Gaussian MIMO Broadcast Channels with Common and Confidential 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 study the two-user Gaussian multiple-input multiple-output (MIMO) broadcast channel with common and confidential messages. In this channel, the transmitter sends a common message to both users, and a confidential message to each user which is kept perfectly secret from the other user. We obtain the entire capacity region of this channel. We also explore the connections between the capacity region we obtained for the Gaussian MIMO broadcast channel with common and confidential messages and the capacity region of its non-confidential counterpart, i.e., the Gaussian MIMO broadcast channel with common and private messages, which is not known completely.**

I. Introduction

We study the two-user Gaussian multiple-input multiple-output (MIMO) broadcast channel for the following scenario: The transmitter sends a common message to both users, and a confidential message to each user which needs to be kept perfectly secret from the other user. We call the channel model arising from this scenario the Gaussian MIMO broadcast channel with common and confidential messages.

The Gaussian MIMO broadcast channel with common and confidential messages subsumes many other channel models as special cases. The first one is the Gaussian MIMO wiretap channel, where the transmitter has only one confidential message for one (legitimate) user, which is kept perfectly secret from the other user (eavesdropper). The secrecy capacity of the Gaussian MIMO wiretap channel is obtained in [1], [2] for the general case, in [3] for the 2-2-1 case. The second channel model that the Gaussian MIMO broadcast channel with common and confidential messages subsumes is the Gaussian MIMO wiretap channel with common message [4], in which the transmitter sends a common message to both legitimate user and the eavesdropper, and a confidential message to the legitimate user that is kept perfectly secret from the eavesdropper. The capacity region of the Gaussian MIMO wiretap channel with common message is obtained in [4]. The last channel model that the Gaussian MIMO broadcast channel with common and confidential messages encompasses is the the Gaussian MIMO broadcast channel with confidential messages [5], where the transmitter sends a confidential message to each user which is kept perfectly secret from the other user. The capacity region of the Gaussian MIMO broadcast channel with confidential messages is established in [5].

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

Here, we obtain the capacity region of the Gaussian MIMO broadcast channel with common and confidential messages. In particular, we show that a variant of the secret dirty-paper coding (S-DPC) scheme proposed in [5] is capacity-achieving. Since the S-DPC scheme proposed in [5] is for the transmission of only two confidential messages, it is modified here to incorporate the transmission of a common message as well. Similar to [5], we also notice an invariance property of this achievable scheme with respect to the encoding order used in the S-DPC scheme. In other words, two achievable rate regions arising from two possible encoding orders used in the S-DPC scheme are identical, and equal to the capacity region. We provide the proof of this statement as well as the converse proof for the capacity region of the Gaussian MIMO broadcast channel with common and confidential messages by using the channel enhancement technique [6] and an extremal inequality from [7].

We also explore the connections between the Gaussian MIMO broadcast channel with common and confidential messages and its non-confidential counterpart, i.e., the (two-user) Gaussian MIMO broadcast channel with common and private messages. In the Gaussian MIMO broadcast channel with common and private messages, the transmitter again sends a common message to both users, and a private message to each user, for which there is no secrecy constraint now, i.e., private message of each user does not need to be kept secret from the other user. Thus, the Gaussian MIMO broadcast channel with common and confidential messages we study here can be viewed as a constrained version of the Gaussian MIMO broadcast channel with common and private messages, where the constraints come through forcing the private messages to be confidential. We note that although there are partial results for the capacity region of the Gaussian MIMO broadcast channel with common and private messages [8], [9], it is not known completely. However, here, we are able to obtain the entire capacity region for a constrained version of the Gaussian MIMO broadcast channel with common and private messages, i.e., for the Gaussian MIMO broadcast channel with common and confidential messages. We provide an intuitive explanation of this at-first-sight surprising point as well as the invariance property of the achievable rate regions with respect to the encoding orders that can be used in the S-DPC scheme by using a result from [9] for the Gaussian MIMO broadcast channel with common and private messages.

