epsilon && (98)\\
&= H(X_{\{\phi\star\},p}^n|W_1) + n\epsilon && (99)\\
&\overset{(b)}{\leq} H(X_{\{\phi\star\},p}^n X_\Lambda^n|W_1) + n\epsilon && (100)\\
&= H(X_\Lambda^n|W_1) + H(X_{\{\phi\star\},p}^n|X_\Lambda^n W_1) + n\epsilon && (101)\\
&\overset{(c)}{\leq} H(X_\Lambda^n|W_1) + H(X_{\Lambda^c,p}^n) + n\epsilon && (102)\\
&\overset{(d)}{\leq} H(X_\Lambda^n|W_1) + n\left(\sum_{\mathcal{S}\in\Lambda^c} |\mathcal{E}_{\mathcal{S},p}|\right) + n\epsilon. && (103)
\end{aligned}
$$

In the above chain of inequalities, step (a) follows from Fano's inequality. Step (b) holds for any subset $\Lambda \subseteq 2^{\mathcal{I}_1}$ and in particular subsets which are superset saturated. Step (c) follows because conditioning decreases entropy. Step (d) follows by by bounding the cardinality of the alphabet set of $X_{\Lambda^c,p}^n$ and using $H(X) \leq \log|\mathcal{X}|$, where $\mathcal{X}$ is the alphabet set of X.

■

The rate-region of Theorem 1 can be obtained explicitly by applying Fourier-Motzkin elimination to (32)-(34) and (79) to eliminate parameters $\alpha_{\mathcal{S}}$. This gives a set of inequalities of the form $m_1R_1 + m_2R_2 \leq E$, each obtained by summing potentially multiple copies of constraints (32)-(34), (79), so that all variables $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, get eliminated. To show a converse for each such inner-bound inequality, $m_1R_1 + m_2R_2 \leq E$, take copies of the corresponding outer-bound constraints (80)-(83) and sum them up to yield an outer-bound inequality of the form

$$
\begin{aligned}
&m_1R_1 + m_2R_2 + \frac{1}{n}\sum_{\Gamma\in\boldsymbol{\Gamma}} H(X_\Gamma^n|W_1)\\
&\leq E + \frac{1}{n}\sum_{\Lambda\in\boldsymbol{\Lambda}} H(X_\Lambda^n|W_1) && (104)
\end{aligned}
$$

where $\boldsymbol{\Gamma}$ is a multi-set of standard pattern and $\boldsymbol{\Lambda}$ is a multi-set of saturated pattern, both consisting of subsets of $2^{\mathcal{I}_1}$ where $\mathcal{I}_1 = \{1,2,3\}$. Notice that $\boldsymbol{\Gamma}$ and $\boldsymbol{\Lambda}$ are balanced since Fourier-Motzkin elimination ensures that all the $\alpha_{\mathcal{S}}$'s are eliminated. So by Lemma 14, $\boldsymbol{\Lambda} \leq \boldsymbol{\Gamma}$ and therefore,

$$
\sum_{\Lambda\in\boldsymbol{\Lambda}} H(X_\Lambda^n|W_1) \leq \sum_{\Gamma\in\boldsymbol{\Gamma}} H(X_\Gamma^n|W_1). \qquad (105)
$$

Using (105) in the outer-bound inequality (104), we conclude the converse to $m_1R_1 + m_2R_2 \leq E$, for every such inequality that appears in the inner-bound. This concludes the proof of the converse of Theorem 4.

Remark 11. *Note that Lemma 13, Lemma 14, and Lemma 15 are valid only for $m \leq 3$, and Lemma 16 holds in general.*

Remark 12. *The following example serves as a counter example for Lemma 13 when $m > 3$. Consider the following multi-sets of subsets of $2^{\{1,2,3,4\}}$:*

$$
\begin{aligned}
\boldsymbol{\Lambda} &= [\{\{1\}\star\{2\}\star\{3\}\star\{4\}\star\}, \{\{1,2\}\star\{1,3\}\star\{2,4\}\}, \{\{1,4\}\star\{2,3\}\star\{3,4\}\star\}, \{\{1,2,3,4\}\}],\\
\boldsymbol{\Gamma} &= [\{\{1\}\star\}, \{\{2\}\star\}, \{\{3\}\star\}, \{\{4\}\star\}].
\end{aligned}
$$

It is easy to see that $\boldsymbol{\Lambda}$ is of saturated pattern, $\boldsymbol{\Gamma}$ is of standard pattern, and they are balanced. Nevertheless, no elementary decompression cab be performed on $\boldsymbol{\Lambda}$.

We would like to remark that one could prove Theorem 5 using the same technique. More precisely, Lemma 15 is already implied and Lemma 16 could accommodate an outer-bound constraint *similar* to the inner-bound constraint of (55) as follows:

$$
\begin{aligned}
\frac{1}{n}H(X_{\{\{i\}\star\}}^n|W_1) &\leq \frac{1}{n}H(X_\Lambda^n|W_1) + \frac{1}{n}H(X_\Lambda^n|X_{\{\{i\}\star\}}^n, W_1) && (106)\\
&\leq \frac{1}{n}H(X_\Lambda^n|W_1) + \frac{1}{n}H(X_{(\{\{i\}\star\}\backslash\Lambda)}^n) && (107)\\
&\leq \frac{1}{n}H(X_\Lambda^n|W_1) + \sum_{\substack{\mathcal{S}\in\Lambda^c\\ \mathcal{S}\ni i}} |\mathcal{E}_{\mathcal{S}}|. && (108)
\end{aligned}
$$

The rest of the converse proof follows, as before, by sub-modularity.

VII. A block Markov encoding scheme for broadcasting two nested message sets over broadcast channels

Finally, to emphasise the generality of our study, in this section we extend our coding technique to general broadcast channels. Let us consider a broadcast channel $p(y_1, \dots, y_K|x)$ with input signal X, output signals $Y_1, \dots, Y_K$ where Y_i, $i \in \mathcal{I}_1$, is the signal available to public receiver i and Y_p, $p \in \mathcal{I}_2$, is the signal available to private receiver p.

In many cases where the optimal rates of communication are known for broadcasting nested messages, the classical techniques of rate splitting and superposition coding have proved optimal, and this motivates us, also, to start with such encoding schemes. In particular, in the context of two message broadcast, we split the private message into different pieces $W_2^{\mathcal{S}}$ of rates $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, where $W_2^{\mathcal{S}}$ is revealed to all public receivers in $\mathcal{S}$ (as well as the private receivers). X is then formed by superposition coding. For $\mathcal{I}_1 = \{1,2\}$, for instance, $W_2^{\{1\}}$ and $W_2^{\{2\}}$ are each independently superposed on $(W_1, W_2^{\{1,2\}})$, and W_2^{ϕ} is superposed on all of them to form the input signal X. The rate-region achievable by superposition coding is given by a feasibility problem (a straightforward generalization of [39, Theorem 8.1]). The rate pair (R_1, R_2) is achievable if there exist parameters $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, and auxiliary random variables $U_{\mathcal{S}}$, $\phi \neq \mathcal{S} \subseteq \mathcal{I}_1$, such that inequalities in (109)-(113) hold for a joint probability distribution $\prod_{k=1}^{K} \prod_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ |\mathcal{S}|=k}} p(u_{\mathcal{S}}|\{u_{\mathcal{T}}\}_{\substack{\mathcal{T} \in \{\mathcal{S}\star\} \\ \mathcal{T} \neq \mathcal{S}}}) p(x|\{u_{\mathcal{S}}\}_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \neq \phi}})$.

