Degrees of Freedom Region of the Gaussian MIMO Broadcast Channel with Common and Private Messages

Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
ersen@umd.edu *ulukus@umd.edu*

***Abstract*— We obtain the degrees of freedom region of the Gaussian multiple-input multiple-output (MIMO) broadcast channel with common and private messages. We first show that a parallel Gaussian broadcast channel with unmatched sub-channels can be constructed from any given Gaussian MIMO broadcast channel by using the generalized singular value decomposition (GSVD) and a relaxation on the power constraint for the channel input, in a way that the capacity region of the constructed parallel channel provides an outer bound for the capacity region of the original channel. The capacity region of the parallel Gaussian broadcast channel with unmatched sub-channels is known, using which we obtain an explicit outer bound for the degrees of freedom region of the Gaussian MIMO broadcast channel. We finally show that this outer bound for the degrees of freedom region can be attained by the achievable scheme that uses a classical Gaussian coding for the common message and dirty-paper coding (DPC) for the private messages.**

I. Introduction

We study the two-user Gaussian multiple-input multiple-output (MIMO) broadcast channel with common and private messages, where the transmitter sends a private message to each user in addition to a common message which is directed to both users. The capacity region of this channel is not known completely. However, when one of the three messages is absent, the corresponding capacity region is known. In particular, the capacity region is known when there is no common message [1], and when there is only one private message [2], [3].

The first work that considers the Gaussian MIMO broadcast channel with common and private messages is [4]. Reference [4] proposes an achievable scheme which uses a classical Gaussian coding scheme for the common message, and dirty-paper coding (DPC) for the private messages. The corresponding achievable rate region is called the DPC region. In addition, [4] obtains the capacity region when the Gaussian MIMO broadcast channel is equivalent to a set of parallel independent Gaussian channels using the results from [5]. The Gaussian MIMO broadcast channel with common and private messages is further studied in [2], [3]. References [2], [3] propose an outer bound for the capacity region of the Gaussian MIMO broadcast channel with common and private messages, which matches the DPC region given in [4] partially. Moreover, [2], [3] show that for a given common message rate, the DPC region achieves the private message sum capacity. Finally, [2], [3] show the optimality of the DPC region in [4] when the common message rate is beyond a certain threshold.

A recent work is [6], where we first obtain an outer bound for the capacity region of the two-user discrete memoryless broadcast channel with common and private messages. We next show that if jointly Gaussian random variables are sufficient to evaluate this outer bound for the Gaussian MIMO case, the DPC region is the capacity region of the Gaussian MIMO broadcast channel with common and private messages. However, we can evaluate only a loosened version of this outer bound, which results in that, extending the DPC region in the common message rate direction by a fixed amount yields an outer bound for the capacity region of the Gaussian MIMO broadcast channel with common and private messages. However, this fixed amount (gap) is not finite for all channels.

Here, we follow a different approach, and establish the degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages. We first show that we can construct a parallel Gaussian broadcast channel with unmatched sub-channels [5] from any given Gaussian MIMO broadcast channel such that the capacity region of this parallel Gaussian broadcast channel with unmatched sub-channels includes the capacity region of the Gaussian MIMO broadcast channel. To construct such a parallel channel, we use the generalized singular value decomposition (GSVD) [7] on the channel gain matrices of the Gaussian MIMO broadcast channel and also relax the power constraint on the channel input. This relaxation on the power constraint is the reason why the capacity region of the parallel channel gives an outer bound for the capacity region of the original MIMO broadcast channel. Consequently, the capacity region of the constructed parallel channel provides an outer bound for the capacity region of the Gaussian MIMO channel. Since the capacity region of the parallel Gaussian broadcast channel with unmatched sub-channels is known [5], we are able to characterize the degrees of freedom region of the parallel Gaussian broadcast channel with unmatched sub-channels, which serves as an outer bound for the degrees of freedom

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

region of the Gaussian MIMO broadcast channel. We next show that this outer bound for the degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages can be attained by a proper selection of the covariance matrices involved in the DPC region.

II. Channel Model and Definitions

The Gaussian MIMO broadcast channel is defined by

$$\mathbf{Y}_1 = \mathbf{H}_1\mathbf{X} + \mathbf{N}_1 \tag{1}$$
$$\mathbf{Y}_2 = \mathbf{H}_2\mathbf{X} + \mathbf{N}_2 \tag{2}$$

where the channel input $\mathbf{X}$ is a $t \times 1$ column vector, $\mathbf{H}_j$ is the jth user's channel gain matrix of size $r_j \times t$, $\mathbf{Y}_j$ is the channel output of the jth user, and the Gaussian random vector $\mathbf{N}_j$ is of size $r_j \times 1$ with an identity covariance matrix. The channel input is subject to an average power constraint as follows

$$E\left[\mathbf{X}^\top \mathbf{X}\right] = \mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\right) \leq P \tag{3}$$

We study the Gaussian MIMO broadcast channel for the scenario where the transmitter sends a common message to both users, and a private message to each user. We call the channel model arising from this scenario the *Gaussian MIMO broadcast channel with common and private messages*.

