

MIMO Broadcasting with Common, Private, and Confidential Messages: A Deterministic Approach

Hung D. Ly and Tie Liu

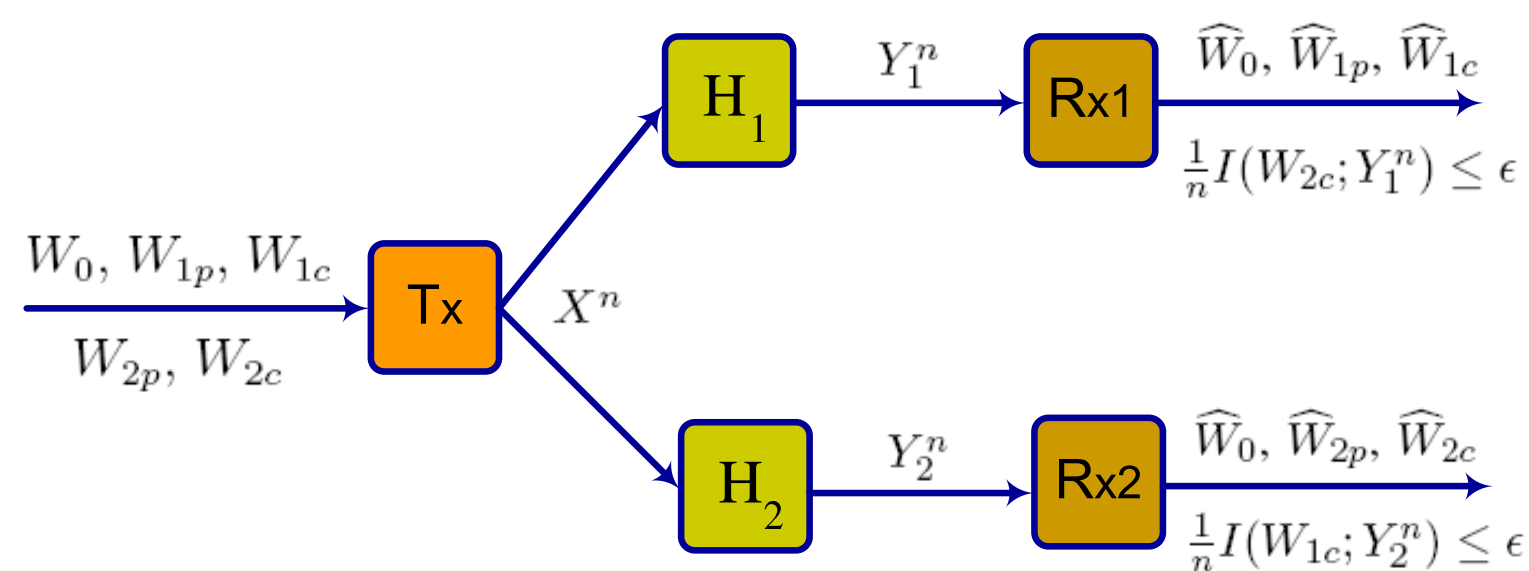
Department of Electrical and Computer Engineering, Texas A&M University, {hungly, tieliu}@ece.tamu.edu

Channel Model

At each time sample, the MIMO linear deterministic broadcast channel model can be written as:

$$Y_k = \mathbf{H}_k X, \quad k = 1, 2 \quad (1)$$

where \mathbf{H}_k is the channel matrix of size $n_k \times m$ for user k , X is the real input vector in a finite field \mathbb{F}^m , and Y_k is the signal received by user k . Let W_0 , W_{kp} , and W_{kc} be the common message, the private message for user k , and the confidential message for user k while assuming the other user as an eavesdropper, respectively.



Motivation

Characterizing the capacity region of the MIMO Gaussian broadcast channel with generalized message sets appears to be difficult. For example, a complete characterization of the capacity region of the MIMO Gaussian broadcast channel with common and private messages remains open. We therefore resort to a linear deterministic broadcast channel [1], which was originated from the recent development of a linear deterministic model for wireless channels and its connection to the Gaussian models.

Main Result

Theorem 1 The capacity region of the two-user MIMO linear deterministic broadcast channel with one common, two private, and two confidential messages is given by all the nonnegative rate tuples $(R_0, R_{1p}, R_{1c}, R_{2p}, R_{2c})$ that satisfy:

$$R_0 + R_{1p} + R_{1c} \leq r_1 \quad (2)$$

$$R_0 + R_{2p} + R_{2c} \leq r_2 \quad (3)$$

$$R_{1c} \leq r_{1,2} - r_2 \quad (4)$$

$$R_{2c} \leq r_{1,2} - r_1 \quad (5)$$

$$R_0 + R_{1p} + R_{1c} + R_{2p} + R_{2c} \leq r_{1,2} \quad (6)$$

where $r_k = \text{rank}(\mathbf{H}_k)$ and $r_{1,2} = \text{rank}\left(\begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}\right)$. Here, $(R_0, R_{1p}, R_{1c}, R_{2p}, R_{2c})$ are all expressed in terms of $\log_2 |\mathbb{F}|$ bits per sample.