Structural constraints:

$$\alpha_{\mathcal{S}} \geq 0, \qquad \forall \mathcal{S} \subseteq \mathcal{I}_1 \tag{109}$$

$$R_2 = \sum_{\mathcal{S} \subseteq \mathcal{I}_1} \alpha_{\mathcal{S}}, \tag{110}$$

Decodability constraints at public receivers:

$$\sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} \alpha_{\mathcal{S}} \leq \sum_{\mathcal{S} \in \Lambda} \alpha_{\mathcal{S}} + I(\cup_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} U_{\mathcal{S}}; Y_i | \cup_{\mathcal{S} \in \Lambda} U_{\mathcal{S}}), \quad \forall \Lambda \subseteq \{\{i\}\star\} \text{ superset saturated}, \ \forall i \in \mathcal{I}_1 \tag{111}$$

$$R_1 + \sum_{\substack{\mathcal{S} \subseteq \mathcal{I}_1 \\ \mathcal{S} \ni i}} \alpha_{\mathcal{S}} \leq I(\cup_{\substack{\mathcal{S} \subseteq \mathcal{I}_1, \\ \mathcal{S} \ni i}} U_{\mathcal{S}}; Y_i), \quad \forall i \in \mathcal{I}_1 \tag{112}$$

Decodability constraints at private receivers:

$$R_2 \leq \sum_{\mathcal{S} \in \Lambda} \alpha_{\mathcal{S}} + I\left(X; Y_p | \cup_{\mathcal{S} \in \Lambda} U_{\mathcal{S}}\right), \quad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \text{ superset saturated}, \ \forall p \in \mathcal{I}_2 \tag{113}$$

$$R_1 + R_2 \leq I(X; Y_p), \quad \forall p \in \mathcal{I}_2. \tag{114}$$

As we show below, with a simple block Markov encoding scheme, we can achieve rate pairs which satisfy a relaxed version of (109)-(114). Specifically, we can relax the constraints in (109) to the following set of constraints:

$$\textstyle\sum_{\mathcal{S} \in \Lambda} \alpha_{\mathcal{S}} \geq 0 \quad \forall \Lambda \subseteq 2^{\mathcal{I}_1} \text{ superset saturated.} \tag{115}$$

We briefly outline this block Markov encoding scheme for the case where we have two public and one private receiver (the same arguments go through for the general case also). We devise our block Markov encoding scheme in three steps.

1) We form an extended broadcast channel with input/output signals X', Y_1', Y_2', Y_3', as shown in Fig. 14. We have $X' = (X, V_{\{1,2\}}, V_{\{2\}}, V_{\{1\}}, V_{\phi})$, $Y_1' = (Y_1, V_{\{1,2\}}, V_{\{1\}})$, $Y_2' = (Y_2, V_{\{1,2\}}, V_{\{2\}})$, and $Y_3' = (X, V_{\{1,2\}}, V_{\{2\}}, V_{\{1\}}, V_{\phi})$, where $V_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2\}$, takes its value in an alphabet set $\mathcal{V}_{\mathcal{S}}$ of size $2^{\beta_{\mathcal{S}}}$. We call variables $V_{\mathcal{S}}$ the *virtual signals*.

2) We design a general multicast code over the extended channel. We say that a multicast code achieves rate tuple $(R_1, \alpha'_{\{1,2\}}, \alpha'_{\{2\}}, \alpha'_{\{1\}}, \alpha'_{\phi})$, if it communicates a message of rate R_1 to all receivers and independent messages of rates $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2\}$, to public receivers in $\mathcal{S}$ and all private receivers. We design such a multicast code, using superposition coding. Conditions under which this encoding scheme achieves a rate tuple $(R_1, \alpha'_{\{1,2\}}, \alpha'_{\{2\}}, \alpha'_{\{1\}}, \alpha'_{\phi})$ over the extended broadcast channel are readily given by inequalities in (111)-(113) (for parameters $\alpha'_{\mathcal{S}}$, auxiliary random variables $U'_{\mathcal{S}}$, $\phi \neq \mathcal{S} \subseteq \mathcal{I}_1$, and input/output signals X', Y_1', Y_2', Y_3').

3) We emulate the virtual signals. An extension to Lemma 10 provides us with sufficient conditions.

We now use the information bits that are to be encoded in block $t+1$, to also convey (the content of) the virtual signals in block t. We use the remaining information bits, not assigned to the virtual signals, to communicate the common and private messages. Putting together the constraints needed in the above three steps (as in Section V), we obtain an achievable rate region for each joint probability distribution of the form $p(u'_{\{1,2\}}) p(u'_{\{1\}}|u'_{\{1,2\}}) p(u_{\{2\}}|u'_{\{1,2\}}) p(x'|u'_{\{2\}}, u'_{\{1\}}, u'_{\{1,2\}})$. In particular, by a proper choice for the auxiliary random variables, we show that the rate region defined in (110)-(115) is achievable. More precisely, we have the following theorem (details of the proof are available in [32, Theorem 4.3]).

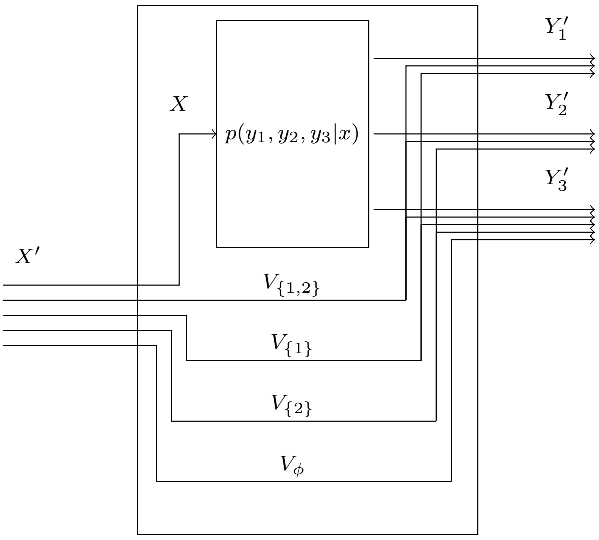


Fig. 14: The extended broadcast channel obtained from $p(y_1, y_2, y_3|x)$ and the virtual signals $V_{\{1,2\}}$, $V_{\{2\}}$, $V_{\{1\}}$, V_ϕ.

Theorem 6. *The rate pair* (R_1, R_2) *is achievable if there exist parameters* $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, *and auxiliary random variables* $U_{\mathcal{S}}$, $\phi \neq \mathcal{S} \subseteq \mathcal{I}_1$, *such that they satisfy inequalities in* (110)-(115) *for a joint probability distribution in the following form:*

$$\prod_{k=1}^{K} \prod_{\substack{\mathcal{S}\subseteq\mathcal{I}_1 \\ |\mathcal{S}|=k}} p(u_{\mathcal{S}}|\{u_{\mathcal{T}}\}_{\substack{\mathcal{T}\in\{\mathcal{S}_\star\} \\ \mathcal{T}\neq\mathcal{S}}}) p(x|\{u_{\mathcal{S}}\}_{\substack{\mathcal{S}\subseteq\mathcal{I}_1 \\ \mathcal{S}\neq\phi}}).$$

Remark 13. *Note that the rate-region in Theorem 6 looks similar to that of superposition coding (see* (109)-(113)*). Clearly, the former rate-region has a less constrained set of non-negativity constraints on* $\alpha_{\mathcal{S}}$ *and includes the latter. It is interesting to ask if this inclusion is strict, and it is non-trivial to answer this question because of the union that is taken over all proper probability distributions. For a fixed joint probability distribution, the inclusion is strict for* $m \geq 3$ *public and any number of private receivers. So it is possible that the proposed block Markov scheme strictly enlarges the rate-region of superposition coding. However, this needs further investigation.*

Remark 14. *It is worth mentioning that one may design a more general coding scheme by using Marton's coding in the second step (when devising a multicast code for the extended broadcast channel). Following similar steps as above (see [32, Theorem 4.3]), one can relax the non-negativity constraints from the more general rate-region (which is achievable by rate-splitting, superposition coding, and Marton's coding).*

VIII. Conclusion

In this paper, we studied the problem of multicasting two nested message sets over combination networks and gave a full characterization of the capacity region for combination networks with three (or fewer) public and any number of private receivers.