An $(n, 2^{nR_0}, 2^{nR_1}, 2^{nR_2})$ code for this channel consists of three message sets $\mathcal{W}_j = \{1, \ldots, 2^{nR_j}\}$, $j = 0, 1, 2$, one encoder $f_n : \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, one decoder at each receiver $g_n^j : \mathcal{Y}_j^n \to \mathcal{W}_0 \times \mathcal{W}_j$, $j = 1, 2$. The probability of error is defined as $P_e^n = \max\{P_{e1}^n, P_{e2}^n\}$, where $P_{ej} = \Pr[g_n^j(f_n(W_0, W_1, W_2)) \neq (W_0, W_j)]$, $j = 1, 2$, and W_j is the message which is a uniformly distributed random variable in $\mathcal{W}_j$, $j = 0, 1, 2$. A rate triple (R_0, R_1, R_2) is said to be achievable if there exists a code $(n, 2^{nR_0}, 2^{nR_1}, 2^{nR_2})$ which has $\lim_{n\to\infty} P_e^n = 0$. The capacity region $\mathcal{C}(P)$ is defined as the convex closure of all achievable rate triples (R_0, R_1, R_2).

We investigate how the capacity region $\mathcal{C}(P)$ behaves when the available power at the transmitter P is arbitrarily large, i.e., P goes to infinity. This investigation can be carried out by obtaining the degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages. A degrees of freedom triple (d_0, d_1, d_2) is said to be achievable if there exists a rate triple $(R_0, R_1, R_2) \in \mathcal{C}(P)$ such that

$$d_j = \lim_{P\to\infty} \frac{R_j}{\frac{1}{2}\log P}, \quad j = 0, 1, 2 \tag{4}$$

The degrees of freedom region $\mathcal{D}$ is defined as the convex closure of all achievable degrees of freedom triples (d_0, d_1, d_2).

We conclude this section by presenting the achievable rate region, hereafter called the *DPC region*, given in [4]. In the achievable scheme in [4], the common message is encoded by a standard Gaussian codebook, and the private messages are encoded by DPC. Each user decodes the common message by treating the signals carrying the private messages as noise. Next, users decode their private messages. Since DPC is used to encode the private messages, one of the users observes an interference-free link depending on the encoding order at the transmitter. We define

$$R_{0j}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{H}_j(\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2)\mathbf{H}_j^\top + \mathbf{I}|}{|\mathbf{H}_j(\mathbf{K}_1 + \mathbf{K}_2)\mathbf{H}_j^\top + \mathbf{I}|}, \quad j = 1, 2 \tag{5}$$

$$R_1(\mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1 + \mathbf{K}_2)\mathbf{H}_1^\top + \mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top + \mathbf{I}|} \tag{6}$$

$$R_2(\mathbf{K}_2) = \frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2 + \mathbf{I}| \tag{7}$$

where $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2$ denote the covariance matrices allotted for the common message, the first user's private message, and the second user's private message, respectively. The DPC region is stated in the following theorem.

Theorem 1 ([4]) *The rate triples (R_0, R_1, R_2) lying in the DPC region*

$$\mathcal{R}^{\mathrm{DPC}}(P) = \mathrm{conv}\left(\mathcal{R}_1^{\mathrm{DPC}}(P) \cup \mathcal{R}_2^{\mathrm{DPC}}(P)\right) \tag{8}$$

are achievable, where conv *is the convex hull operator, $\mathcal{R}_1^{\mathrm{DPC}}(P)$ consists of rate triples (R_0, R_1, R_2) satisfying*

$$R_0 \leq R_{0j}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2), \quad j = 1, 2 \tag{9}$$
$$R_1 \leq R_1(\mathbf{K}_1, \mathbf{K}_2) \tag{10}$$
$$R_2 \leq R_2(\mathbf{K}_2) \tag{11}$$

for some positive semi-definite matrices $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2$ such that $\mathrm{tr}(\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2) \leq P$, and $\mathcal{R}_2^{\mathrm{DPC}}(P)$ can be obtained from $\mathcal{R}_1^{\mathrm{DPC}}(P)$ by swapping the subscripts 1 and 2.