II. Channel Model and Main Result

We study the two-user Gaussian MIMO broadcast channel which 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 $t \times 1$ vector, $\mathbf{H}_j$ is the channel gain matrix of size $r_j \times t$, the channel output of the jth user $\mathbf{Y}_j$ is an $r_j \times 1$ vector, and the Gaussian random vector $\mathbf{N}_j$ is of size $r_j \times 1$ with a covariance matrix $\mathbf{\Sigma}_j$ which is assumed to be strictly positive-definite, i.e., $\mathbf{\Sigma}_j \succ \mathbf{0}$. We consider a covariance constraint on the channel input as follows

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{3}$$

where $\mathbf{S} \succeq \mathbf{0}$.

We study the following scenario for the Gaussian MIMO broadcast channel: There are three independent messages (W_0, W_1, W_2) with rates (R_0, R_1, R_2), respectively, where W_0 is the common message that needs to be delivered to both users, W_1 is the confidential message of the first user which needs to be kept perfectly secret from the second user, and similarly, W_2 is the confidential message of the second user which needs to be kept perfectly secret from the first user. The secrecy of the confidential messages is measured by the normalized equivocation rates [10], i.e, we require

$$\frac{1}{n}I(W_1; W_0, W_2, \mathbf{Y}_2^n) \rightarrow 0 \quad \text{and} \quad \frac{1}{n}I(W_2; W_0, W_1, \mathbf{Y}_1^n) \rightarrow 0 \tag{4}$$

as $n \rightarrow \infty$, where n denotes the number of channel uses. The closure of all achievable rate triples (R_0, R_1, R_2) is defined to be the capacity region, and will be denoted by $\mathcal{C}(\mathbf{S})$. We next define the following shorthand notations

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

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

$$R_2(\mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{7}$$

using which, our main result can be stated as follows.

Theorem 1 *The capacity region of the Gaussian MIMO broadcast channel with common and confidential messages $\mathcal{C}(\mathbf{S})$ is given by*

$$\mathcal{C}(\mathbf{S}) = \mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S}) = \mathcal{R}_{21}^{\text{S-DPC}}(\mathbf{S}) \tag{8}$$

where $\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S})$ is given by the union of the rate triples (R_0, R_1, R_2) satisfying

$$R_0 \leq \min\{R_{01}(\mathbf{K}_1, \mathbf{K}_2), R_{02}(\mathbf{K}_1, \mathbf{K}_2)\} \tag{9}$$
$$R_1 \leq R_1(\mathbf{K}_1, \mathbf{K}_2) \tag{10}$$
$$R_2 \leq R_2(\mathbf{K}_2) \tag{11}$$

for some positive semi-definite matrices $\mathbf{K}_1, \mathbf{K}_2$ such that $\mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$, and $\mathcal{R}_{21}^{\text{S-DPC}}(\mathbf{S})$ can be obtained from $\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S})$ by swapping the subscripts 1 and 2.

Theorem 1 states that the common message, for which a covariance matrix $\mathbf{S} - \mathbf{K}_1 - \mathbf{K}_2$ is allotted, should be encoded by using a standard Gaussian codebook, and the confidential messages, for which covariance matrices $\mathbf{K}_1, \mathbf{K}_2$ are allotted, need to be encoded by using the S-DPC scheme proposed in [5]. The receivers first decode the common message by treating the confidential messages as noise, and then each receiver decodes the confidential message intended to itself. Depending on the encoding order used in S-DPC, one of the users gets a clean link for the transmission of its confidential message, where there is no interference due to the other user's confidential message. Although one might expect that the two achievable regions arising from two possible encoding orders that can be used in S-DPC could be different, i.e., $\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S}) \neq \mathcal{R}_{21}^{\text{S-DPC}}(\mathbf{S})$, and taking a convex closure of these two regions would yield a larger achievable rate region, Theorem 1 states that $\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S}) = \mathcal{R}_{21}^{\text{S-DPC}}(\mathbf{S})$, i.e., the achievable rate region is invariant with respect to the encoding order used in S-DPC. We acknowledge an independent and concurrent work [11], which also obtained Theorem 1.