The Converse

The inequalities (2) and (3) follow readily from the point-to-point consideration for users 1 and 2, respectively. The inequality (6) follows from the point-to-point consideration by letting user 1 and user 2 cooperate to decode the message. Following standard wiretap channel argument, we have

$$\begin{aligned} R_{1c} &\leq \max_{P(X)} [I(X; Y_1, Y_2) - I(X; Y_2)] \\ &= \max_{P(X)} I(X; Y_1 | Y_2) \\ &= \max_{P(X)} [H(Y_1 | Y_2) - H(Y_1 | X, Y_2)] \\ &\stackrel{(a)}{=} \max_{P(X)} H(Y_1 | Y_2) \\ &\stackrel{(b)}{\leq} r_{1,2} - r_2 \end{aligned}$$

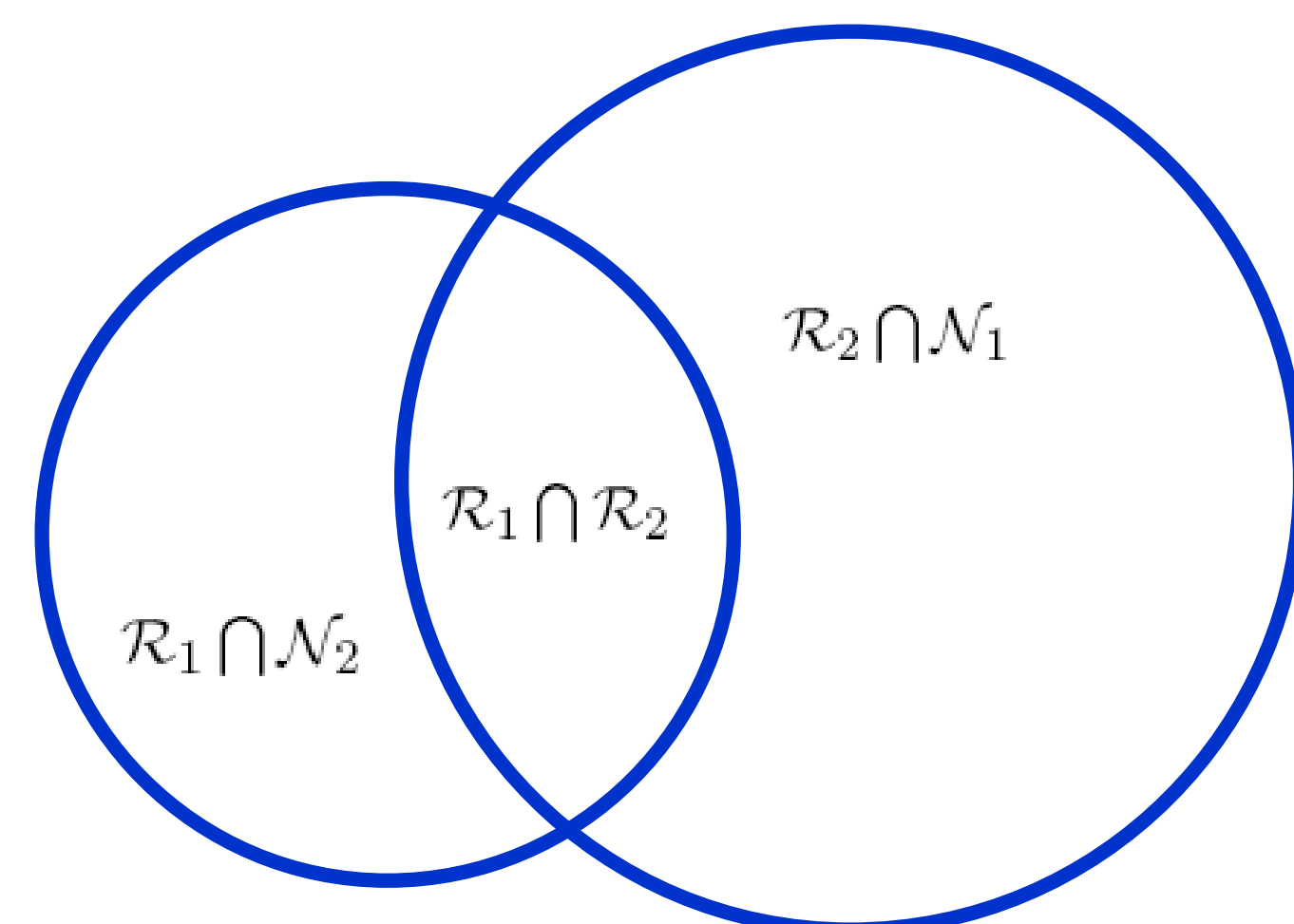
where (a) follows from $H(Y_1 | X, Y_2) = 0$ since the channel is deterministic, and (b) follows from the fact that the number of possible values for Y_1 given Y_2 is no more than $r_{1,2} - r_2$. The inequality (5) can be obtained in a similar fashion.