The DPC region is tight in several cases. The first one is the case where each receiver gets only a private message, i.e., $R_0 = 0$ [1]. The other case is the degraded message set scenario in which we have either $R_1 = 0$ or $R_2 = 0$ [2]. In both of these cases, there are only two messages to be sent. Furthermore, the DPC region is known to be partially tight for the case when both private messages and a common message are present [2], [3]. However, it is still unknown whether the DPC region is equal to the capacity region of the Gaussian MIMO broadcast channel with common and private messages.

III. Main Result

We now present our main result which characterizes the degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages. Our result shows that this degrees of freedom region can be attained by the DPC region in Theorem 1, i.e., the DPC region in Theorem 1 is asymptotically tight. Before stating our main result, we introduce the generalized singular value decomposition (GSVD) [7] which plays a crucial role in the proof of our main result, and provides the necessary notation to express this result.

Definition 1 ([7], Theorem 1) *Given two matrices $\mathbf{H}_1 \in \mathbb{R}^{r_1 \times t}$ and $\mathbf{H}_2 \in \mathbb{R}^{r_2 \times t}$, there exist orthonormal matrices $\mathbf{\Psi}_1 \in \mathbb{R}^{r_1 \times r_1}, \mathbf{\Psi}_2 \in \mathbb{R}^{r_2 \times r_2}, \mathbf{\Psi}_t \in \mathbb{R}^{t \times t}$, a non-singular, lower triangular matrix $\mathbf{\Omega} \in \mathbb{R}^{k \times k}$, and two matrices $\mathbf{\Sigma}_1 \in \mathbb{R}^{r_1 \times k}, \mathbf{\Sigma}_2 \in \mathbb{R}^{r_2 \times k}$ such that*

$$\mathbf{\Psi}_j^\top \mathbf{H}_j \mathbf{\Psi}_t = \mathbf{\Sigma}_j \left[\begin{array}{cc} \mathbf{\Omega}^{-1} & \mathbf{0}_{k \times t-k} \end{array}\right], \quad j = 1, 2 \tag{12}$$

where $\mathbf{\Sigma}_1$ *and* $\mathbf{\Sigma}_2$ *are given by*

$$\mathbf{\Sigma}_1 = \begin{bmatrix} \mathbf{I}_{k-p-s \times k-p-s} & & \\ & \mathbf{D}_{1,s\times s} & \\ & & \mathbf{0}_{r_1+p-k \times p} \end{bmatrix} \quad (13)$$

$$\mathbf{\Sigma}_2 = \begin{bmatrix} \mathbf{0}_{r_2-p-s \times k-p-s} & & \\ & \mathbf{D}_{2,s\times s} & \\ & & \mathbf{I}_{p\times p} \end{bmatrix} \quad (14)$$

and the constants k, p *are given as*

$$k = \text{rank}\left(\begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix} \right) \quad (15)$$

$$p = \dim\left(\text{Null}(\mathbf{H}_1) \cap \text{Null}(\mathbf{H}_2)^{\perp}\right) \quad (16)$$

and s depends on the matrices $\mathbf{H}_1, \mathbf{H}_2$*. The matrices* $\mathbf{D}_1, \mathbf{D}_2$ *are diagonal with the diagonal elements being strictly positive.*

We define the sets $\mathcal{S}_1, \mathcal{S}_c, \mathcal{S}_2$ as follows

$$\mathcal{S}_1 = \{1, \ldots, k-p-s\} \quad (17)$$

$$\mathcal{S}_c = \{k-p-s+1, \ldots, k-p\} \quad (18)$$

$$\mathcal{S}_2 = \{k-p+1, \ldots, k\} \quad (19)$$

Our main result is stated in the following theorem.

Theorem 2 *The degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages is given by the union of degrees of freedom triples* (d_0, d_1, d_2) *satisfying*

$$d_0 \leq |\mathcal{S}_c| - \alpha_1 - \alpha_2 + \beta \quad (20)$$

$$d_1 \leq \alpha_1 + |\mathcal{S}_1| - \beta \quad (21)$$

$$d_2 \leq \alpha_2 + |\mathcal{S}_2| - \beta \quad (22)$$

for some non-negative $\alpha_1, \alpha_2, \beta$ *such that* $\alpha_1 + \alpha_2 \leq |\mathcal{S}_c|$*,* $\beta \leq \min\{|\mathcal{S}_1|, |\mathcal{S}_2|\}$*. Moreover, the degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages can be attained by the DPC region given in Theorem 1.*