More generally, we discussed three encoding schemes which are based on linear superposition schemes. We showed that the standard linear superposition encoding scheme is optimal for networks with two public and any number of private receivers. For networks with more than two public receivers, however, this scheme is sub-optimal. We discussed two improved schemes. The first scheme uses an appropriate pre-encoding at the source, followed by a linear superposition scheme. We characterized the achievable rate-region in terms of a feasibility problem (Theorem 1) and showed its tightness for networks with three (or fewer) public and any number of private receivers (Theorem 4). We illustrated an example (Example 6) where this scheme performs sub-optimally, and proposed an optimal block Markov encoding scheme. Motivated by this example, we proposed a block Markov encoding scheme and characterized its achievable rate-region (Theorem reflb-CombNetbme-Theorem). This scheme, also, is capacity achieving for network with three (or fewer) public and any number of receivers (Theorem 5). While the rate-regions of Theorem 1 and Theorem 2 are not comparable in general, we showed an example where Theorem 2 strictly includes Theorem 1. We conjecture that this inclusion always holds.

We discussed that combination networks are an interesting class of networks to study specially since they also form a class of resource-based broadcast channels. To illustrate the implications of our study over broadcast channels, we generalized the block Markov encoding scheme that we proposed in the context of combination networks and derived a new achievable scheme for broadcast channels with two nested message sets. The rate-region achieved by this scheme includes the previous rate-regions. It remains open whether this inclusion is strict.

Appendix A
Proof of Lemma 1

We start with proving the "only if" statement. Since W_1 is recoverable from Y, for any W_1, W_2, W_1', W_2' it holds that if $Y = Y'$ (or equivalently $\mathbf{T}_1(W_1 - W_1') + \mathbf{T}_2(W_2 - W_2') = 0$), then $W_1 = W_1'$. In particular, for $W_2 = W_2'$ one finds that for any W_1, W_1' equation $\mathbf{T}_1(W_1 - W_1') = 0$ results in $W_1 = W_1'$. Therefore, $\mathbf{T}_1$ is full column rank; i.e., rank($\mathbf{T}_1$) $= R_1$. Furthermore, for all vectors W_1, W_1', W_2, W_2' such that $W_1 \neq W_1'$, one obtains $\mathbf{T}_1(W_1 - W_1') \neq \mathbf{T}_2(W_2' - W_2)$; i.e., the column space of matrix $\mathbf{T}_2$ is disjoint from the column space of matrix $\mathbf{T}_1$.

To prove the "if" statement, we prove that if it holds that rank($\mathbf{T}_1$) $= R_1$ and column spaces of $\mathbf{T}_1$ and $\mathbf{T}_2$ are disjoint, then equation $Y = Y'$ (or equivalently $\mathbf{T}_1(W_1 - W_1') + \mathbf{T}_2(W_2 - W_2') = 0$) results in $W_1 = W_1'$ for all vectors W_1, W_2, W_1', W_2'. We show this by contradiction. Let $\mathbf{T}_1(W_1 - W_1') + \mathbf{T}_2(W_2 - W_2') = 0$ and $W_1 \neq W_1'$. For the cases where $\mathbf{T}_2(W_2 - W_2') = 0$, we get $\mathbf{T}_1(W_1 - W_1') = 0$ for $W_1 \neq W_1'$, which contradicts the original assumption of rank($\mathbf{T}_1$) $= R_1$. If $\mathbf{T}_2(W_2 - W_2') \neq 0$, then $\mathbf{T}_1(W_1 - W_1') + \mathbf{T}_2(W_2 - W_2') = 0$ implies that there exists at least one non-zero vector in the intersection of the column spaces of $\mathbf{T}_1$ and $\mathbf{T}_2$ which contradicts the assumption that column space of $\mathbf{T}_1$ and $\mathbf{T}_2$ are disjoint.

Appendix B
Proof of Lemma 3

We start with proving that (i) implies (ii). Assume that matrix $\mathbf{T}$ is assigned full column rank. Over the equivalent unicast network, we propose a network code that constitutes a transfer matrix (from node A to node B) exactly equal to the full-rank matrix $\mathbf{T}$: First, let each outgoing edge of the source carry one uncoded symbol of the message. Then, let the first $r_{\{1,2\}}$ rows of matrix $\mathbf{T}$ specify the local encoding matrix at node $n'_{\{1,2\}}$. Similarly, let the second $r_{\{2\}}$, the third $r_{\{1\}}$, and the last r_ϕ set of rows of matrix $\mathbf{T}$ specify the local encoding matrices at nodes $n'_{\{2\}}$, $n'_{\{1\}}$, and n'_ϕ, respectively. Note that the zero structure of matrix $\mathbf{T}$, which is given in equation (5), ensures that this is a well defined construction. It follows that $\mathbf{T}$ is the transfer matrix from node A to node B and, since it is full column rank, the encoded message can be decoded at sink node B.

Statement (ii) also implies (i) and the proof is by construction. If a message of rate c could be sent over the equivalent unicast network (from node A to node B), then there are c edge disjoint paths from the source A to the sink B. Each such path matches one of the outgoing edges of source node A to one of the incoming edges of sink node B. We call this matching between the outgoing edges of the source and the incoming edges of the sink matching M and we note that its size is c. We use this matching to fill the indeterminates of matrix $\mathbf{T}$ with $0 - 1$. First of all, note that each column j of matrix $\mathbf{T}$ corresponds to an outgoing edge of the source, say e_j, and each row i of matrix $\mathbf{T}$ corresponds to an incoming edge of the sink, say e_i'. So each entry (i, j) of matrix $\mathbf{T}$ is priorly set to zero if and only if edges e_j and e_j' cannot be matched. Now, put a 1 in entry (i, j) of matrix $\mathbf{T}$ if edge e_j is matched to edge e_j' over the matching M. Since matching M has a size equal to c, matrix $\mathbf{T}$ is made full column rank.

Appendix C
Proof of Lemma 4

Consider all (edge-) cuts separating the source node A from the sink node B. Since the intermediate edges all have infinite capacity, the minimum cut does not contain any edges from them. One can verify the following fact over Fig. 6: If an edge $(n'_{\mathcal{S}'}, B)$, $\mathcal{S}' \subseteq \{1, \dots, t\}$, does not belong to the cut, then all edges $(A, n_{\mathcal{S}})$ where $\mathcal{S} \supseteq \mathcal{S}'$ belong to that cut. So each (finite-valued) cut corresponds to a subset of the nodes $n'_{\mathcal{S}}$ in the third layer. Denoting this subset of nodes by $\{n'_{\mathcal{S}}\}_{\mathcal{S}\in\Gamma}$, for some $\Gamma \subseteq 2^{\{1,\dots,t\}}$, we have the value of the cut given by

$$\sum_{\mathcal{S}\in\Gamma} r_{\mathcal{S}} + \sum_{\mathcal{S}\supseteq\mathcal{S}',\ \mathcal{S}'\in\Gamma^c} c_{\mathcal{S}}. \tag{116}$$

It is not difficult to verify that the (inclusion-wise) minimal cuts are derived for sets Γ^c that are superset saturated. Renaming Γ^c as Λ concludes the proof.