Achievability

We first consider a linear coding scheme with unit block length that achieves every integer rate tuple that satisfies the inequalities (2)-(6). The channel input X is given by:

$$X = \mathbf{B}_0 W_0 + \mathbf{B}_{1p} W_{1p} + \mathbf{B}_{2p} W_{2p} + \mathbf{B}_{1c} W_{1c} + \mathbf{B}_{2c} W_{2c}$$

where \mathbf{B}_0 , \mathbf{B}_{kp} , and \mathbf{B}_{kc} are the encoding matrices for the messages W_0 , W_{kp} , and W_{kc} , respectively. Let $\{b_i^{(1)}\}_{i=1}^{r_{1,2}-r_2}$, $\{b_i^{(2)}\}_{i=1}^{r_{1,2}-r_1}$, and $\{b_i^{(0)}\}_{i=1}^{r_1+r_2-r_{1,2}}$ be sets of basis vectors for the subspaces $\mathcal{R}_1 \cap \mathcal{N}_2$, $\mathcal{R}_2 \cap \mathcal{N}_1$, and $\mathcal{R}_1 \cap \mathcal{R}_2$, respectively. Here, \mathcal{R}_k and \mathcal{N}_k are the row and null spaces of \mathbf{H}_k , respectively.



Case 1

Suppose $R_0 \leq \dim(\mathcal{R}_1 \cap \mathcal{R}_2) = r_1 + r_2 - r_{1,2}$. We choose

$$\begin{aligned} \mathbf{B}_0 &= \begin{bmatrix} b_1^{(0)} & b_2^{(0)} & \dots & b_{R_0}^{(0)} \end{bmatrix} \\ \mathbf{B}_{1c} &= \begin{bmatrix} b_1^{(1)} & b_2^{(1)} & \dots & b_{R_{1c}}^{(1)} \end{bmatrix} \\ \mathbf{B}_{2c} &= \begin{bmatrix} b_1^{(2)} & b_2^{(2)} & \dots & b_{R_{2c}}^{(2)} \end{bmatrix} \\ \mathbf{B}_{1p} &= \begin{bmatrix} \mathbf{B}_{1p}^{(1)} & \mathbf{B}_{1p}^{(0)} \end{bmatrix} \\ \mathbf{B}_{2p} &= \begin{bmatrix} \mathbf{B}_{2p}^{(2)} & \mathbf{B}_{2p}^{(0)} \end{bmatrix} \end{aligned}$$

where

$$\begin{aligned} \mathbf{B}_{1p}^{(1)} &= \begin{bmatrix} b_{R_{1c}+1}^{(1)} & b_{R_{1c}+2}^{(1)} & \dots & b_{r_{1,2}-r_2}^{(1)} \end{bmatrix} \\ \mathbf{B}_{1p}^{(0)} &= \begin{bmatrix} b_{R_0+1}^{(0)} & b_{R_0+2}^{(0)} & \dots & b_{R_0+t_1}^{(0)} \end{bmatrix} \\ \mathbf{B}_{2p}^{(2)} &= \begin{bmatrix} b_{R_{2c}+1}^{(2)} & b_{R_{2c}+2}^{(2)} & \dots & b_{r_{1,2}-r_1}^{(2)} \end{bmatrix} \\ \mathbf{B}_{2p}^{(0)} &= \begin{bmatrix} b_{R_0+t_1+1}^{(0)} & b_{R_0+t_1+2}^{(0)} & \dots & b_{R_0+t_1+t_2}^{(0)} \end{bmatrix} \end{aligned}$$

and

$$\begin{aligned} t_1 &= R_{1p} + R_{1c} + r_2 - r_{1,2} \\ t_2 &= R_{2p} + R_{2c} + r_1 - r_{1,2}. \end{aligned}$$

The received signals at users 1 and 2 are given by:

$$Y_1 = \mathbf{H}_1 \begin{bmatrix} \mathbf{B}_0 & \mathbf{B}_{1p} & \mathbf{B}_{1c} & \mathbf{B}_{2p}^{(0)} \end{bmatrix} \begin{bmatrix} W_0 \\ W_{1p} \\ W_{1c} \\ W_{2p}^{(0)} \end{bmatrix} \quad (7)$$

$$Y_2 = \mathbf{H}_2 \begin{bmatrix} \mathbf{B}_0 & \mathbf{B}_{2p} & \mathbf{B}_{2c} & \mathbf{B}_{1p}^{(0)} \end{bmatrix} \begin{bmatrix} W_0 \\ W_{2p} \\ W_{2c} \\ W_{1p}^{(0)} \end{bmatrix} \quad (8)$$

From our construction, it is clear that both users can recover their desired messages by solving the linear equations (7) and (8), respectively. Note that in this case each user may also be able to partially decode the private message intended for the other user.