This theorem states that if the available power P is sufficiently large, the Gaussian MIMO broadcast channel behaves as if it is a parallel Gaussian broadcast channel with $|\mathcal{S}_1| + |\mathcal{S}_c| + |\mathcal{S}_2|$ sub-channels. $|\mathcal{S}_1|$ (resp. $|\mathcal{S}_2|$) of these sub-channels can be accessed by only the first (resp. second) user and $|\mathcal{S}_c|$ of these sub-channels can be accessed by both users. For a fixed $(\alpha_1, \alpha_2, \beta)$, $|\mathcal{S}_c| - \alpha_1 - \alpha_2$ of the sub-channels that both users can access need to be used for the transmission of the common message in addition to β of the $|\mathcal{S}_1|$ sub-channels that only the first user can access and β of the $|\mathcal{S}_2|$ sub-channels that only the second user can access. Thus, each user gets the common message over $|\mathcal{S}_c| - \alpha_1 - \alpha_2$ common sub-channels, which can be observed by both users, and β private sub-channels, which can be observed by only one user. This leads to a $\beta + |\mathcal{S}_c| - \alpha_1 - \alpha_2$ degrees of freedom for the common message. The first user's message needs to be transmitted over α_1 of the $|\mathcal{S}_c|$ sub-channels that are observed by both users, and the remaining $|\mathcal{S}_1| - \beta$ of the first user's private sub-channels (the rest of these sub-channels were dedicated to the transmission of the common message) that cannot be observed by the second user. This results in an $\alpha_1 + |\mathcal{S}_1| - \beta$ degrees of freedom for the first user's private message. The second user's private message needs to be transmitted in analogous way which will yield an $\alpha_2 + |\mathcal{S}_2| - \beta$ degrees of freedom.

We prove Theorem 2 in the next two sections. In Section IV, we show that the region given in Theorem 2 is an outer bound for the degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages. Then, we complete the proof of Theorem 2 in Section V by showing the achievability of this region.

IV. Outer Bound

We first obtain a new channel from the original one in (1)-(2)-(3) by using the GSVD, where the capacity region of the new channel includes the capacity region of the original one in (1)-(2)-(3). To this end, we note that

$$\mathbf{\Psi}_j^{\top} \mathbf{H}_j = \mathbf{\Sigma}_j \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times t-k} \end{bmatrix} \mathbf{\Psi}_t^{\top}, \quad j = 1, 2 \quad (23)$$

which is due to (12), and the fact that $\mathbf{\Psi}_t$ is orthonormal. Since $\mathbf{\Psi}_j$ is also orthonormal, and therefore non-singular, the capacity region of the following channel

$$\tilde{\mathbf{Y}}_j = \mathbf{\Psi}_j^{\top} \mathbf{Y}_j, \quad j = 1, 2 \quad (24)$$

is equal to the capacity region of the original one in (1)-(2)-(3). The channel defined in (24) can be written as

$$\tilde{\mathbf{Y}}_j = \mathbf{\Sigma}_j \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times t-k} \end{bmatrix} \mathbf{\Psi}_t^{\top} \mathbf{X} + \mathbf{\Psi}_j^{\top} \mathbf{N}_j, \quad j = 1, 2 \quad (25)$$

where we used (23). We define $\tilde{\mathbf{N}}_j = \mathbf{\Psi}_j^{\top} \mathbf{N}_j$ which is also a white Gaussian random vector, i.e.,

$$E\left[\tilde{\mathbf{N}}_j \tilde{\mathbf{N}}_j^{\top}\right] = \mathbf{I} \quad (26)$$

due to the fact that $\mathbf{\Psi}_j$ is orthonormal and $\mathbf{N}_j$ is white. We also define

$$\tilde{\mathbf{X}} = \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times t-k} \end{bmatrix} \mathbf{\Psi}_t^{\top} \mathbf{X} \quad (27)$$

using which the channel in (25) can be written as

$$\tilde{\mathbf{Y}}_j = \mathbf{\Sigma}_j \tilde{\mathbf{X}} + \tilde{\mathbf{N}}_j, \quad j = 1, 2 \quad (28)$$

where the channel input $\tilde{\mathbf{X}}$ should be chosen according to the trace constraint on $\mathbf{X}$ stated in (3). We now relax the power constraint on $\tilde{\mathbf{X}}$, and consequently, obtain the new channel whose capacity region includes the capacity region of the original channel in (1)-(2)-(3). To this end, we note that