Appendix D
Proof of Lemma 6

Let r_i denote the number of rows in $\mathbf{G}^{(i)}$; i.e., let $r_i = \sum_{\mathcal{S}\subseteq\mathcal{I}_1\ \mathcal{S}\ni i} |\mathcal{E}_{\mathcal{S}}|$. In the matrix $\mathbf{G}^{(i)} = [\mathbf{B}^{(i)}|\mathbf{L}_1^{(i)}]$, first select an assignment for the columns of $\mathbf{L}_1^{(i)}$ that makes them linearly independent (such an assignment exists from construction). Since the element variables in $\mathbf{L}_1^{(i)}$ are independent of those in $\mathbf{B}^{(i)}$, $\mathbf{G}^{(i)}$ can be made full-rank just by picking R_1 vectors from $\mathbb{F}^{r_i}$, linearly independent from the columns of $\mathbf{L}_1^{(i)}$, for the columns of $\mathbf{B}^{(i)}$. This is possible since rank($\mathbf{B}^{(i)}$) is at most $\sum_{\mathcal{S}\subseteq\mathcal{I}_1\ \mathcal{S}\ni i} \alpha_{\mathcal{S}}$ which is bounded by $r_i - R_1$ (by assumption).

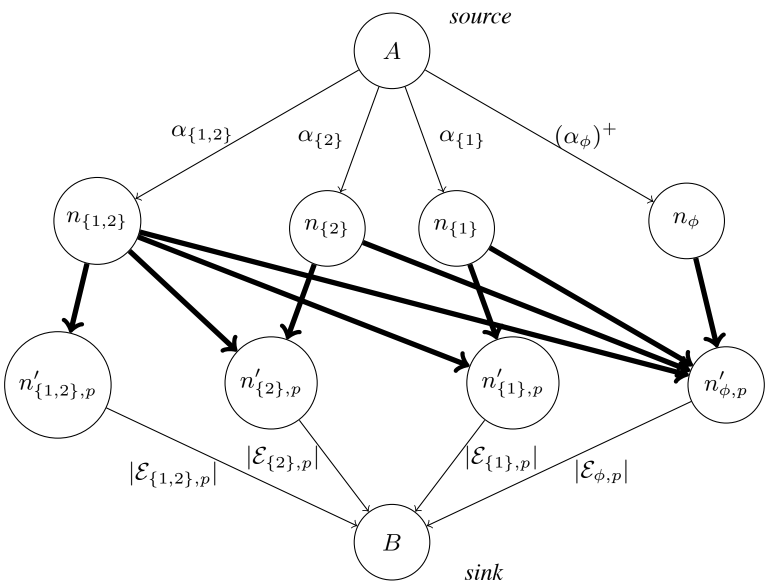


Fig. 15: Source node A communicates a message of rate R_2 to the sink node, B.

Appendix E
Proof of Lemma 9

For simplicity of notation, we give the proof for the case where $m = 2$. We prove that $\mathbf{T}^{(p)}\mathbf{P}$ could be made full column rank if and only if message W_2 could be unicast over the network of Fig. 15. In this network the outgoing edges of the source and the incoming edges of the sink are all of unit capacity and the bold edges in the middle are of infinite capacity. Define $\mathbf{T}^{(p)\prime} := \mathbf{T}^{(p)}\mathbf{P}$ which is given by

$$\mathbf{T}^{(p)\prime} = \begin{array}{c|c|c|c|l} \overset{\alpha_{\{1,2\}}}{\longleftrightarrow} & \overset{\alpha_{\{1\}}}{\leftrightarrow} & \overset{\alpha_{\{2\}}}{\leftrightarrow} & \overset{\alpha_\phi}{\leftrightarrow} & \\ & 0 & 0 & 0 & \updownarrow |\mathcal{E}_{\{1,2\},p}| \\ \hline & & 0 & 0 & \updownarrow |\mathcal{E}_{\{1\},p}| \\ \hline & 0 & & 0 & \updownarrow |\mathcal{E}_{\{2\},p}| \\ \hline & & & & \updownarrow |\mathcal{E}_{\phi,p}| \end{array} \quad \cdot \quad \mathbf{P}. \tag{117}$$

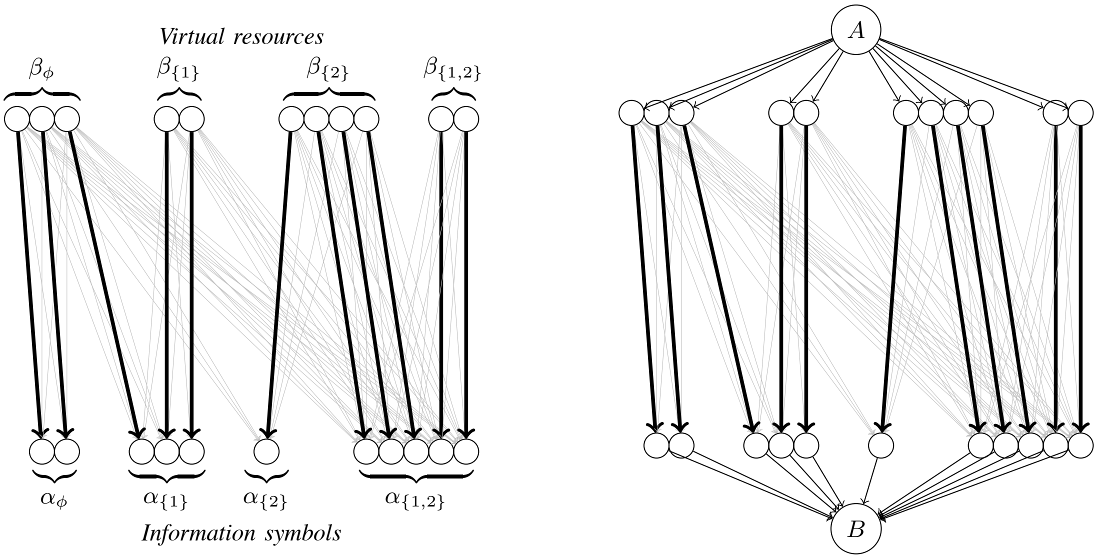
Think of matrix $\mathbf{P}$ as the local transfer matrix at source node A. Also, think of the matrix formed by the first $|\mathcal{E}_{\{1,2\},p}|$ rows of $\mathbf{T}^{(p)\prime}$ as the local transfer matrix at intermediate node $n_{\{1,2\},p}$, the matrix formed by the second $|\mathcal{E}_{\{1\},p}|$ rows of $\mathbf{T}^{(p)\prime}$ as the local transfer matrix at intermediate node $n_{\{1\}}$ and so on. Notice the equivalence between matrix $\mathbf{T}^{(p)\prime}$ and the transfer matrix imposed by a linear network code from node A to node B over the network of Fig. 15, and conclude that message W_2 is decodable if and only if message W_2 could be unicast from A to B. Decodability conditions at receiver p can, therefore, be inferred from the min-cut separating nodes A and B over the network of Fig. 15. Lemma 4 gives this min-cut by the following expression.

$$\min\left\{ \min_{\substack{\Lambda\subset 2^{\mathcal{I}_1} \\ \Lambda\text{superset saturated}}} \sum_{\mathcal{S}\in\Lambda} \alpha_{\mathcal{S}} + \sum_{\mathcal{S}\in\Gamma^c} |\mathcal{E}_{\mathcal{S},p}|, \sum_{\mathcal{S}\in 2^{\mathcal{I}_1},\ \mathcal{S}\neq\phi} \alpha_{\mathcal{S}} + (\alpha_\phi)^+ \right\}. \tag{118}$$

One can verify that R_2 is smaller than the expression in (118), provided that inequalities in (33) hold.