Conclusions

A complete characterization of the capacity region of the MIMO linear deterministic broadcast channel model is provided when there are two users and a set of five messages including one common, two private, and two confidential messages. The result will be used to obtain an approximate characterization of the capacity region of the MIMO Gaussian broadcast channel with generalized message sets.

Case 2

Suppose $R_0 > \dim(\mathcal{R}_1 \cap \mathcal{R}_2) = r_1 + r_2 - r_{1,2}$. We choose

$$\begin{aligned} \mathbf{B}_0 &= \begin{bmatrix} \mathbf{B}_0^{(0)} & \mathbf{B}_0^{(1)} + \mathbf{B}_0^{(2)} \end{bmatrix} \\ \mathbf{B}_{1c} &= \begin{bmatrix} b_1^{(1)} & b_2^{(1)} & \dots & b_{R_{1c}}^{(1)} \end{bmatrix} \\ \mathbf{B}_{2c} &= \begin{bmatrix} b_1^{(2)} & b_2^{(2)} & \dots & b_{R_{2c}}^{(2)} \end{bmatrix} \\ \mathbf{B}_{1p} &= \begin{bmatrix} b_{R_{1c}+1}^{(1)} & b_{R_{1c}+2}^{(1)} & \dots & b_{R_{1c}+R_{1p}}^{(1)} \end{bmatrix} \\ \mathbf{B}_{2p} &= \begin{bmatrix} b_{R_{2c}+1}^{(2)} & b_{R_{2c}+2}^{(2)} & \dots & b_{R_{2c}+R_{2p}}^{(2)} \end{bmatrix} \end{aligned}$$

where

$$\begin{aligned} \mathbf{B}_0^{(0)} &= \begin{bmatrix} b_1^{(0)} & b_2^{(0)} & \dots & b_{r_1+r_2-r_{1,2}}^{(0)} \end{bmatrix} \\ \mathbf{B}_0^{(1)} &= \begin{bmatrix} b_{R_{1c}+R_{1p}+1}^{(1)} & b_{R_{1c}+R_{1p}+2}^{(1)} & \dots & b_{R_{1c}+R_{1p}+t}^{(1)} \end{bmatrix} \\ \mathbf{B}_0^{(2)} &= \begin{bmatrix} b_{R_{2c}+R_{2p}+1}^{(2)} & b_{R_{2c}+R_{2p}+2}^{(2)} & \dots & b_{R_{2c}+R_{2p}+t}^{(2)} \end{bmatrix} \end{aligned}$$

and

$$t = R_0 + r_{1,2} - r_1 - r_2.$$

The received signal at user $k = 1, 2$ is given by:

$$Y_k = \mathbf{H}_k \begin{bmatrix} \mathbf{B}_0^{(0)} & \mathbf{B}_0^{(k)} & \mathbf{B}_{kp} & \mathbf{B}_{kc} \end{bmatrix} \begin{bmatrix} W_0^{(0)} \\ W_0^{(1,2)} \\ W_{kp} \\ W_{kc} \end{bmatrix} \quad (9)$$

where $W_0^{(0)}$ is the message vector formed by the first $r_1 + r_2 - r_{1,2}$ entries in W_0 and $W_0^{(1,2)}$ is the message vector formed by the rest of the entries in W_0 .

The achievability of the rational rate tuples that satisfy the inequalities (2)-(6) can be proved by extending the above linear coding scheme to block length n such that $(nR_0, nR_{1p}, nR_{1c}, nR_{2p}, nR_{2c})$ is an integer rate tuple. The achievability of the general rate tuples that satisfy the inequalities (2)-(6) follows from the fact that rational numbers are dense in the real line.

References

- [1] S. Avestimehr, S. N. Diggavi, D. N. C. Tse, "Wireless network information flow," in Proc. 45th Annual Allerton Conf. Comm., Contr., Comp., Monticello, IL, Sept. 2007.
- [2] V. Prabhakaran, S. N. Diggavi, D. N. C. Tse, "Broadcasting with degraded message sets: A deterministic approach," in Proc. 45th Annual Allerton Conf. Comm., Contr., Comp., Monticello, IL, Sept. 2007.