ISIT'2013 1569720029

A Block Markov Encoding Scheme for Broadcasting Nested Message Sets

Shirin Saeedi Bidokhti
TUM, Germany
shirin.saeedi@tum.de

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

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

***Abstract*—Encoding schemes for broadcasting two nested message sets are studied. We start with a simple class of deterministic broadcast channels for which (variants of) linear superposition coding are optimal in several cases [1], [2]. Such schemes are sub-optimal in general, and we propose a block Markov encoding scheme which achieves (for some deterministic channels) rates not achievable by the previous schemes in [1], [2]. We adapt this block Markov encoding scheme to general broadcast channels, and show that it achieves a rate-region which includes the previously known rate-regions[1].**

I. Introduction

Broadcast channels were formulated by Cover [3] as a model for the simultaneous transmission of information to multiple users. The problem of determining the capacity region is still open; but, results are available for many special cases (see [4] and the references therein).

One particular case of interest in broadcast scenarios is when nested (prioritized) messages are communicated; i.e, when a first message is destined for all users, a second message is destined for a subset of the users, a third message is destined for a subset of the subset of users, and so on. Such scenarios have recently drawn attention mostly due to their applications in video streaming for users with heterogeneous demands. Within this class of problems, the capacity region of the two-user broadcast channel was characterized in [5], where superposition coding was shown to be optimal. The case of 2-user multi-antenna Gaussian broadcast channel was explicitly derived in [6]. In [7], inner and outer bounds were derived for three receivers, and it was shown that the bounds match for a class of 3-receiver broadcast channels with two nested message sets. Also, the capacity region of linear deterministic broadcast channels with three receivers was derived in [8] .

In this work, we study delivery of two nested messages (a common and a private message) over channels with an arbitrary number of receivers, where a subset of the receivers (public receivers) demand only the common message and a subset of the receivers (private receivers) demand both the common and the private messages. We undertake a deterministic approach to this problem. Deterministic models have proved useful in finding approximate solutions and in giving insight on the development of new encoding techniques. The latter is the main focus of this paper. To this end, we start with particular linear deterministic models where we develop intuition together with new encoding techniques that may be generalized to general broadcast channels.

In [1], we studied linear deterministic channels with two public and any number of private receivers and gave a full characterization of the capacity region. The achievability proof in [1] uses techniques of rate splitting and linear superposition coding (the private message is broken into independent pieces and each piece is revealed to a subset of the public receivers through linear coding). In [2], we investigated the problem over combination networks [9] (which are a class of linear deterministic broadcast channels). In particular, [2] improves the (linear superposition encoding) scheme in [1] by employing a particular pre-encoding at the source. This scheme yields an inner bound to the capacity region of combination networks, which is tight for three (or fewer) public and any number of private receivers. In this paper, we first show that the aforementioned inner bound [2] is not tight in general. We then develop a new block Markov encoding scheme that (for some channels) achieves rates not achievable by the previous schemes in [2]. We further adapt this scheme to general broadcast channels and obtain a rate region that includes the previously known rate-regions. We do not know if this inclusion is strict.

II. A linear deterministic model

Linear deterministic broadcast channels form a special class of broadcast channels where the output signals are linear transformations of the input signal. This model is motivated by the MIMO Gaussian broadcast channel in the high SNR regime. The input to a linear deterministic broadcast channel is a signal X (which lies in a $d-$dimensional vector space $\mathbb{F}^d$, where $\mathbb{F}$ is a fixed finite field), and each output signal Y_i, $i = 1, \ldots, K$, is a linear transformations of the sent signal; i.e., $Y_i = \mathbf{H}_i X$, where $\mathbf{H}_i$ denotes the channel matrix whose elements are from a finite field $\mathbb{F}$. When working with linear deterministic channels, we express all rates in terms of $\log_2 |\mathbb{F}|$. Having all the channel matrices as row submatrices of the identity matrix, we arrive at a simple, yet rich, class of linear deterministic broadcast channels, *combination-network channels*. Combination-network channels have each of their outputs as a collection of the input symbols. This class of channels model the broadcast channel via a set of

[1]The work of S. Saeedi Bidokhti was supported by SNSF fellowship 146617. Vinod M. Prabhakaran's work was supported in part 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 award 1136174 and MURI award AFOSR FA9550-09-064.