Appendix F
Application of the Sparse Zeros Lemma to the proof of Theorem 1

We constructed matrices $\mathbf{G}^{(i)}$, $i \in \mathcal{I}$ and reduced the problem to making all these matrices simultaneously full-rank. Matrices $\mathbf{G}^{(i)}$ have their entries defined by the variables in $\mathbf{A}$ and $\mathbf{P}$. We also discussed that each of these matrices could be made full column rank. This implies that there exists a square submatrix of each $\mathbf{G}^{(i)}$, say $\mathbf{G}_s^{(i)}$, that could be made full-rank. Let $\mathcal{P}^{(i)}$ be the polynomial corresponding to the determinant of $\mathbf{G}_s^{(i)}$, and $\mathcal{P} = \prod_i \mathcal{P}^{(i)}$. Given that there exists an assignment for the variables such that each individual polynomial $\mathcal{P}^{(i)}$ is non-zero, we can conclude from the sparse zeros lemma that there



(a) The bi-partite graph between the virtual resources and the decodable information symbols.

(b) The equivalent unicast information flow problem.

Fig. 16: The virtual resources are emulatable if there exists a matching of size $\sum_{\mathcal{S}\subseteq\mathcal{I}_1}\beta_{\mathcal{S}}$ between the virtual resources and the information symbols that can emulate them. The light edges connect the virtual resources to the information symbols that can emulate them, and the bold edges show a matching between them.

exists an assignment such that all polynomials are simultaneously non-zero. We can furthermore provide an upper bound on the required size for $\mathbb{F}$. This is done next by finding the degree of each polynomial $\mathcal{P}^{(i)}$ in each variable.

For $i \in \mathcal{I}_1$, since all variables in $\mathbf{G}_s^{(i)}$ are independent of each other, the desired degree is at most 1. For $\mathcal{P}^{(p)}$, $p \in \mathcal{I}_2$, also, we can show that the maximum degree in each variable is 1. To see this, we proceed as follows. Recall that for $p \in \mathcal{I}_2$, $\mathbf{G}^{(p)} = \mathbf{T}^{(p)}\mathbf{P}$. Let us denote the $(i,j)^{\text{th}}$ entry of $\mathbf{G}^{(p)}$ by $g_{i,j}$. So each $g_{i,j} = \sum_l t_{i,l}p_{l,j}$, where $t_{i,l}$ refers to the $(i,l)^{\text{th}}$ entry of $\mathbf{T}^{(p)}$ and $p_{l,j}$ refers to the $(l,j)^{\text{th}}$ entry of $\mathbf{P}$. Using Laplace expansion, we have

$$\det \mathbf{G}_s^{(p)} = \sum_i (-1)^{i+j} g_{i,j} \det \mathbf{G}_{i,j}^{(p)}, \tag{119}$$

where $\det \mathbf{G}_{i,j}$ is the matrix obtained from $\mathbf{G}_s^{(p)}$ after removing the i^{th} row and the j^{th} column. Now, note that $\det \mathbf{G}_{i,j}$ is not a function of variables $\{t_{i,l}\}_l$ (which are indeed variables of $\mathbf{A}$), nor is it a function of variables $\{p_{l,j}\}_l$. Thus, the degree of $\mathcal{P}^{(p)}$ is at most 1 in each of the variables of $\mathbf{A}$ and $\mathbf{P}$.

Let us construct the polynomial $\mathcal{P} = \prod_{i\in\mathcal{I}}\mathcal{P}^{(i)}$. Each $\mathcal{P}^{(i)}$ is of degree at most 1 in each variable. So, the degree of $\mathcal{P}$ is at most K in each variable. From the sparse zeros lemma [37, Lemma 2.3], $\mathbb{F}$ need only be such that $|\mathbb{F}| \geq K$.

Appendix G
Proof of Lemma 10

Each virtual resource $v \in \mathcal{V}_{\mathcal{S}}$ can be emulated by one information symbol from any of the messages that are destined to all end-destinations of v; i.e., all messages $W_2^{\prime\mathcal{S}'}$ where $\mathcal{S}' \supseteq \mathcal{S}$. One can form a bipartite graph with the virtual resources as one set of nodes and the information symbols as the other set of nodes (see Fig. 16a). Each virtual resource is connected to those information symbols that can emulate it. These edges are shown in light colour in Fig. 16a. Therefore, all resources are emulatable if there exists a matching of size $\sum_{\mathcal{S}\subseteq\mathcal{I}_1}\beta_{\mathcal{S}}$ over the bipartite graph of Fig. 16a. The matching is shown via bold edges. It is well-known that there exists such a matching if and only if a flow of amount $\sum_{\mathcal{S}\subseteq\mathcal{I}_1}\beta_{\mathcal{S}}$ could be sent over the network of Fig. 16b from node A to node B. The min-cut separating nodes A and B is given by the following expression (see the proof of Lemma 4):

$$\min_{\substack{\forall \mathcal{S}\subseteq\mathcal{I}_1 \\ \Gamma \text{ superset saturated}}} \sum_{\mathcal{S}\in\Gamma}\alpha_{\mathcal{S}} + \sum_{\mathcal{S}\in\Gamma^c}\beta_{\mathcal{S}}. \tag{120}$$

It is easy to see that the flow value, $\sum_{\mathcal{S}\subseteq\mathcal{I}_1}\beta_{\mathcal{S}}$, is no more than this term provided that inequalities in (50) hold and, therefore, there is an assignment of information symbols to virtual resources so that all virtual resources are emulatable.

APPENDIX H
PROOF OF LEMMA 13

Let $\mathbf{\Lambda}$ be a multiset of $2^{\{1,2,3\}}$ with saturated pattern, $\mathbf{\Gamma}$ be a multi-set of $2^{\{1,2,3\}}$ with standard pattern, and $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ be balanced and such that $\mathbf{\Lambda} \neq \mathbf{\Gamma}$. We prove that no matter what $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ are, at least one of the cases of the table in Fig. 13 must hold for $\mathbf{\Lambda}$, and therefore a non-trivial elementary decompression of $\mathbf{\Lambda}$ is feasible.

Let us first count, in two different ways (once in $\mathbf{\Lambda}$ and once in $\mathbf{\Gamma}$), the number of times a set $\mathcal{S} \subseteq \mathcal{I}_1$ appears in the sets of multi-sets $\mathbf{\Lambda}$ and $\mathbf{\Gamma}$. First of all, define $n_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, to be the number of all sets $\Gamma \in \mathbf{\Gamma}$ that contain $\mathcal{S}$ as an element. One observes (from the standard pattern of multi-set $\mathbf{\Gamma}$) that $n_S = \sum_{i \in S} n_{\{i\}}$. Similarly, define m_Λ, $\Lambda \in \mathbf{\Lambda}$, to be the number of times the set Λ appears in the multi-set $\mathbf{\Lambda}$. For simplicity of notation, we use $m_{\Lambda\cup}$ to denote the number of all sets Λ' in $\mathbf{\Lambda}$ which are of the form $\Lambda' = \Lambda \cup \Sigma$ where $\Sigma \subseteq 2^{\mathcal{I}_1}$ is superset saturated, and $\Sigma \not\supseteq \Lambda$. For example, $m_{\{\{1,2\}\star\}\cup}$ counts the number of all sets such as $\{\{1,2\}\star\}$, $\{\{1,3\}\star, \{1,2\}\star\}$, $\{\{2,3\}\star, \{1,2\}\star\}$, $\{\{2,3\}\star, \{1,3\}\star, \{1,2\}\star\}$, and $\{\{3\} \star \{1,2\}\star\}$ in $\mathbf{\Lambda}$, but not $\{\{1\}\star\}$ or $\{\{1\}\star, \{3\}\star\}$.