$$\begin{aligned} &\text{tr}\left(E\left[\tilde{\mathbf{X}}\tilde{\mathbf{X}}^{\top}\right]\right) \\ &= \text{tr}\left(\begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times t-k} \end{bmatrix} \mathbf{\Psi}_t^{\top} E\left[\mathbf{X}\mathbf{X}^{\top}\right] \mathbf{\Psi}_t \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times t-k} \end{bmatrix}^{\top}\right) \quad (29) \\ &= \text{tr}\left(E\left[\mathbf{X}\mathbf{X}^{\top}\right] \mathbf{\Psi}_t \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times t-k} \end{bmatrix}^{\top} \begin{bmatrix} \mathbf{\Omega}^{-1} & \mathbf{0}_{k\times t-k} \end{bmatrix} \mathbf{\Psi}_t^{\top}\right) \quad (30) \end{aligned}$$

where (29) comes from the definition of $\tilde{\mathbf{X}}$ in (27), and (30) comes from the fact that $\text{tr}(\mathbf{AB}) = \text{tr}(\mathbf{BA})$. We next note that there exists a $\zeta > 0$ such that

$$\left[\mathbf{\Omega}^{-1} \quad \mathbf{0}_{k\times t-k}\right]^\top \left[\mathbf{\Omega}^{-1} \quad \mathbf{0}_{k\times t-k}\right] \preceq \zeta \mathbf{I} \tag{31}$$

Since $\text{tr}(\mathbf{A}_1\mathbf{A}_2) \geq 0$ if $\mathbf{A}_j \succeq \mathbf{0}$, using (31) in (30), we get

$$\text{tr}\left(E\left[\tilde{\mathbf{X}}\tilde{\mathbf{X}}^\top\right]\right) \leq \zeta \text{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\mathbf{\Psi}_t\mathbf{\Psi}_t^\top\right) \tag{32}$$

$$= \zeta \text{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\right) \tag{33}$$

$$\leq \zeta P \tag{34}$$

where (33) comes from the fact that $\mathbf{\Psi}_t$ is orthonormal, and (34) is due to the total power constraint on $\mathbf{X}$ given in (3). We now consider the following channel

$$\tilde{\mathbf{Y}}_j = \mathbf{\Sigma}_j\tilde{\mathbf{X}} + \tilde{\mathbf{N}}_j, \quad j = 1, 2 \tag{35}$$

where the channel input is subject to the following trace constraint

$$\text{tr}\left(E\left[\tilde{\mathbf{X}}\tilde{\mathbf{X}}^\top\right]\right) \leq \zeta P \tag{36}$$

We note that this new channel in (35)-(36) is obtained from the original channel in (1)-(2)-(3) by two main operations: The first one is the multiplication of the channel outputs in the original channel, i.e., (1)-(2), with invertible matrices $\mathbf{\Psi}_1, \mathbf{\Psi}_2$ which preserves the capacity region. The second operation is the relaxation of the power constraint in the new channel to get (36) which increases the capacity region by means of increasing the set of all feasible input distributions. Thus, due to this second operation, the capacity region of the new channel in (35)-(36) serves as an outer bound for the capacity region of the original channel in (1)-(2)-(3). Similarly, the degrees of freedom region of the new channel in (35)-(36) is an outer bound for the degrees of freedom region of the original channel in (1)-(2)-(3).

We next rewrite the channel in (35)-(36) in an alternative form. To this end, we note that the last $(r_1 + p - k)$ entries of $\tilde{\mathbf{Y}}_1$ come from only the noise. Since the noise is white, see (26), we can omit these last $r_1 + p - k$ entries of $\tilde{\mathbf{Y}}_1$ without loss of optimality. Furthermore, we define

$$\tilde{h}_{1\ell} = \Sigma_{1,\ell\ell}, \quad 1 \leq \ell \leq k - p \tag{37}$$

Similarly, the first $r_2 - p - s$ entries of $\tilde{\mathbf{Y}}_2$ come from only the noise. Since the noise is white, see (26), we can again omit these first $r_2 - p - s$ entries of $\tilde{\mathbf{Y}}_2$ without loss of optimality. Similarly, we also define

$$\tilde{h}_{2\ell} = \Sigma_{2,(r_2-k+\ell)\ell}, \quad k - p - s + 1 \leq \ell \leq k \tag{38}$$