We conclude this section by defining a sub-class of Gaussian MIMO broadcast channels called the aligned Gaussian MIMO broadcast channel, which can be obtained from (1)-(2) by setting $\mathbf{H}_1 = \mathbf{H}_2 = \mathbf{I}$,

$$\mathbf{Y}_1 = \mathbf{X} + \mathbf{N}_1 \tag{12}$$
$$\mathbf{Y}_2 = \mathbf{X} + \mathbf{N}_2 \tag{13}$$

Here, we prove Theorem 1 for the aligned channel. The proof for the general case in (1)-(2) can be carried out by using the capacity result for the aligned case and the analysis in [12].

III. Proof of Theorem 1 for the Aligned Case

Due to space limitations here, we omit the achievability proof for Theorem 1. We provide the converse proof. Since the capacity region $\mathcal{C}(\mathbf{S})$ is convex due to time-sharing, it can be characterized by the solution of

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}(\mathbf{S})} R_0 + \mu_1 R_1 + \mu_2 R_2 \tag{14}$$

for $\mu_j \in [0, \infty), \ j = 1, 2$. To this end, we first characterize the boundary of $\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S})$ by studying the following optimization problem

$$\max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S})} R_0 + \mu_1 R_1 + \mu_2 R_2 \tag{15}$$

which can be written as

$$\max_{\substack{\mathbf{0}\preceq\mathbf{K}_j, \ j=1,2 \\ \mathbf{K}_1+\mathbf{K}_2\preceq\mathbf{S}}} \min\{R_{01}(\mathbf{K}_1, \mathbf{K}_2), R_{02}(\mathbf{K}_1, \mathbf{K}_2)\} + \mu_1 R_1(\mathbf{K}_1, \mathbf{K}_2) + \mu_2 R_2(\mathbf{K}_2) \tag{16}$$

Let $\mathbf{K}_1^*, \mathbf{K}_2^*$ be the maximizer of (16), which needs to satisfy the following KKT conditions.

Lemma 1 *$\mathbf{K}_1^*, \mathbf{K}_2^*$ need to satisfy*

$$\begin{aligned}(\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1 \\ =(\lambda+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1} \\ +(\bar{\lambda}+\mu_1)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_S \end{aligned} \quad (17)$$

$$\begin{aligned}(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_2 \\ =(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1\end{aligned} \quad (18)$$

for some positive semi-definite matrices $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_S$ such that $\mathbf{K}_1^*\mathbf{M}_1=\mathbf{K}_2^*\mathbf{M}_2=(\mathbf{S}-\mathbf{K}_1^*-\mathbf{K}_2^*)\mathbf{M}_S=\mathbf{0}$ and for some $\lambda=1-\bar{\lambda}$ such that it satisfies $0\le\lambda\le 1$ and

$$\lambda\begin{cases} = & 0 \quad \text{if} \quad R_{01}(\mathbf{K}_1^*,\mathbf{K}_2^*) > R_{02}(\mathbf{K}_1^*,\mathbf{K}_2^*) \\ = & 1 \quad \text{if} \quad R_{01}(\mathbf{K}_1^*,\mathbf{K}_2^*) < R_{02}(\mathbf{K}_1^*,\mathbf{K}_2^*) \\ \neq & 0,1 \quad \text{if} \quad R_{01}(\mathbf{K}_1^*,\mathbf{K}_2^*) = R_{02}(\mathbf{K}_1^*,\mathbf{K}_2^*) \end{cases} \quad (19)$$

Due to space limitations here, the proof of this lemma as well as the proofs of the upcoming lemmas are omitted. They can be found in [13]. We now use channel enhancement [6] to define a new noise covariance matrix $\tilde{\mathbf{\Sigma}}$ as follows

$$(\mu_1+\mu_2)(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}=(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_2 \quad (20)$$

These new noise covariance matrix $\tilde{\mathbf{\Sigma}}$ has some useful properties which are listed in the following lemma.