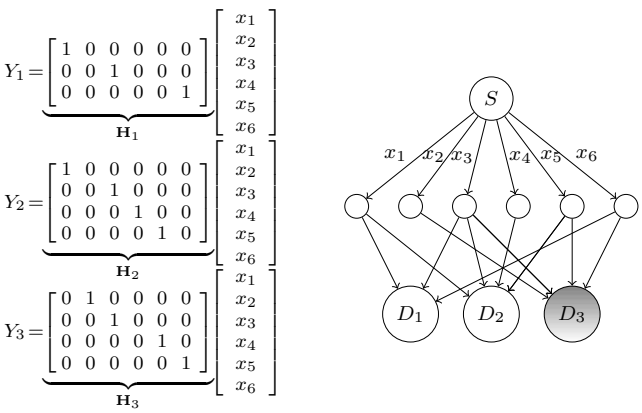

Fig. 1: A combination-network channel and its equivalent graphical description as a combination network.

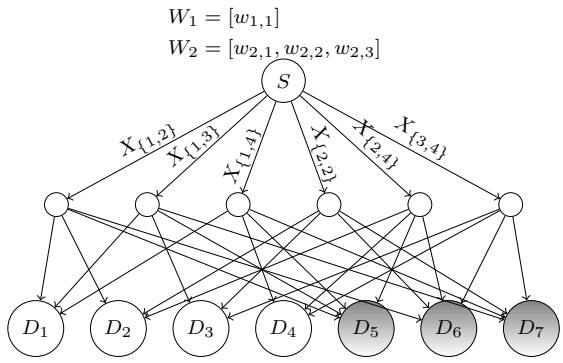

Fig. 2: Rate pair $(1, 3)$ is not within the rate-region of [2].

resources that are shared among the receivers (see Figure 1); in this regard, combination-network channels are (equivalently) represented by *combination networks* (and hence the name).

The problem of broadcasting messages to receivers which have (two) different demands over a shared media (such as the combination-network channel) is, in a sense, finding an optimal solution to a trade-off. This trade-off is imposed because on the one hand, public receivers need *only* enough information so that each can decode the common message. On the other hand, private receivers need to be able to decode both messages. It is, therefore, desirable from private receivers' point of view to have these messages fully mixed (when the number of private receivers is large) in contrast to the public receivers' decodability requirement. To optimally resolve this tension, one might need to reveal some *partial information* about the private message to the public receivers. One standard approach to do so is through rate splitting and superposition coding. This scheme essentially breaks the private information into independent pieces and reveals each piece to a subset of the public receivers. It turns out that one may, depending on the structure of the resources, achieve a rate gain by introducing dependency among the revealed partial (private) information.

One way of introducing such dependency is investigated in [2] through a particular pre-encoder at the source, which transforms the R_2 symbols of the private message into a larger number of dependent symbols through a random MDS (Maximum Distance Separable) matrix. The encoder then uses linear superposition coding to reveal pieces of this new pseudo private message to the public receivers. This scheme is optimal for three (or fewer) public and any number of private receivers.

In this section, we first show (through an example) that the aforementioned scheme [2] is not optimal in general and then develop a block Markov encoding scheme which achieves higher rates. We adapt this encoding scheme to general broadcast channels in the next section.

A. Notation

We index all receivers in a set $I = \{1, \ldots, K\}$ where public receivers are indexed by $I_1 = \{1, \ldots, m\}$ and private receivers are indexed by $I_2 = \{m+1, \ldots, K\}$. We refer to the outgoing edges of the source as the *resources* of the combination network and we denote them by a set $\mathcal{E}$. We denote the set of all resources that are connected to every public receiver in $S \subseteq I_1$ (and not connected to other public receivers) by $\mathcal{E}_S \subseteq \mathcal{E}$. Note that edges of set $\mathcal{E}_S$ may or may not be connected to the private receivers. We identify the subset of edges in $\mathcal{E}_S$ that are also connected to private receiver p, by $\mathcal{E}_S^p$. We denote the symbol carried over a resource edge e by x_e, which is a scalar from finite field $\mathbb{F}$. For $S \subseteq I_1$ and $p \in I_2$, we denote the set of all symbols carried over $\mathcal{E}_S$ (resp. $\mathcal{E}_S^p$) by X_S (resp. X_S^p) .

Finally, subset $\mathcal{T} \subseteq 2^{I_1}$ is called superset saturated if inclusion of set S in $\mathcal{T}$ implies inclusion of all its supersets (see [2]). In notation, we abbreviate a subset $\mathcal{T}$ by its few sets that are not implied by other sets in $\mathcal{T}$. E.g., among subsets of $2^{\{1,2,3\}}$, we denote $\{\{1\},\{1,2\},\{1,3\},\{1,2,3\}\}$ by $\{\{1\}\star\}$.