Since multi-sets $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ are balanced, the number of sets in $\mathbf{\Gamma}$ which contain a set $\mathcal{S}$ is equal to the number of the sets in $\mathbf{\Lambda}$ which contain it. Thus, counting the number of sets in $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ which contain $\{i\}$ and $\{i,j\}$ as elements, we obtain the following relationship. In the following, we assume (i,j,k) to be a permutation of $(1,2,3)$.

$$n_{\{i\}} = m_{\{\{i\}\star\}\cup} \tag{121}$$

$$n_{\{i,j\}} = m_{\{\{i\}\star\}\cup} + m_{\{\{j\}\star\}\cup} - m_{\{\{i\}\star,\{j\}\star\}\cup} + m_{\{\{i,j\}\star\}\cup} \tag{122}$$

Since $n_{\{i,j\}} = n_{\{i\}} + n_{\{j\}}$, we conclude from (121) and (122) the following equation.

$$m_{\{\{i\}\star,\{j\}\star\}\cup} = m_{\{\{i,j\}\star\}\cup} \tag{123}$$

Similarly, counting the number of sets in $\mathbf{\Gamma}$ and $\mathbf{\Lambda}$ which contain $\{1,2,3\}$ as an element, we arrive at the following equation.

$$\begin{aligned} n_{\{1,2,3\}} \quad = \quad & m_{\{\{1\}\star\}\cup} + m_{\{\{2\}\star\}\cup} + m_{\{\{3\}\star\}\cup} + m_{\{\{1,2\}\star\}\cup} + m_{\{\{1,3\}\star\}\cup} + m_{\{\{2,3\}\star\}\cup} + \\ & + m_{\{\{1,2,3\}\star\}\cup} - m_{\{\{1\}\star,\{2\}\star\}\cup} - m_{\{\{1\}\star,\{3\}\star\}\cup} - m_{\{\{2\}\star,\{3\}\star\}\cup} - m_{\{\{1\}\star,\{2,3\}\star\}\cup} + \\ & - m_{\{\{2\}\star,\{1,3\}\star\}\cup} - m_{\{\{3\}\star,\{1,2\}\star\}\cup} - m_{\{\{1,2\}\star,\{1,3\}\star\}\cup} - m_{\{\{1,2\}\star,\{2,3\}\star\}\cup} + \\ & - m_{\{\{1,3\}\star,\{2,3\}\star\}\cup} + m_{\{\{1,2\}\star,\{1,3\}\star,\{2,3\}\star\}\cup} + m_{\{\{1\}\star,\{2\}\star,\{3\}\star\}\cup} \end{aligned} \tag{124}$$

Using $n_{\{1,2,3\}} = n_{\{1\}} + n_{\{2\}} + n_{\{3\}}$, equation (121) and equation (123) in equation (124), one obtains the following equation.

$$\begin{aligned} m_{\{\{1,2,3\}\star\}\cup} + m_{\{\{1\}\star,\{2\}\star,\{3\}\star\}\cup} \quad = \quad & m_{\{\{1\}\star,\{2,3\}\star\}\cup} + m_{\{\{2\}\star,\{1,3\}\star\}\cup} + m_{\{\{3\}\star,\{1,2\}\star\}\cup} + \\ & + m_{\{\{1,2\}\star,\{1,3\}\star\}\cup} + m_{\{\{1,2\}\star,\{2,3\}\star\}\cup} + m_{\{\{1,3\}\star,\{2,3\}\star\}\cup} \\ & - m_{\{\{1,2\}\star,\{1,3\}\star,\{2,3\}\star\}\cup} \end{aligned} \tag{125}$$

Now we write each $m_{\Lambda\cup}$ in terms of m_Λ's to derive the equation of our interest.

$$\begin{aligned} m_{\{\{1,2,3\}\star\}} + m_{\{\{1\}\star,\{2\}\star,\{3\}\star\}} \quad = \quad & m_{\{\{1\}\star,\{2,3\}\star\}} + m_{\{\{2\}\star,\{1,3\}\star\}} + m_{\{\{3\}\star,\{1,2\}\star\}} + m_{\{\{1,2\}\star,\{1,3\}\star\}} + \\ & + m_{\{\{1,2\}\star,\{1,3\}\star,\{2,3\}\star\}} + m_{\{\{1,2\}\star,\{2,3\}\star\}} + m_{\{\{1,2\}\star,\{1,3\}\star,\{2,3\}\star\}} + \\ & + m_{\{\{1,3\}\star,\{2,3\}\star\}} + m_{\{\{1,2\}\star,\{1,3\}\star,\{2,3\}\star\}} - m_{\{\{1,2\}\star,\{1,3\}\star,\{2,3\}\star\}} \\ = \quad & m_{\{\{1\}\star,\{2,3\}\star\}} + m_{\{\{2\}\star,\{1,3\}\star\}} + m_{\{\{3\}\star,\{1,2\}\star\}} + m_{\{\{1,2\}\star,\{1,3\}\star\}} + \\ & + m_{\{\{1,2\}\star,\{2,3\}\star\}} + m_{\{\{1,3\}\star,\{2,3\}\star\}} + 2m_{\{\{1,2\}\star,\{1,3\}\star,\{2,3\}\star\}} \end{aligned} \tag{126}$$

Observe from equality (126) that if there is a non-zero term, m_{Λ_1}, on the left hand, there is at least one other non-zero term, m_{Λ_2}, on the right hand of the equality. No matter what Λ_1 and Λ_2 are, see that we are in one of the decompression cases in the table in Fig. 13. If both sides of equality (126) are zero, then one concludes that $m_{\{\{i\}\star,\{j\}\star\}\cup} = m_{\{\{i\}\star,\{j\}\star\}}$ and $m_{\{\{i,j\}\star\}\cup} = m_{\{\{i,j\}\star\}}$ and therefore, by equation (123), we have another equation of interest.

$$m_{\{\{i\}\star,\{j\}\star\}} = m_{\{\{i,j\}\star\}} \tag{127}$$

Again, if $m_{\{\{i\}\star,\{j\}\star\}}$ is non-zero so is $m_{\{\{i,j\}\star\}}$, and we have the first case described in the table of Fig. 13.

We have proved that a non-trivial elementary decomposition is possible unless all terms in (126) and (127) are zero, and all terms in (126) and (127) are zero only if $\mathbf{\Lambda} = \mathbf{\Gamma}$ which contradicts the hypothesis.

APPENDIX I
PROOF OF LEMMA 15

Let us call the rate-region characterized in Theorem 1 (when $\mathcal{I}_1 = \{1,2,3\}$) region $\mathcal{R}_1$ and the rate-region obtained from relaxing inequality (30) to inequality (79) (when $\mathcal{I}_1 = \{1,2,3\}$) region $\mathcal{R}_2$. Clearly, $\mathcal{R}_1 \subseteq \mathcal{R}_2$. It is, therefore, sufficient to show that $\mathcal{R}_2 \subseteq \mathcal{R}_1$. Both rate-regions $\mathcal{R}_1$ and $\mathcal{R}_2$ are in terms of feasibility problems. In this sense, rate pair (R_1, R_2) belongs to $\mathcal{R}_1$ if and only if feasibility problem 1 (characterized by inequalities (30)-(34)) is feasible. Similarly, rate pair (R_1, R_2) belongs to $\mathcal{R}_2$ if and only if feasibility problem 2 (characterized by inequalities (79), (31)-(34)) is feasible.

In order to show that $\mathcal{R}_2 \subseteq \mathcal{R}_1$, we show that if (R_1, R_2) is such that there exists a solution, $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, to feasibility problem 2, then there also exists a solution $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, to feasibility problem 1. Note that problem 1 varies from problem 2 only in the non-negativity constraints on parameters $\alpha'_{\mathcal{S}}$, $\phi \neq \mathcal{S} \subseteq \mathcal{I}_1$. The goal is to construct parameters $\alpha'_{\mathcal{S}}$ (from parameters $\alpha_{\mathcal{S}}$) such that besides satisfying constraints (31)-(34), they all become non-negative except for α_ϕ.

