A Block Markov Encoding Scheme for Broadcasting Nested Message Sets

Shirin Saeedi, Vinod Prabhakaran and Suhas Diggavi

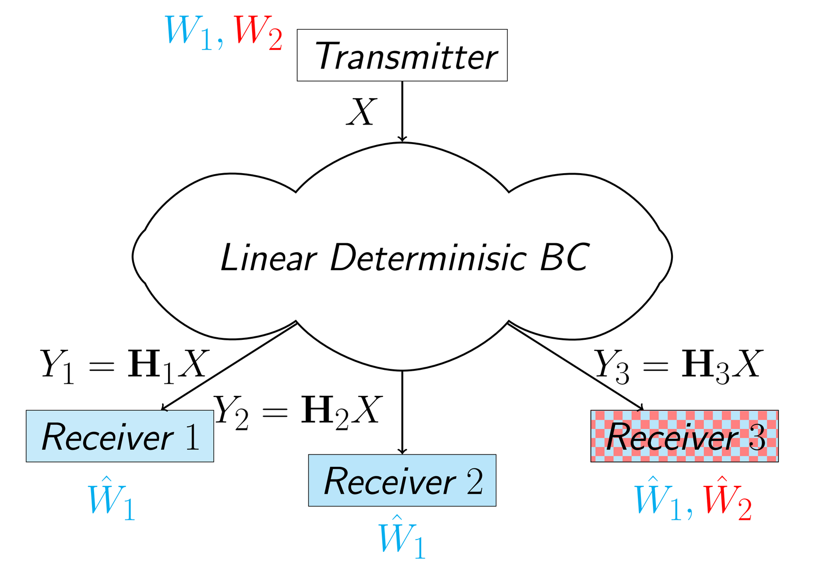
shirin.saeedi@tum.de, vinodmp@tifr.res.in, suhasdiggavi@ucla.edu

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. 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.

A Linear Deterministic Model

A common message W_1 of rate R_1 and a private message of rate R_2 are communicated over a broadcast channel (BC) towards K receivers.



m **Public receivers** demand W_1 and
$K-m$ **Private receivers** demand W_1, W_2.

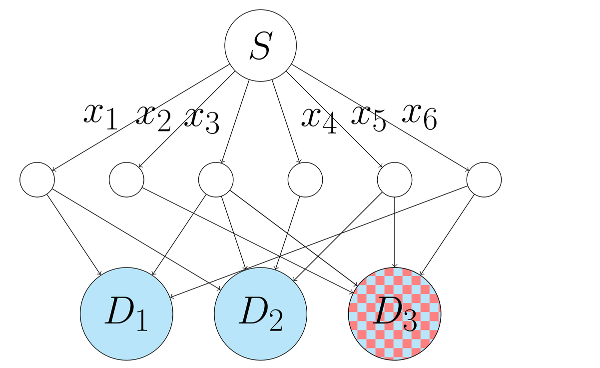
Motivation:

- Video Streaming to heterogeneous devices
- A first step towards multi-antenna(MIMO) BC

Assumptions:

- Channel matrices $\mathbf{H}_i$ take their elements over finite field $\mathbb{F}$.
- X lies in a $d-$dimensional vector space $\mathbb{F}^d$.
- The channel matrices are sub-matrices of the identity matrix.
- we express all rates in terms of $\log_2|\mathbb{F}|$.

$$Y_1 = \underbrace{\begin{bmatrix}100000\\001000\\000001\end{bmatrix}}_{\mathbf{H}_1}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\end{bmatrix},\ Y_2 = \underbrace{\begin{bmatrix}100000\\001000\\000100\\000010\end{bmatrix}}_{\mathbf{H}_2}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\end{bmatrix},\ Y_3 = \underbrace{\begin{bmatrix}010000\\001000\\000010\\000001\end{bmatrix}}_{\mathbf{H}_3}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\\x_5\\x_6\end{bmatrix}$$



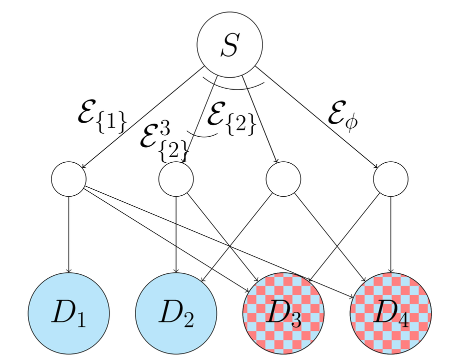
The Challenge

The underlying **trade-off**:

- 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 mixed.