B. An example

Consider the combination network depicted in Figure 2, where a source wishes to communicate 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. It is not difficult to verify that splitting the private message into independent pieces and using linear superposition coding does not achieve the desired rate-pair. The pre-encoding technique of [2] does not make this communication possible either. However, rate-pair $(1, 3)$ is achievable by the following code design. $X_{\{1,2\}} = w_{1,1} + w_{2,1}$, $X_{\{2,3\}} = w_{1,1} + w_{2,3}$, $X_{\{1,3\}} = w_{1,1} + w_{2,2}$, $X_{\{2,4\}} = w_{1,1} + w_{2,1} + w_{2,3}$, $X_{\{1,4\}} = w_{1,1} + w_{2,1} + w_{2,2}$, and $X_{\{3,4\}} = w_{1,1} + w_{2,2} - w_{2,3}$.

The proposed code ensures decodability of the common and private messages at their intended receivers. Furthermore, the private information that is revealed to subsets (of public receivers) $\{1,2,3,4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}$ is null, 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 to $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$ is null. The dependency structure that is imposed among the partial private information is more involved than what the MDS pre-encoding scheme in [2] can support (see [10, Example 2.3] for details).

In the rest of this section, we develop a simple block Markov encoding scheme and characterize the rate-region it achieves.

C. A Block Markov Encoding Scheme

We start with the example in Figure 2, where rate-pair $(1,3)$ is not achievable by linear superposition coding, even after employing the pre-encoding technique of [2]. We show how to achieve this rate-pair through a block Markov encoding scheme, and hence, show that such a scheme could augment the achievable rate-region. Finally, we derive a new inner-bound to the capacity region for an arbitrary number of public and private receivers using a simple block Markov encoding.

Example 1. *Consider the combination network in Figure 2. Let us first extend it by adding one resource to the set $\mathcal{E}_{\{4\}}$, and connecting it to all private receivers (see Figure 3). One can verify that rate pair $(1,4)$ is achievable over this extended combination network, using linear superposition coding. An example of such a code is given below, where $[w_{1,1}]$ is a common message of rate $R_1 = 1$ and $[w'_{2,1}, w'_{2,2}, w'_{2,3}, w'_{2,4}]$ is a private message of rate $R'_2 = 4$. We assume that $|\mathbb{F}| > 2$.*

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

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 (1)*, receiver* 4 *decodes, besides the common message, three private information symbols ($w'_{2,1}$, $w'_{2,2}$, $w'_{2,4}$). Since all three symbols are ensured to be decoded at receiver* 4 *and all private receivers, any of them could undertake the role of 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 (1)*. 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 at the receivers, we perform backward decoding [11].*

So in n transmissions, we 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 achieve rate-pair $(1,3)$.

In Example 1, we constructed an achievable code with the help of an *extended combination network*. Let us first clarify what we mean by an extended combination network. An extended combination network is formed from the original combination network by adding some extra resource that we call *virtual resources*. Each virtual resource is connected to a subset of the receivers to which we refer as the end-destinations of that virtual resource. This subset is chosen, depending on the structure of the original combination network

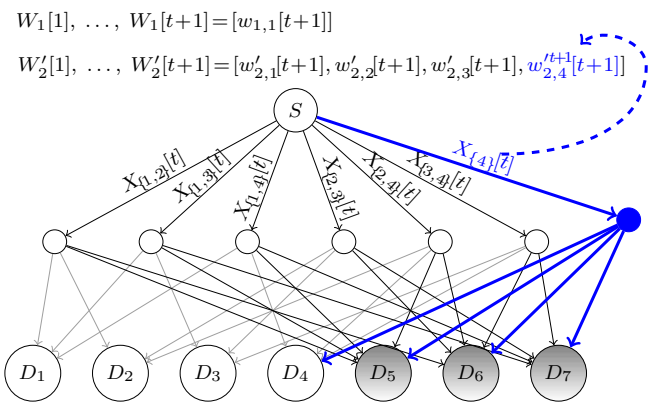

Fig. 3: The extended combination network of Example 1. A block Markov encoding scheme achieves rate pair $(1,3)$ over the original combination network. At time $t+1$, information symbol $w'^{t+1}_{2,4}$ contains the information of symbol $X^t_{\{4\}}$.