Lemma 2 *We have the following facts.*

- $\tilde{\mathbf{\Sigma}}\preceq\mathbf{\Sigma}_1,\ \tilde{\mathbf{\Sigma}}\preceq\mathbf{\Sigma}_2$.
- $(\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}= (\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1$
- $(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}\tilde{\mathbf{\Sigma}}=(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}\mathbf{\Sigma}_2$
- $(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})= (\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^*+\mathbf{\Sigma}_1)$

We now construct an enhanced channel using the new covariance matrix $\tilde{\mathbf{\Sigma}}$ as follows

$$\tilde{\mathbf{Y}}_1=\tilde{\mathbf{Y}}_2=\tilde{\mathbf{Y}}=\mathbf{X}+\tilde{\mathbf{N}} \quad (21)$$

$$\mathbf{Y}_1=\mathbf{X}+\mathbf{N}_1 \quad (22)$$

$$\mathbf{Y}_2=\mathbf{X}+\mathbf{N}_2 \quad (23)$$

where $\tilde{\mathbf{N}}$ is a Gaussian random vector with the covariance matrix $\tilde{\mathbf{\Sigma}}$. In the channel given by (21)-(23), the enhanced first and second users have the same observation $\tilde{\mathbf{Y}}$. For the enhanced channel in (21)-(23), we consider the scenario that a common message W_0 with rate R_0 is directed to the first and second users, i.e., the users with observations $\mathbf{Y}_1$ and $\mathbf{Y}_2$, respectively, W_1 (resp. W_2) with rate R_1 (resp. R_2) is the confidential message of the enhanced first (resp. second) user which is kept perfectly hidden from the second (resp. first) user. We denote the capacity region by $\tilde{C}(\mathbf{S})$. Since in the enhanced channel, the receivers to which only the common message is sent are identical to the receivers in the original channel in (12)-(13), and the receivers to which confidential messages are sent have better observations with respect to the receivers in the original channel in (12)-(13), we have $\mathcal{C}(\mathbf{S})\subseteq\tilde{C}(\mathbf{S})$. We next introduce an outer bound for $\tilde{C}(\mathbf{S})$.

Lemma 3 *The capacity region of the enhanced channel in (21)-(23) $\tilde{C}(\mathbf{S})$ is contained in the union of the rate triples (R_0,R_1,R_2) satisfying*

$$R_0\le\min\{I(U;\mathbf{Y}_1),I(U;\mathbf{Y}_2)\} \quad (24)$$

$$R_1\le I(\mathbf{X};\tilde{\mathbf{Y}}|U)-I(\mathbf{X};\mathbf{Y}_2|U) \quad (25)$$

$$R_2\le I(\mathbf{X};\tilde{\mathbf{Y}}|U)-I(\mathbf{X};\mathbf{Y}_1|U) \quad (26)$$

for some $(U,\mathbf{X})$ such that $U\rightarrow\mathbf{X}\rightarrow\tilde{\mathbf{Y}}\rightarrow(\mathbf{Y}_1,\mathbf{Y}_2)$ and $E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}$.

We also introduce the following extremal inequality from [7]:

Lemma 4 ([7, Corollary 4]) *$(U,\mathbf{X})$ is an arbitrary random vector, where $E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}$ and $\mathbf{S}\succ\mathbf{0}$. Let $\tilde{\mathbf{N}},\mathbf{N}_1,\mathbf{N}_2$ be Gaussian with covariance matrices $\tilde{\mathbf{\Sigma}},\mathbf{\Sigma}_1,\mathbf{\Sigma}_2$, respectively. They are independent of $(U,\mathbf{X})$. Moreover, $\tilde{\mathbf{\Sigma}},\mathbf{\Sigma}_1,\mathbf{\Sigma}_2$ satisfy $\tilde{\mathbf{\Sigma}}\preceq\mathbf{\Sigma}_j,\ j=1,2$. Assume that there exists a covariance matrix $\mathbf{K}^*$ such that $\mathbf{K}^*\preceq\mathbf{S}$ and*