Using the definitions in (37)-(38) and omitting the entries of $\tilde{\mathbf{Y}}_1, \tilde{\mathbf{Y}}_2$ which contain only noise, the channel in (35) can be expressed as

$$\tilde{Y}_{1\ell} = \tilde{h}_{1\ell}\tilde{X}_\ell + \tilde{N}_{1,\ell}, \quad \ell = 1, \ldots, |\mathcal{S}_1| + |\mathcal{S}_c| \tag{39}$$

$$\tilde{Y}_{2\ell} = \tilde{h}_{2\ell}\tilde{X}_\ell + \tilde{N}_{2,\ell}, \quad \ell = |\mathcal{S}_1| + 1, \ldots, |\mathcal{S}_1| + |\mathcal{S}_c| + |\mathcal{S}_2| \tag{40}$$

where we used the definitions of $\mathcal{S}_1, \mathcal{S}_c, \mathcal{S}_2$ given in (17)-(19) in conjunction with (37)-(38). Note that $\{\tilde{N}_{1,\ell}\}_{\ell=1}^{\ell=|\mathcal{S}_1|+|\mathcal{S}_c|}, \{\tilde{N}_{2,\ell}\}_{\ell=|\mathcal{S}_1|+1}^{|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|}$ are i.i.d. Gaussian random variables with unit variance. The power constraint on the channel input in (36) can be rewritten as

$$\sum_{\ell=1}^{|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|} E\left[\tilde{X}_\ell^2\right] \leq \zeta P \tag{41}$$

We note that the channel defined by (39)-(40) is a parallel Gaussian broadcast channel with unmatched sub-channels, whose capacity region is obtained in [5]. In particular, the capacity region of the channel in (39)-(40) is given by the union of the rate triples (R_0, R_1, R_2) satisfying

$$R_0 \leq \sum_{\ell\in\mathcal{S}_1\cup\mathcal{S}_c} C\left(\frac{\tilde{h}_{1\ell}^2\gamma_\ell P_\ell}{1+\tilde{h}_{1\ell}^2\bar{\gamma}_\ell P_\ell}\right) \tag{42}$$

$$R_0 \leq \sum_{\ell\in\mathcal{S}_2\cup\mathcal{S}_c} C\left(\frac{\tilde{h}_{2\ell}^2\gamma_\ell P_\ell}{1+\tilde{h}_{2\ell}^2\bar{\gamma}_\ell P_\ell}\right) \tag{43}$$

$$\sum_{j=0}^{1} R_j \leq \sum_{\ell\in\mathcal{S}_{c2}} C\left(\frac{\tilde{h}_{1\ell}^2\gamma_\ell P_\ell}{1+\tilde{h}_{1\ell}^2\bar{\gamma}_\ell P_\ell}\right) + \sum_{\ell\in\mathcal{S}_1\cup\mathcal{S}_{c1}} C\left(\tilde{h}_{1\ell}^2 P_\ell\right) \tag{44}$$

$$\sum_{j=0}^{1} R_{2j} \leq \sum_{\ell\in\mathcal{S}_{c1}} C\left(\frac{\tilde{h}_{2\ell}^2\gamma_\ell P_\ell}{1+\tilde{h}_{2\ell}^2\bar{\gamma}_\ell P_\ell}\right) + \sum_{\ell\in\mathcal{S}_2\cup\mathcal{S}_{c2}} C\left(\tilde{h}_{2\ell}^2 P_\ell\right) \tag{45}$$

$$\sum_{j=0}^{2} R_j \leq \sum_{\ell\in\mathcal{S}_{c2}} C\left(\frac{\tilde{h}_{1\ell}^2\gamma_\ell P_\ell}{1+\tilde{h}_{1\ell}^2\bar{\gamma}_\ell P_\ell}\right) + \sum_{\ell\in\mathcal{S}_2\cup\mathcal{S}_{c2}} C\left(\tilde{h}_{2\ell}^2 \bar{\gamma}_\ell P_\ell\right) + \sum_{\ell\in\mathcal{S}_1\cup\mathcal{S}_{c1}} C\left(\tilde{h}_{1\ell}^2 P_\ell\right) \tag{46}$$

$$\sum_{j=0}^{2} R_j \leq \sum_{\ell\in\mathcal{S}_{c1}} C\left(\frac{\tilde{h}_{2\ell}^2\gamma_\ell P_\ell}{1+\tilde{h}_{2\ell}^2\bar{\gamma}_\ell P_\ell}\right) + \sum_{\ell\in\mathcal{S}_1\cup\mathcal{S}_{c1}} C\left(\tilde{h}_{1\ell}^2 \bar{\gamma}_\ell P_\ell\right) + \sum_{\ell\in\mathcal{S}_2\cup\mathcal{S}_{c2}} C\left(\tilde{h}_{2\ell}^2 P_\ell\right) \tag{47}$$

for some $\gamma_\ell = 1 - \bar{\gamma}_\ell \in [0, 1]$, $\ell = 1, \ldots, |\mathcal{S}_1| + |\mathcal{S}_c| + |\mathcal{S}_2|$, and $\{P_\ell\}_{\ell=1}^{|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|}$ such that $\sum_{\ell=1}^{|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|} P_\ell = \zeta P$, where $C(x) = (1/2)\log(1+x)$, $\mathcal{S}_{c1}$ and $\mathcal{S}_{c2}$ are given by

$$\mathcal{S}_{c1} = \left\{\ell \in \mathcal{S}_c : \tilde{h}_{1\ell}^2 \geq \tilde{h}_{2\ell}^2\right\} \tag{48}$$

$$\mathcal{S}_{c2} = \left\{\ell \in \mathcal{S}_c : \tilde{h}_{2\ell}^2 \geq \tilde{h}_{1\ell}^2\right\} \tag{49}$$