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 to decode the common and private messages in block t, each receiver needs the information that it will decode in block $t+1$ (recall that receivers performed backward decoding). So, the source wants to design the information that it is sending on the resources of the combination network in block t together with the information that the receiver will have in block $t+1$ (and will use in the decoding). This extra information is captured through the virtual resources of the extended combination network. In this regard, adding the virtual resources and forming the extended combination network is arbitrary, as long as the source can emulate them. More formally,

Definition 1 (Emulatable virtual resources)**.** *Given an extended combination network and a general broadcast code over it, a virtual resource v is called emulatable if the broadcast 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 messages) broadcast code over the extended combination network.
3) Use the broadcast code to make all virtual resources emulatable. More precisely, use the information symbols in block $t+1$ to also convey the content of the virtual resources in block t. Use the remaining information symbols to communicate the common and private messages.

An achievable rate-region could then be found by optimizing over the virtual resources and the broadcast code. Yet, one immediately spots the second step to be suspect, as it essentially

asks for the solution to a general broadcast problem.

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 broadcast code that we design over the extended combination network is a basic linear superposition code.

In order to devise our simple block Markov scheme, we first create an extended combination network by adding for every $S \subseteq I_1$, β_S many virtual resources which are connected to all private receivers and all the public receivers in $S \subseteq I_1$ (and only those). We denote this subset of virtual resources by $\mathcal{V}_S$.

Over this extended combination network, we then design a (more general) broadcast code. We say that a broadcast 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 α_S, $S \subseteq I_1$, to all public receivers in S and all private receivers. To design such a broadcast code, we use a basic linear superposition coding. Rate tuple $(R_1, \alpha_{\{1,\ldots,m\}}, \ldots, \alpha_\phi)$ is achievable if the following inequalities are satisfied [2].

Decodability constraints at public receiver $i \in I_1$ (2)

$$\sum_{\substack{S\subseteq I_1\\ S\ni i}} \alpha_S \le \sum_{S\in\mathcal{T}} \alpha_S + \sum_{\substack{S\in\mathcal{T}^c\\ S\ni i}} (|\mathcal{E}_S| + \beta_S) \quad \underset{\text{superset saturated}}{\forall \mathcal{T}\subseteq\{\{i\}\star\}}$$
$$R_1 + \sum_{\substack{S\subseteq I_1\\ S\ni i}} \alpha_S \le \sum_{\substack{S\subseteq I_1\\ S\ni i}} (|\mathcal{E}_S| + \beta_S)$$

Decodability constraints at private receiver $p \in I_2$ (3)

$$R_2' \le \sum_{S\in\mathcal{T}} \alpha_S + \sum_{S\in\mathcal{T}^c} (|\mathcal{E}_S^p| + \beta_S) \quad \underset{\text{superset saturated}}{\forall \mathcal{T}\subseteq 2^{I_1}}$$
$$R_1 + R_2' \le \sum_{S\subseteq I_1} (|\mathcal{E}_S^p| + \beta_S)$$

Now, given such a broadcast code, Lemma 1 provides conditions for the virtual resources to be emulatable. The proof is deferred to [10, Lemma 2.6].

Lemma 1. *Given an extended combination network with β_S virtual resources $\mathcal{V}_S$, $S \subseteq I_1$, and a broadcast code design that achieves rate tuple $(R_1, \alpha_{\{1,\ldots,m\}}, \ldots, \alpha_\phi)$, all virtual resources are emulatable provided that inequalities in* (4) *hold.*

$$\sum_{S\in\mathcal{T}} \beta_S \le \sum_{S\in\mathcal{T}} \alpha_S \quad \forall \mathcal{T} \subseteq 2^{I_1} \textit{superset saturated} \quad (4)$$

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 assigned to 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 $(R_1, R_2' - \sum_{S\subseteq I_1} \beta_S)$, where $R_2' = \sum_{S\subseteq I_1} \alpha_S$ and the real valued parameters α_S, $\beta_S \ge 0$ satisfy inequalities (2)-(4).

We have therefore characterized an achievable rate-region. To simplify the representation, we define $\gamma_S = \alpha_S - \beta_S$, $\forall S \subseteq I_1$, and then eliminate α's and β's from all inequalities involved. We thus have the following theorem.