To optimally resolve this tension, one might need to reveal some partial information about the private message to the public receivers.

Notation

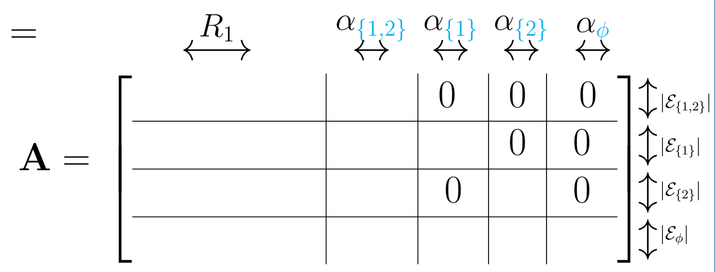


- I_1 : set of public receivers, I_2: set of private receivers.
- $\mathcal{E}_S$, $S \subseteq I_1$: resources connected to every (public) receiver in S and not to other public receivers.
- $\mathcal{E}^p_S$, $S \subseteq I_1$, $p \in I_2$: resources in $\mathcal{E}_S$ that are also connected to private receiver p.
- X_S: vectors of symbols carried over $\mathcal{E}_S$.
- X^p_S: vectors of symbols carried over $\mathcal{E}^p_S$.
- $X = \begin{bmatrix}X_{\{1,2\}}\\X_{\{2\}}\\X_{\{1\}}\\X_\phi\end{bmatrix}$.
- We call a subset $\mathcal{T}$ of 2^I_1 superset saturated if inclusion of a set S in $\mathcal{T}$ implies inclusion of all its supersets.

The Standard Approach: Linear Superposition Coding

Reveal partial information about the private message to public receivers through a zero-structured encoding matrix:

- Let $W = [w_{1,1}\dots w_{1,R_1} w_{2,1}\dots w_{2,R_2}]^T$.
- Let $X = \mathbf{A}W$.
- Each $Y_i = \mathbf{H}_i X$, $i = 1, \dots, K$.



A feasibility problem:

$$\alpha_{\{1,2\}}, \alpha_{\{2\}}, \alpha_{\{1\}}, \alpha_\phi \geq 0$$
$$R_2 = \alpha_{\{1,2\}} + \alpha_{\{2\}} + \alpha_{\{1\}} + \alpha_\phi$$

Decodability at public receivers

$$R_1 + \alpha_{\{1\}} + \alpha_{\{1,2\}} \leq \mathcal{E}_{\{1\}} + \mathcal{E}_{\{1,2\}}$$
$$R_1 + \alpha_{\{2\}} + \alpha_{\{1,2\}} \leq \mathcal{E}_{\{2\}} + \mathcal{E}_{\{1,2\}}$$

Decodability at private receiver p

$$R_2 \leq \mathcal{E}_\phi + \alpha_{\{1\}} + \alpha_{\{2\}} + \alpha_{\{1,2\}}$$
$$R_2 \leq \mathcal{E}^p_\phi + \mathcal{E}^p_{\{1\}} + \alpha_{\{2\}} + \alpha_{\{1,2\}}$$
$$R_2 \leq \mathcal{E}^p_\phi + \alpha_{\{1\}} + \mathcal{E}^p_{\{2\}} + \alpha_{\{1,2\}}$$
$$R_2 \leq \mathcal{E}^p_\phi + \mathcal{E}^p_{\{1\}} + \mathcal{E}^p_{\{2\}} + \alpha_{\{1,2\}}$$
$$R_1 + R_2 \leq \mathcal{E}^p_\phi + \mathcal{E}^p_{\{1\}} + \mathcal{E}^p_{\{2\}} + \mathcal{E}^p_{\{1,2\}}$$

Summarizing $\longrightarrow$

$$\alpha_S \geq 0 \quad \forall S \subseteq I_1$$
$$R_2 = \sum \alpha_S$$

$\forall i$: public receiver

$$R_1 + \sum_{S \ni i} \alpha_S \leq \sum_{S \ni i} |\mathcal{E}_S|$$

$\forall p$: private receiver

$$R_2 \leq \sum_{S \in \mathcal{T}} \alpha_S + \sum_{S \in \mathcal{T}^c} |\mathcal{E}^p_S| \quad \forall \mathcal{T} \subseteq 2^{I_1} \text{ superset saturated}$$
$$R_1 + R_2 \leq \sum_{S \subseteq I_1} |\mathcal{E}^p_S|$$

- The achievable scheme is generalizable.
- Optimal for $m = 2$ public and any number of private receivers.