We can obtain an outer bound $\mathcal{D}^{\text{out}}$ for the degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages by using (42)-(47). $\mathcal{D}^{\text{out}}$ contains all the degrees of freedom triples (d_0, d_1, d_2) satisfying

$$d_0 \leq \eta + \delta \tag{50}$$

$$d_0 + d_1 \leq |\mathcal{S}_c| + |\mathcal{S}_1| \tag{51}$$

$$d_0 + d_2 \leq |\mathcal{S}_c| + |\mathcal{S}_2| \tag{52}$$

$$d_0 + d_1 + d_2 \leq |\mathcal{S}_1| + |\mathcal{S}_2| + |\mathcal{S}_c| - \eta \tag{53}$$

for some η, δ such that $0 \leq \eta \leq \min_{j=1,2}|\mathcal{S}_j|$, $0 \leq \delta \leq |\mathcal{S}_c|$. The equivalence between $\mathcal{D}^{\text{out}}$ and the region in Theorem 2 can be shown by using the Fourier-Motzkin elimination.

V. Inner Bound

We now show that the degrees of freedom region given in Theorem 2 is achievable. To this end, we define the covariance matrices $\mathbf{K}_u,\ u=0,1,2,$ as follows

$$\mathbf{K}_u = (\xi P)\mathbf{\Psi}_t \begin{bmatrix} \mathbf{\Omega} \\ \mathbf{0}_{t-k\times k} \end{bmatrix} \mathbf{\Lambda}_u \begin{bmatrix} \mathbf{\Omega}^\top & \mathbf{0}_{k\times t-k} \end{bmatrix} \mathbf{\Psi}_t^\top \tag{54}$$

where $\mathbf{\Lambda}_u$ is a diagonal matrix of size $k\times k$. ξ in (54) is selected to ensure that $\text{tr}(\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2)\leq P$. We next specify the diagonal matrices $\mathbf{\Lambda}_0,\mathbf{\Lambda}_1,\mathbf{\Lambda}_2$ as follows

$$\Lambda_{0,\ell\ell} = \begin{cases} 1, & 1\leq \ell\leq\beta \\ 0, & \beta+1\leq\ell\leq|\mathcal{S}_1|+\alpha_1 \\ 1, & |\mathcal{S}_1|+\alpha_1+1\leq\ell\leq|\mathcal{S}_1|+|\mathcal{S}_c|-\alpha_2 \\ 0, & |\mathcal{S}_1|+|\mathcal{S}_c|-\alpha_2+1\leq\ell\leq|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|-\beta \\ 1, & |\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|-\beta+1\leq\ell\leq|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2| \end{cases} \tag{55}$$

$$\Lambda_{1,\ell\ell} = \begin{cases} 0, & 1\leq\ell\leq\beta \\ 1, & \beta+1\leq\ell\leq|\mathcal{S}_1|+\alpha_1 \\ 0, & |\mathcal{S}_1|+\alpha_1+1\leq\ell\leq|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2| \end{cases} \tag{56}$$

$$\Lambda_{2,\ell\ell} = \begin{cases} 0, & 1\leq\ell\leq|\mathcal{S}_1|+|\mathcal{S}_c|-\alpha_2 \\ 1, & |\mathcal{S}_1|+|\mathcal{S}_c|-\alpha_2+1\leq\ell\leq|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|-\beta \\ 0, & |\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|-\beta+1\leq\ell\leq|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2| \end{cases} \tag{57}$$

where $0\leq\beta\leq\min\{|\mathcal{S}_1|,|\mathcal{S}_2|\}$, $0\leq\alpha_j$, $\alpha_1+\alpha_2\leq|\mathcal{S}_c|$.