Theorem 1. *Consider a combination network with m public receivers (indexed within set $I_1 = \{1, \ldots, m\}$) and an $K - m$ private receivers (indexed within set $I_2 = \{m+1, \ldots, K\}$). The rate pair (R_1, R_2) is achievable if there exist parameters γ_S, $S \subseteq I_1$, such that they satisfy the following inequalities.*

$$\sum_{S\in\mathcal{T}} \gamma_S \ge 0 \quad \forall \mathcal{T} \subseteq 2^{I_1} \textit{ superset saturated} \quad (5)$$

$$R_2 = \sum_{S\subseteq I_1} \gamma_S \quad (6)$$

Decodability constraints at public receiver $i \in I_1$ (7)

$$\sum_{\substack{S\subseteq I_1\\ S\ni i}} \gamma_S \le \sum_{S\in\mathcal{T}} \gamma_S + \sum_{\substack{S\in\mathcal{T}^c\\ S\ni i}} |\mathcal{E}_S| \quad \underset{\textit{superset saturated}}{\forall \mathcal{T}\subseteq\{\{i\}\star\}}$$
$$R_1 + \sum_{\substack{S\subseteq I_1\\ S\ni i}} \gamma_S \le \sum_{\substack{S\subseteq I_1\\ S\ni i}} |\mathcal{E}_S|$$

Decodability constraints at private receiver $p \in I_2$ (8)

$$R_2 \le \sum_{S\in\mathcal{T}} \gamma_S + \sum_{S\in\mathcal{T}^c} |\mathcal{E}_S^p| \quad \underset{\textit{superset saturated}}{\forall \mathcal{T}\subseteq 2^{I_1}}$$
$$R_1 + R_2 \le \sum_{S\subseteq I_1} |\mathcal{E}_S^p|.$$

Remark 1. *Comparing the rate-region in Theorem 1 and that derived in [2], one sees that the former has a more relaxed set of inequalities in* (6) *while the latter is more relaxed in inequalities* (8)*. It turns out that for $m \le 3$, the two rate-regions coincide and characterize the capacity region (See [10, Chapter 2]). For $m > 3$, the rate-region in Theorem 1 contains rate-pairs that are not attainable by previous schemes in [2].*

III. General Broadcast Channels

In the last section, we described a block Markov encoding scheme which was built on top of a linear superposition coding scheme. In terms of the achievable rate-region, this scheme relaxed the non-negativity constraints on the rate-split parameters, and allowed achievability of higher rates of transmission. In this section, we follow a similar line of arguments and investigate the potential of block Markov encoding schemes over general channels.

Let us consider a broadcast channel $p(y_1, \ldots, y_K|x)$ with input signal X, output signals $Y_1, \ldots, Y_K$ where Y_i, $i \in I_1$, is the signal available to public receiver i and Y_p, $p \in I_2$, is the signal available to private receiver p.

In all cases where the optimal rates of communication are known for broadcasting nested messages, the classical techniques of rate splitting and superposition coding have been 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^S of rates α_S, $S \subseteq I_1$, where W_2^S is revealed to all public receivers in S (as well as the private receivers). X is then formed by superposition coding. For $I_1 = \{1, 2\}$, 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 [12, Theorem 8.1]). The rate pair (R_1, R_2) is achievable if there exist parameters α_S, $S \subseteq I_1$, and auxiliary random variables $U_\mathcal{T}$, $\phi \ne \mathcal{T} \subseteq 2^{I_1}$, such that inequalities in (9)-(12) hold for a joint probability

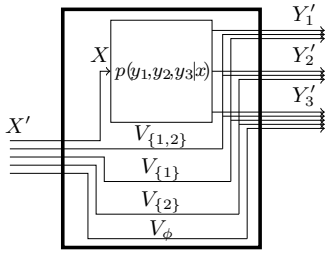

Fig. 4: The extended broadcast channel.

distribution $\prod_{k=1}^{K}\prod_{\substack{S\subseteq I_1\\|S|=k}} p(u_S|\{u_T\}_{\substack{T\in\{S\star\}\\T\neq S}})p(x|\{u_S\}_{\substack{S\subseteq I_1\\S\neq\phi}})$.