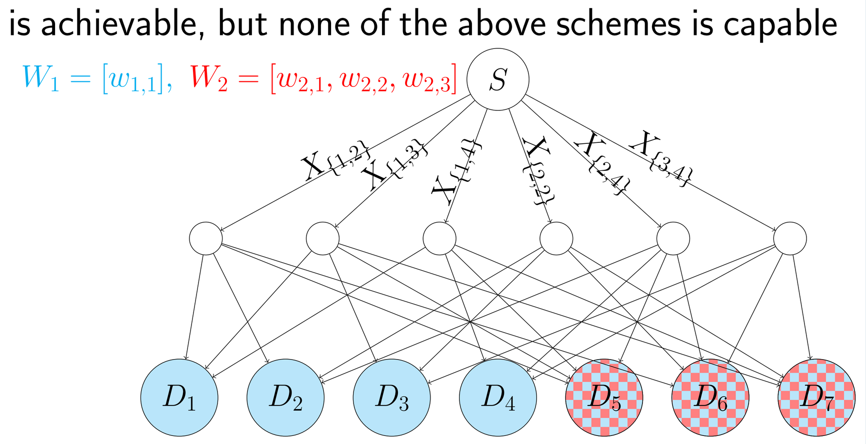
It turns out ...

- The above basic linear superposition scheme breaks the private information into independent pieces and reveals each piece to a subset of the public receivers.
- It turns out that one may achieve a rate gain by introducing some 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. Linear superposition coding is then used for this pseudo private message.
- This scheme is not optimal in general (for $m > 3$) and we propose a block Markov encoding scheme which strictly outperforms it.

An Example

- Rate pair $(R_1 = 1, R_2 = 3)$ is achievable, but none of the above schemes is capable of achieving it.

$$X_{\{1,2\}} = w_{1,1} + w_{2,1}$$
$$X_{\{2,3\}} = w_{1,1} + w_{2,3}$$
$$X_{\{1,3\}} = w_{1,1} + w_{2,2}$$
$$X_{\{2,4\}} = w_{1,1} + w_{2,1} + w_{2,3}$$
$$X_{\{1,4\}} = w_{1,1} + w_{2,1} + w_{2,2}$$
$$X_{\{3,4\}} = w_{1,1} + w_{2,2} - w_{2,3}$$

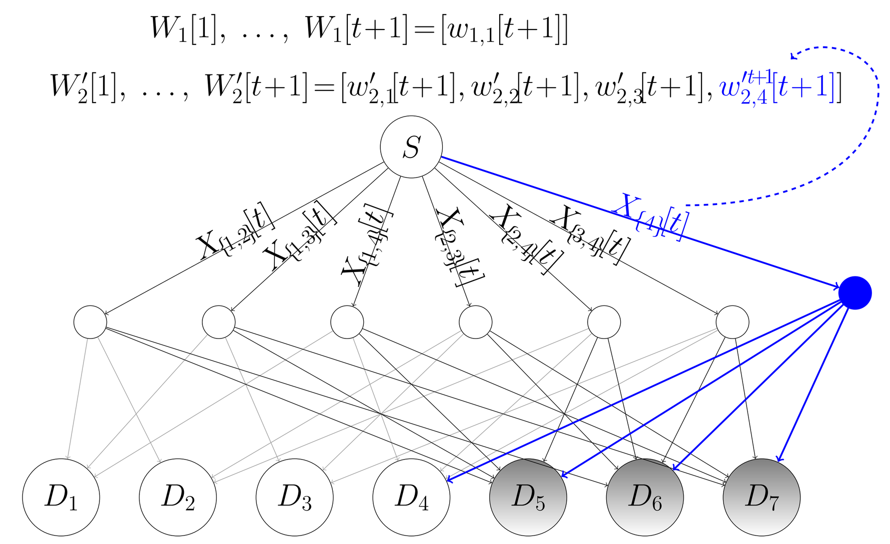


A Block Markov Encoding Scheme

- Extend the channel by introducing a "virtual resource" in $\mathcal{E}_{\{4\}}$.
- Rate Pair $(R'_1 = 1, R'_2 = 4)$ is achievable over this extended channel using the basic linear superposition coding. E.g., for $W'_1 = [w'_{1,1}]$ and $W'_2 = [w'_{2,1}, w'_{2,2}, w'_{2,3}, w'_{2,4}]$, the following code achieves rate pair $(R' = 1, R'_2 = 3)$.