$$\beta(\mathbf{K}^*+\tilde{\mathbf{\Sigma}})^{-1}=\sum_{j=1}^{2}\gamma_j(\mathbf{K}^*+\mathbf{\Sigma}_j)^{-1}+\mathbf{M}_S \quad (27)$$

where $\beta\ge 0,\gamma_j\ge 0,\ j=1,2$ and $\mathbf{M}_S$ is positive semi-definite matrix such that $(\mathbf{S}-\mathbf{K}^*)\mathbf{M}_S=\mathbf{0}$. Then, for any $(U,\mathbf{X})$, we have

$$\begin{aligned}\beta h(\mathbf{X}+\tilde{\mathbf{N}}|U)-\sum_{j=1}^{2}\gamma_j h(\mathbf{X}+\mathbf{N}_j|U)\le \\ \frac{\beta}{2}\log|(2\pi e)(\mathbf{K}^*+\tilde{\mathbf{\Sigma}})|-\sum_{j=1}^{2}\frac{\gamma_j}{2}\log|(2\pi e)(\mathbf{K}^*+\mathbf{\Sigma}_j)|\end{aligned} \quad (28)$$

We now use this lemma. For that purpose, we note that using the second statement of Lemma 2 in (17) yields

$$\begin{aligned}(\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}=(\lambda+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1} \\ +(\bar{\lambda}+\mu_1)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_S\end{aligned} \quad (29)$$

using which in conjunction with Lemma 4, we get

$$\begin{aligned}&(\mu_1+\mu_2)h(\tilde{\mathbf{Y}}|U)-(\lambda+\mu_2)h(\mathbf{Y}_1|U)-(\bar{\lambda}+\mu_1)h(\mathbf{Y}_2|U) \\ &\le\frac{\mu_1+\mu_2}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})| \\ &\quad -\frac{\lambda+\mu_2}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)| \\ &\quad -\frac{\bar{\lambda}+\mu_1}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)|\end{aligned} \quad (30)$$

which will be used subsequently. We are now ready to complete the converse proof as follows

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}(\mathbf{S})} R_0+\mu_1R_1+\mu_2R_2 \quad (31)$$

$$\le\max_{(R_0,R_1,R_2)\in\tilde{\mathcal{C}}(\mathbf{S})} R_0+\mu_1R_1+\mu_2R_2 \quad (32)$$

$$\begin{aligned}\le\max\ \min\{I(U;\mathbf{Y}_1),I(U;\mathbf{Y}_2)\}+(\mu_1+\mu_2)I(\mathbf{X};\tilde{\mathbf{Y}}|U) \\ -\mu_1I(\mathbf{X};\mathbf{Y}_2|U)-\mu_2I(\mathbf{X};\mathbf{Y}_1|U)\end{aligned} \quad (33)$$

$$\leq \max \; \lambda I(U;\mathbf{Y}_1)+\bar{\lambda} I(U;\mathbf{Y}_2)+(\mu_1+\mu_2)I(\mathbf{X};\tilde{\mathbf{Y}}|U) - \mu_1 I(\mathbf{X};\mathbf{Y}_2|U)-\mu_2 I(\mathbf{X};\mathbf{Y}_1|U) \quad (34)$$

$$= \max \; \lambda h(\mathbf{Y}_1)+\bar{\lambda} h(\mathbf{Y}_2)+(\mu_1+\mu_2)h(\tilde{\mathbf{Y}}|U) - (\lambda+\mu_2)h(\mathbf{Y}_1|U)-(\bar{\lambda}+\mu_1)h(\mathbf{Y}_2|U) - \frac{\mu_1}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_2|}-\frac{\mu_2}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_1|} \quad (35)$$