$$\alpha_S \geq 0 \qquad \forall S \subseteq I_1 \tag{9}$$

$$R_2 = \textstyle\sum_{S\subseteq I_1}\alpha_S \tag{10}$$

Decodability constraints at public receiver $i \in I_1$ (11)

$$\textstyle\sum_{\substack{S\subseteq I_1\\S\ni i}}\alpha_S \leq \sum_{S\in\mathcal{T}}\alpha_S + I(\cup_{\substack{S\subseteq I_1\\S\ni i}}U_S; Y_i|\cup_{S\in\mathcal{T}}U_S) \quad \substack{\forall\mathcal{T}\subseteq\{\{i\}\star\}\\ \text{superset saturated}}$$

$$R_1 + \textstyle\sum_{\substack{S\subseteq I_1\\S\ni i}}\alpha_S \leq I(\cup_{\substack{S\subseteq I_1\\S\ni i}}U_S; Y_i)$$

Decodability constraints at private receiver $p \in I_2$ (12)

$$R_2 \leq \textstyle\sum_{S\in\mathcal{T}}\alpha_S + I\left(X; Y_p|\cup_{S\in\mathcal{T}}U_S\right) \quad \substack{\forall\mathcal{T}\subseteq 2^{I_1}\\ \text{superset saturated}}$$

$$R_1 + R_2 \leq I(X; Y_p).$$

It turns out that a simple block Markov encoding scheme relaxes the constraints in (9) to the following set of constraints.

$$\textstyle\sum_{S\in\mathcal{T}}\alpha_S \geq 0 \quad \forall\mathcal{T}\subseteq 2^{I_1} \text{ superset saturated} \tag{13}$$

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 described in Figure 4. 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_S, $S \subseteq \{1,2\}$, takes its value in an alphabet set $\mathcal{V}_S$ of size 2^{β_S}. We call variables V_S the *virtual signals*.

2) We design a general broadcast code over the extended channel. We say that a broadcast 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 α'_S, $S \subseteq \{1,2\}$, to public receivers in S and all private receivers. We design such a broadcast 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 (11)-(12) (for parameters α'_S, auxiliary random variables $U'_\mathcal{T}$, $\phi \neq \mathcal{T} \subseteq 2^{I_1}$, and input/output signals X', Y_1', Y_2', Y_3').

3) We emulate the virtual signals. An extension to Lemma 1 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 Subsection II-C) yields 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 (10)-(13) is achievable. More precisely, we have the following theorem (details of the proof are deferred to [10, Theorem 4.3]).

Theorem 2. *The rate pair (R_1, R_2) is achievable if there exist parameters α_S, $S \subseteq I_1$, and auxiliary random variables $U_\mathcal{T}$, $\phi \neq \mathcal{T} \subseteq 2^{I_1}$, such that they satisfy inequalities in* (10)-(13) *for a joint probability distribution* $\prod_{k=1}^{K}\prod_{\substack{S\subseteq I_1\\|S|=k}} p(u_S|\{u_T\}_{\substack{T\in\{S\star\}\\T\neq S}})p(x|\{u_S\}_{\substack{S\subseteq I_1\\S\neq\phi}})$.

Note that the rate-region in Theorem 2 looks similar to that of superposition coding (see (9)-(12)). Clearly, the former rate-region has a less constrained set of non-negativity constraints on α_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. So it is possible that the proposed block Markov scheme strictly enlarges the rate-region of superposition coding. However, this needs further investigation.

Remark 2. *It is worthwhile to mention that one may design a more general coding scheme by using Marton's coding in the second step (when devising a broadcast code for the extended broadcast channel). Following similar steps as above (see [10, 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).*

REFERENCES

[1] S. Saeedi Bidokhti, S. Diggavi, C. Fragouli, and V. Prabhakaran, "On degraded two message set broadcasting," in Proc. IEEE Inf. Theory Workshop, Oct. 2009.

[2] S. Saeedi Bidokhti, V. Prabhakaran, and S. Diggavi, "On multicasting nested message sets over combination networks," in Proc. IEEE Inf. Theory Workshop, Sept 2012.

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

[4] ——, "Comments on broadcast channels," Inf. Theory, IEEE Trans., vol. 44, no. 6, pp. 2524 –2530, Oct. 1998.

[5] J. Korner and K. Marton, "General broadcast channels with degraded message sets," Inf. Theory, IEEE Trans., vol.23, no.1, pp. 60 – 64, Jan1977.

[6] H. Weingarten, Y. Steinberg, and S. Shamai, "On the capacity region of the multi-antenna broadcast channel with common messages," in Proc. IEEE Int. Symp. Inf. Theory, Jul 2006.

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

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

[9] C. K. Ngai and R. Yeung, "Network coding gain of combination networks," in Proc. IEEE Inf. Theory Workshop, Oct. 2004.

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

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

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