$$\begin{array}{ll} X_{\{1,2\}} = w'_{1,1} + w'_{2,3} & X_{\{2,3\}} = w'_{1,1} + 2w'_{2,3} \\ X_{\{1,3\}} = 2w'_{1,1} + w'_{2,3} & X_{\{2,4\}} = w'_{1,1} + w'_{2,2} \\ X_{\{1,4\}} = w'_{1,1} + w'_{2,1} & X_{\{3,4\}} = w'_{1,1} + w'_{2,4} \\ X_{\{4\}} = w_{1,1} + w'_{2,1} + w'_{2,2} + w'_{2,4} & \end{array} \quad (1)$$

- Can we use the above code to achieve rate pair $(R_1 = 1, R_2 = 3)$ over the original channel?
- We emulate the virtual signal using a block Markov encoding scheme.
- In the t^{th} block, encoding is done as suggested by the code in (1). 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 $X_{\{4\}}[t]$. This symbol is ensured to be decoded at receiver 4 and the private receivers and it indeed emulates $\mathcal{E}_{\{4\}}$.
- In the n^{th} block, we simply encode $X_{\{4\}}[n-1]$ and directly send it to receiver 4 and the private receivers.
- Decoding is via backward decoding.



- This encoding technique can be applied more generally and results in an achievable rate-region which is strictly larger than those addressed in [1, 2].

Theorem 1. *The rate pair (R_1, R_2) is achievable if there exist parameters γ_S, $S \subseteq I_1$, such that*

Relaxed non-negativity constraints

$$\textstyle\sum_{S \in \mathcal{T}} \gamma_S \geq 0 \quad \forall \mathcal{T} \subseteq 2^{I_1} \text{ superset saturated}$$
$$R_2 = \textstyle\sum_{S \subseteq I_1} \gamma_S$$

Decodability at public receiver $i \in I_1$

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

Decodability at private receiver $p \in I_2$

$$R_2 \leq \textstyle\sum_{S \in \mathcal{T}} \gamma_S + \sum_{S \in \mathcal{T}^c} |\mathcal{E}^p_S| \quad \forall \mathcal{T} \subseteq 2^{I_1} \text{ superset saturated}$$
$$R_1 + R_2 \leq \textstyle\sum_{S \subseteq I_1} |\mathcal{E}^p_S|.$$

The General BC

Similarly, superposition coding can be enhanced via a block Markov scheme and achieve the following rate-region:

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 $U_\mathcal{T}$, $\phi \neq \mathcal{T} \subseteq 2^{I_1}$ (with joint pmf $\prod_{k=1}^{K} \prod_{\substack{S \subseteq I_1 \\ |S|=k}} p(u_S | \{u_T\}_{\substack{T \in \{S\star\} \\ T \neq S}}) p(x | \{u_S\}_{\substack{S \subseteq I_1 \\ S \neq \phi}})$) such that*

Relaxed non-negativity constraints

$$\textstyle\sum_{S \in \mathcal{T}} \alpha_S \geq 0 \quad \forall \mathcal{T} \subseteq 2^{I_1} \text{ superset saturated}$$
$$R_2 = \textstyle\sum_{S \subseteq I_1} \alpha_S$$

Decodability at public receiver $i \in I_1$

$$\sum_{\substack{S \subseteq I_1 \\ S \ni i}} \alpha_S \leq \sum_{S \in \mathcal{T}} \alpha_S + I(\cup_{\substack{S \subseteq I_1 \\ S \ni i}} U_S; Y_i | \cup_{S \in \mathcal{T}} U_S) \quad \forall \mathcal{T} \subseteq \{\{i\}\star\} \text{ superset saturated}$$
$$R_1 + \sum_{\substack{S \subseteq I_1 \\ S \ni i}} \alpha_S \leq I(\cup_{\substack{S \subseteq I_1, \\ S \ni i}} U_S; Y_i)$$

Decodability at private receiver $p \in I_2$

$$R_2 \leq \textstyle\sum_{S \in \mathcal{T}} \alpha_S + I\left(X; Y_p | \cup_{S \in \mathcal{T}} U_S\right) \quad \forall \mathcal{T} \subseteq 2^{I_1} \text{ superset saturated}$$
$$R_1 + R_2 \leq I(X; Y_p).$$

- This rate-region includes the rate-region of superposition coding. Whether or not this inclusion is strict needs further investigation.

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

LNT Institute for Communications Engineering

FNSNF Swiss National Science Foundation

tifr UCLA

Technische Universität München