$$\leq \frac{\lambda}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_1)|+\frac{\bar{\lambda}}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_1)| + \max\Big[(\mu_1+\mu_2)h(\tilde{\mathbf{Y}}|U)-(\lambda+\mu_2)h(\mathbf{Y}_1|U) - (\bar{\lambda}+\mu_1)h(\mathbf{Y}_2|U)\Big]-\frac{\mu_1}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_2|}-\frac{\mu_2}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_1|} \quad (36)$$

$$\leq \frac{\lambda}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_1)|+\frac{\bar{\lambda}}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_1)| + \frac{(\mu_1+\mu_2)}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})| - \frac{(\lambda+\mu_2)}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)| - \frac{\bar{\lambda}+\mu_1}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)| - \frac{\mu_1}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_2|}-\frac{\mu_2}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_1|} \quad (37)$$

$$= \min\{R_{01}(\mathbf{K}_1^*,\mathbf{K}_2^*),R_{02}(\mathbf{K}_1^*,\mathbf{K}_2^*)\} + \frac{\mu_1}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_2|}{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)\tilde{\mathbf{\Sigma}}|} + \frac{\mu_2}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_1|}{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)\tilde{\mathbf{\Sigma}}|} \quad (38)$$

$$= \min\{R_{01}(\mathbf{K}_1^*,\mathbf{K}_2^*),R_{02}(\mathbf{K}_1^*,\mathbf{K}_2^*)\}+\mu_1 R_1(\mathbf{K}_1^*,\mathbf{K}_2^*) + \mu_2 R_2(\mathbf{K}_2^*) \quad (39)$$

where (32) comes from the fact that $\mathcal{C}(\mathbf{S})\subseteq\tilde{\mathcal{C}}(\mathbf{S})$, (33) is due to Lemma 3, (34) results from the fact that $0\leq\lambda=1-\bar{\lambda}\leq 1$, (36) is due to the maximum entropy theorem, (37) comes from (30), and (39) will be shown next. We first note the following

$$R_1(\mathbf{K}_1^*,\mathbf{K}_2^*)=\frac{1}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}|}{|(\mathbf{K}_2^*+\mathbf{\Sigma}_1)(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}|} \quad (40)$$

$$=\frac{1}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}|}{|(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}|} \quad (41)$$

$$=\frac{1}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_2|}{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)\tilde{\mathbf{\Sigma}}|} \quad (42)$$

where (41) is due to the fourth statement of Lemma 2 and (42) comes from the third statement of Lemma 2. We next note the following identity

$$R_2(\mathbf{K}_2^*)=\frac{1}{2}\log\frac{|(\mathbf{K}_2^*+\mathbf{\Sigma}_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}|}{|\mathbf{\Sigma}_2\mathbf{\Sigma}_1^{-1}|} \quad (43)$$

$$=\frac{1}{2}\log\frac{|(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})(\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}|}{|\tilde{\mathbf{\Sigma}}\mathbf{\Sigma}_1^{-1}|} \quad (44)$$

$$=\frac{1}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_1|}{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)\tilde{\mathbf{\Sigma}}|} \quad (45)$$

where (44) is due to the third statement of Lemma 2, and (2) comes from the fourth statement of Lemma 2. Identities in (42) and (45) give (39). Thus, in the view of (39), we have shown that $\mathcal{C}(\mathbf{S})=\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S})$. Similarly, one can also show $\mathcal{C}(\mathbf{S})=\mathcal{R}_{21}^{\text{S-DPC}}(\mathbf{S})$; completing the proof of Theorem 1.

IV. Connections to the Gaussian MIMO Broadcast Channel with Common and Private Messages

Here, we provide an intuitive explanation for the two facts that Theorem 1 reveals: i) The achievable rate region does not depend on the encoding order used in S-DPC, i.e., $\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S})=\mathcal{R}_{21}^{\text{S-DPC}}(\mathbf{S})$, ii) The capacity region of the Gaussian MIMO broadcast channel with common and confidential messages can be completely characterized, although the capacity region of the its non-confidential counterpart, i.e., the Gaussian MIMO broadcast channel with common and private messages, is not known completely.