We now use the covariance matrices in (54) to compute an achievable degrees of freedom region by using the achievable rate region given in Theorem 1. We first note that

$$R_{01}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2) = \frac{1}{2}\sum_{\ell=1}^{\beta}\log\left((\xi P)(\mathbf{\Sigma}_1^\top\mathbf{\Sigma}_1)_{\ell\ell}+1\right) + \frac{1}{2}\sum_{\ell=|\mathcal{S}_1|+\alpha_1+1}^{|\mathcal{S}_1|+|\mathcal{S}_c|-\alpha_2}\log\left((\xi P)(\mathbf{\Sigma}_1^\top\mathbf{\Sigma}_1)_{\ell\ell}+1\right) \tag{58}$$

which implies that

$$\lim_{P\to\infty}\frac{R_{01}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)}{\frac{1}{2}\log P} = \beta+|\mathcal{S}_c|-\alpha_1-\alpha_2 \tag{59}$$

Similarly, we have

$$R_{02}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2) = \frac{1}{2}\sum_{\ell=|\mathcal{S}_1|+\alpha_1+1}^{|\mathcal{S}_1|+|\mathcal{S}_c|-\alpha_2}\log\left((\xi P)(\mathbf{\Sigma}_2^\top\mathbf{\Sigma}_2)_{\ell\ell}+1\right) + \frac{1}{2}\sum_{\ell=|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|-\beta+1}^{|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|}\log\left((\xi P)(\mathbf{\Sigma}_2^\top\mathbf{\Sigma}_2)_{\ell\ell}+1\right) \tag{60}$$

which implies that

$$\lim_{P\to\infty}\frac{R_{02}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)}{\frac{1}{2}\log P} = \beta+|\mathcal{S}_c|-\alpha_1-\alpha_2 \tag{61}$$

Hence, combining (59) and (61) yields that

$$d_0 = \beta+|\mathcal{S}_c|-\alpha_1-\alpha_2 \tag{62}$$

is an achievable degrees of freedom for the common message.

We now consider the first user's rate as follows

$$R_1(\mathbf{K}_1,\mathbf{K}_2) = \frac{1}{2}\sum_{\ell=\beta+1}^{|\mathcal{S}_1|+\alpha_1}\log\left((\xi P)(\mathbf{\Sigma}_1^\top\mathbf{\Sigma}_1)_{\ell\ell}+1\right) \tag{63}$$

which implies that

$$d_1 = \alpha_1+|\mathcal{S}_1|-\beta \tag{64}$$

is an achievable degrees of freedom for the first user's private message. We finally consider the second user's rate as follows

$$R_2(\mathbf{K}_2) = \frac{1}{2}\sum_{\ell=|\mathcal{S}_1|+|\mathcal{S}_c|-\alpha_2+1}^{|\mathcal{S}_1|+|\mathcal{S}_c|+|\mathcal{S}_2|-\beta}\log\left((\xi P)(\mathbf{\Sigma}_2^\top\mathbf{\Sigma}_2)_{\ell\ell}+1\right) \tag{65}$$

which implies that

$$d_2 = \alpha_2+|\mathcal{S}_2|-\beta \tag{66}$$

is an achievable degrees of freedom for the second user's private message. Thus, in view of (62), (64), (66), we have shown the achievability of the degrees of freedom region given in Theorem 2.

VI. Conclusions

We obtain the degrees of freedom region of the Gaussian MIMO broadcast channel with common and private messages. The key step for this result is to construct a parallel Gaussian broadcast channel from the Gaussian MIMO broadcast channel by using the GSVD and a power relaxation, where the capacity region of the parallel channel provides an outer bound for the capacity region of the original channel. Using the capacity result for the parallel channel, we obtain an outer bound for the degrees of freedom region of the Gaussian MIMO broadcast channel. Finally, we show that this outer bound can be attained by the DPC region, i.e., the DPC region is asymptotically optimal.

References

[1] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inf. Theory*, 52(9):3936–3964, Sep. 2006.

[2] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). On the capacity region of the multi-antenna broadcast channel with common messages. In *IEEE ISIT*, Jul. 2006.

[3] H. Weingarten. *Multiple-input multiple-output broadcast systems*. PhD thesis, Technion, Haifa, Israel, 2007.

[4] N. Jindal and A. Goldsmith. Optimal power allocation for parallel broadcast channels with independent and common information. In *IEEE Intl. Symp. Inf. Theory*, page 215, Jun. 2004.

[5] A. El Gamal. Capacity of the product and sum of two unmatched broadcast channels. *Problems of Information Transmission*, 16(1):3–23, Jan. 1980.

[6] E. Ekrem and S. Ulukus. On Gaussian MIMO broadcast channels with common and private messages. *IEEE ISIT*, Jul. 2010.

[7] C. Paige and M. A. Saunders. Towards a generalized singular value decomposition. *SIAM. J. Numer. Anal.*, 18(398-405), Jun. 1981.