We prove the existence of a solution $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq 2^{\mathcal{I}_1}$ by construction. This construction is done recursively. We start from a solution to feasibility problem 2, $\alpha_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, and, at each step, we propose a solution $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$ which is still a solution to feasibility problem 2 but is "strictly less negative" (excluding α_ϕ). So after enough number of steps, we end up with a set of parameters $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \mathcal{I}_1$, that satisfies (31)-(34) and also satisfies the non-negativity constraints in (30).

1. First, we set $\alpha'_{\mathcal{S}} = \alpha_{\mathcal{S}}$ for all $\mathcal{S} \subseteq \{1,2,3\}$. All $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2,3\}$, satisfy (31)-(34), (79). $\alpha_{\{1,2,3\}}$ is ensured to be non-negative by (79) (for $\Lambda = \{\{1,2,3\}\}$).
2. We then choose non-negative parameters $\alpha'_{\{i,j\}}$, $i, j \in \{1,2,3\}$. Without loss of generality, take the following three cases, and set $\alpha'_{\mathcal{S}}$'s as suggested (other cases are dealt with similarly).
   (a) If $\alpha_{\{1,2\}} < 0$ and $\alpha_{\{1,3\}} < 0$ and $\alpha_{\{2,3\}} < 0$:
   set $\alpha'_{\{1,2,3\}} = \alpha_{\{1,2,3\}} + \alpha_{\{1,2\}} + \alpha_{\{1,3\}} + \alpha_{\{2,3\}}$, $\alpha'_{\{1,2\}} = \alpha'_{\{1,3\}} = \alpha'_{\{2,3\}} = 0$, $\alpha'_{\{i\}} = \alpha_{\{i\}}$, for $i = 1,2,3$, and $\alpha'_\phi = \alpha_\phi$. One can verify that all $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2,3\}$, satisfy (31)-(34), (79). We outline this verification in the following. (31), (32), (34), and (79) clearly hold. We show how to verify (33) through an example, say, $\Lambda = \{\{1,2\},\{1,2,3\}\}$ and some $p \in \mathcal{I}_2$. From feasibility of problem 2, we know that $\alpha_{\mathcal{S}}$ is such that it satisfies (33) for all superset saturated subsets Λ, and in particular for $\Lambda = \{\{1,2\}\star, \{1,3\}\star, \{2,3\}\star\}$. So, we have

$$R_2 \leq \alpha_{\{1,2,3\}} + \alpha_{\{1,2\}} + \alpha_{\{1,3\}} + \alpha_{\{2,3\}} + \sum_{\mathcal{S} \in \{\phi,\{1\},\{2\},\{3\}\}} |\mathcal{E}_{\mathcal{S},p}| \tag{128}$$

$$= \alpha'_{\{1,2,3\}} + \sum_{\mathcal{S} \in \{\phi,\{1\},\{2\},\{3\}\}} |\mathcal{E}_{\mathcal{S},p}| \tag{129}$$

$$\leq \alpha'_{\{1,2,3\}} + \alpha'_{\{1,2\}} + \sum_{\mathcal{S} \in \{\{1,3\},\{2,3\},\phi,\{1\},\{2\},\{3\}\}} |\mathcal{E}_{\mathcal{S},p}|. \tag{130}$$

   (b) If $\alpha_{\{1,2\}} < 0$ and $\alpha_{\{1,3\}} < 0$:
   set $\alpha'_{\{1,2,3\}} = \alpha_{\{1,2,3\}} + \alpha_{\{1,2\}} + \alpha_{\{1,3\}}$, $\alpha'_{\{1,2\}} = \alpha'_{\{1,3\}} = 0$, $\alpha'_{\{2,3\}} = \alpha_{\{2,3\}}$, $\alpha'_{\{i\}} = \alpha_{\{i\}}$ for $i = 1,2,3$, and $\alpha'_\phi = \alpha_\phi$. Verify that all $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2,3\}$, satisfy (31)-(34), (79).
   (c) If $\alpha_{\{1,2\}} < 0$:
   set $\alpha'_{\{1,2,3\}} = \alpha_{\{1,2,3\}} + \alpha_{\{1,2\}} \geq 0$. $\alpha'_{\{1,2\}} = 0$, $\alpha'_{\{1,3\}} = \alpha_{\{1,3\}}$, $\alpha'_{\{2,3\}} = \alpha_{\{2,3\}}$, $\alpha'_{\{i\}} = \alpha_{\{i\}}$ for $i = 1,2,3$, and $\alpha'_\phi = \alpha_\phi$. Verify that all $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2,3\}$, satisfy (31)-(34), (79).
3. Finally, we choose non-negative parameters $\alpha'_{\{i\}}$, $i \in \{1,2,3\}$. This is done recursively, following the procedure below, for each $\alpha'_i < 0$, until all $\alpha'_{\{i\}}$, $i = 1,2,3$, are non-negative. δ is assumed a small enough positive number.
   (a) If $\alpha'_{\{i,j\}}, \alpha'_{\{i,k\}} > 0$:
   set $\alpha'_{\{i\}} = \alpha'_{\{i\}} + \delta$, $\alpha'_{\{i,j\}} = \alpha'_{\{i,j\}} - \delta$, $\alpha'_{\{i,k\}} = \alpha'_{\{i,k\}} - \delta$, $\alpha'_{\{1,2,3\}} = \alpha'_{\{1,2,3\}} + \delta$, and keep the rest of $\alpha'_{\mathcal{S}}$'s unchanged. Verify that all $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2,3\}$, satisfy (31)-(34), (79). We show (33) for one example: $\Lambda = \{\{1,2\}\star, \{1,3\}\star\}$ and some $p \in \mathcal{I}_2$. Since the $\alpha_{\mathcal{S}}$'s we start with satisfy (33) for any superset saturated Λ, and in particular for $\Lambda = \{\{1\}\star\}$, we have

$$R_2 \leq \alpha_{\{1\}} + \alpha_{\{1,2\}} + \alpha_{\{1,3\}} + \alpha_{\{1,2,3\}} + \sum_{\mathcal{S} \in \{\phi,\{2\},\{3\},\{2,3\}\}} |\mathcal{E}_{\mathcal{S},p}| \tag{131}$$

$$\leq \alpha'_{\{1\}} + \alpha'_{\{1,2\}} + \alpha'_{\{1,3\}} + \alpha'_{\{1,2,3\}} + \sum_{\mathcal{S} \in \{\phi,\{2\},\{3\},\{2,3\}\}} |\mathcal{E}_{\mathcal{S},p}| \tag{132}$$

$$\leq \alpha'_{\{1,2\}} + \alpha'_{\{1,3\}} + \alpha'_{\{1,2,3\}} + \sum_{\mathcal{S} \in \{\phi,\{2\},\{3\},\{2,3\}\}} |\mathcal{E}_{\mathcal{S},p}|, \tag{133}$$

   where the last inequality is because $\alpha'_{\{1\}}$ is either still negative, or has just become zero after adding the small δ.

(b) If $\alpha'_{\{i,j\}} = 0$, $\alpha'_{\{i,k\}} > 0$:
set $\alpha'_{\{i\}} = \alpha'_{\{i\}} + \delta$, $\alpha'_{\{i,k\}} = \alpha'_{\{i,k\}} - \delta$, and keep the rest of $\alpha'_{\mathcal{S}}$'s unchanged. Verify that all $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2,3\}$, satisfy (31)-(34), (79).

(c) If $\alpha'_{\{i,j\}} > 0$, $\alpha'_{\{i,k\}} = 0$:
set $\alpha'_{\{i\}} = \alpha'_{\{i\}} + \delta$, $\alpha'_{\{i,j\}} = \alpha'_{\{i,j\}} - \delta$, and keep the rest of $\alpha'_{\mathcal{S}}$'s unchanged. Verify that all $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2,3\}$, satisfy (31)-(34), (79).

(d) If $\alpha'_{\{i,j\}} = 0$, $\alpha'_{\{i,k\}} = 0$:
set $\alpha'_{\{i\}} = \alpha'_{\{i\}} + \delta$, $\alpha'_{\{1,2,3\}} = \alpha'_{\{1,2,3\}} - \delta$, and keep the rest of $\alpha'_{\mathcal{S}}$'s unchanged. Verify that all $\alpha'_{\mathcal{S}}$, $\mathcal{S} \subseteq \{1,2,3\}$, satisfy (31)-(34), (79).

Note that in step 1, we obtain a solution to feasibility problem 2 with $\alpha_{\{1,2,3\}} \geq 0$. After step 2, the solution is such that $\alpha_{\{1,2\}}, \alpha_{\{1,3\}}, \alpha_{\{2,3\}}, \alpha_{\{1,2,3\}}$ are all non-negative. In step 3, after each iteration, $\alpha_{\{1,2\}}, \alpha_{\{1,3\}}, \alpha_{\{2,3\}}, \alpha_{\{1,2,3\}}$ all remain non-negative and at the same time one negative $\alpha_{\{i\}}$ is increased. So after step 3, all parameters $\alpha_{\mathcal{S}}$, $\phi \neq S \subseteq \{1,2,3\}$, become non-negative. This is the solution to feasibility problem 1 that we were looking for.

REFERENCES

[1] T. Cover, "Comments on broadcast channels," IEEE Trans. Inf. Theory, vol. 44, no. 6, pp. 2524–2530, oct 1998.

[2] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204 –1216, jul 2000.

[3] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the gaussian multiple-input multiple-output broadcast channel," IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 3936 –3964, sept 2006.

[4] A. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow: A deterministic approach," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 1872 –1905, apr 2011.

[5] Y. Geng and C. Nair, "The capacity region of the two-receiver gaussian vector broadcast channel with private and common messages," IEEE Trans. Inf. Theory, vol. 60, no. 4, pp. 2087–2104, apr 2014.

[6] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," IEEE Trans. Inf. Theory, vol. 25, no. 3, pp. 306 – 311, may 1979.

[7] A. Gohari, A. El Gamal, and V. Anantharam, "On an outer bound and an inner bound for the general broadcast channel," in IEEE Int. Symp. Inf. Theory, jun 2010, pp. 540 –544.

[8] C. Nair and A. El Gamal, "An outer bound to the capacity region of the broadcast channel," IEEE Trans. Inf. Theory, vol. 53, no. 1, pp. 350 –355, jan 2007.

[9] Y. Liang, G. Kramer, and H. Poor, "On the equivalence of two achievable regions for the broadcast channel," IEEE Trans. Inf. Theory, vol. 57, no. 1, pp. 95 –100, jan 2011.

[10] T. Chan and A. Grant, "Entropy vectors and network codes," in IEEE Int. Symp. Inf. Theory, jun 2007, pp. 1586–1590.

[11] R. W. Yeung, Information Theory and Network Coding, 1st ed. Springer Publishing Company, 2008.

[12] L. Song, R. Yeung, and N. Cai, "Zero-error network coding for acyclic networks," IEEE Trans. Inf. Theory, vol. 49, no. 12, pp. 3129–3139, dec 2003.

[13] T. Cover, "Broadcast channels," IEEE Trans. Inf. Theory, vol. 18, no. 1, pp. 2 – 14, jan 1972.

[14] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," IEEE Trans. Inf. Theory, vol. 19, no. 2, pp. 197 – 207, mar 1973.

[15] K. Marton, "The capacity region of deterministic broadcast channels," in IEEE Int. Symp. Inf. Theory, 1977.

[16] M. S. Pinsker, "The capacity region of noiseless broadcast channels," Probl. Inf. Transm, vol. 14, pp. 97 – 102, 1974.

[17] J. Korner and K. Marton, "General broadcast channels with degraded message sets," IEEE Trans. Inf. Theory, vol. 23, no. 1, pp. 60 – 64, jan 1977.

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

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

[20] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," IEEE Trans. Inf. Theory, vol. 27, no. 1, pp. 49–60, jan 1981.

[21] H. F. Chong, M. Motani, H. K. Garg, and H. El Gamal, "On the Han-Kobayashi region for the interference channel," IEEE Trans. Inf. Theory, vol. 57, no. 7, pp. 3188–3195, Jul 2008.

[22] C. Nair and A. El Gamal, "The capacity region of a class of 3-receiver broadcast channels with degraded message sets," IEEE Trans. Inf. Theory, vol. 55, no. 10, pp. 4479–4493, oct 2009.

[23] S. Saeedi Bidokhti and V. Prabhakaran, "Is non-unique decoding necessary?" IEEE Trans. Inf. Theory, vol. 60, no. 5, pp. 2594–2610, may 2014.

[24] A. Ramamoorthy and R. D. Wesel, "The single source two terminal network with network coding," ArXiv e-prints, 2009, available on http://arxiv.org/abs/0908.2847.

[25] C. Ngai and R. Yeung, "Multisource network coding with two sinks," in Int. Conf. Commun., Circuits and Sys, vol. 1, jun 2004, pp. 34 – 37 Vol.1.

[26] 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.

[27] S. Diggavi and D. Tse, "On opportunistic codes and broadcast codes with degraded message sets," in IEEE Inf. Theory Workshop, mar 2006.

[28] S. Borade, L. Zheng, and M. Trott, "Multilevel broadcast networks," in IEEE Int. Symp. Inf. Theory, jun 2007, pp. 1151 –1155.

[29] V. Prabhakaran, S. Diggavi, and D. Tse, "Broadcasting with degraded message sets: A deterministic approach," in Annual Allerton Conf. on Commun., Control and Computing, 2007.

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

[31] S. Gheorghiu, S. Saeedi Bidokhti, C. Fragouli, and A. Toledo, "Degraded multicasting with network coding over the combination network," in IEEE Int. Symp. Network Coding, 2011, available on http://infoscience.epfl.ch/record/174452.

[32] S. Saeedi Bidokhti, Broadcasting and Multicasting Nested Message Sets. PhD dissertation, Ecole Polytechnique Fédéral de Lausanne, 2012.

[33] X. Xu and Y. L. Guan, "Joint routing and random network coding for multi-session networks," in IEEE Int. Conf. Networks, dec 2013, pp. 1–5.

[34] T. H. Chan and A. J. Grant, "Network coding capacity regions via entropy functions," ArXiv e-prints, 2012, available on http://arxiv.org/abs/1201.1062.

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

[36] F. Willems and E. van der Meulen, "The discrete memoryless multiple-access channel with cribbing encoders," IEEE Trans. Inf. Theory, vol. 31, no. 3, pp. 313 – 327, may 1985.

[37] C. Fragouli and E. Soljanin, "Network coding fundamentals," Foundations and Trends in Networking, vol. 2, no. 1, pp. 1–133, 2007. [Online]. Available: http://dx.doi.org/10.1561/1300000003

[38] P. Balister and B. Bollobás, "Projections, Entropy and Sumsets," ArXiv e-prints, Nov. 2007, available on http://adsabs.harvard.edu/abs/2007arXiv0711.1151B.

[39] A. El Gamal and Y. H. Kim, Network Information Theory. Cambridge University Press, 2011.