In the Gaussian MIMO broadcast channel with common and private messages, there are again three messages W_0,W_1,W_2 with rates R_0,R_1,R_2, respectively, such that W_0 is again sent to both users, W_1 (resp. W_2) is again directed to only the first (resp. second) user, however, there are no secrecy constraints on W_1,W_2. The capacity region of the Gaussian MIMO broadcast channel with common and private messages will be denoted by $\mathcal{C}^{\text{NS}}(\mathbf{S})$. The achievable rate region for the Gaussian MIMO broadcast channel with common and private messages that can be obtained by using DPC will be denoted by $\mathcal{R}_{12}^{\text{NS-DPC}}(\mathbf{S}),\mathcal{R}_{21}^{\text{NS-DPC}}(\mathbf{S})$ (depending on the encoding order), where $\mathcal{R}_{12}^{\text{NS-DPC}}(\mathbf{S})$ is given by the rate triples (R_0,R_1,R_2) satisfying

$$R_0\leq\min\{R_{01}^{\text{NS}}(\mathbf{K}_1,\mathbf{K}_2),R_{02}^{\text{NS}}(\mathbf{K}_1,\mathbf{K}_2)\} \quad (46)$$

$$R_1\leq R_1^{\text{NS}}(\mathbf{K}_1,\mathbf{K}_2) \quad (47)$$

$$R_2\leq R_2^{\text{NS}}(\mathbf{K}_2) \quad (48)$$

for some positive semi-definite matrices $\mathbf{K}_1,\mathbf{K}_2$ such that $\mathbf{K}_1+\mathbf{K}_2\preceq\mathbf{S}$, and $\{R_{0j}^{\text{NS}}(\mathbf{K}_1,\mathbf{K}_2)\}_{j=1}^2$, $R_1^{\text{NS}}(\mathbf{K}_1,\mathbf{K}_2),R_2^{\text{NS}}(\mathbf{K}_2)$ are defined as

$$R_{0j}^{\text{NS}}(\mathbf{K}_1,\mathbf{K}_2)=\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_j|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_j|},\quad j=1,2 \quad (49)$$

$$R_1^{\text{NS}}(\mathbf{K}_1,\mathbf{K}_2)=\frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_1|}{|\mathbf{K}_2+\mathbf{\Sigma}_1|} \quad (50)$$

$$R_2^{\text{NS}}(\mathbf{K}_2)=\frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} \quad (51)$$

Moreover, $\mathcal{R}_{21}^{\text{NS-DPC}}(\mathbf{S})$ can be obtained from $\mathcal{R}_{12}^{\text{NS-DPC}}(\mathbf{S})$ by swapping the subscripts 2 and 1. This achievable rate region was proposed in [14].

We now state a result of [9] on the capacity region of the Gaussian MIMO broadcast channel with common and private messages, which is that for a given common message rate R_0, the private messages sum rate capacity, i.e., R_1+R_2, is achieved by both $\mathcal{R}_{12}^{\text{NS}}(\mathbf{S})$ and $\mathcal{R}_{21}^{\text{NS}}(\mathbf{S})$. This result can also be stated as follows

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}^{\rm NS}(\mathbf{S})} \mu_0' R_0 + \mu_1' R_1 + \mu_2' R_2$$
$$= \max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\rm NS-DPC}(\mathbf{S})} \mu_0' R_0 + \mu_1' R_1 + \mu_2' R_2 \quad (52)$$
$$= \max_{(R_0,R_1,R_2)\in\mathcal{R}_{21}^{\rm NS-DPC}(\mathbf{S})} \mu_0' R_0 + \mu_1' R_1 + \mu_2' R_2 \quad (53)$$

for $\mu_1' = \mu_2' = \mu'$. This result is crucial to understand the aforementioned two facts suggested by Theorem 1, which will be explained next using (52)-(53).

In the proof of Theorem 1, first, we characterize the boundary of $\mathcal{R}_{12}^{\rm S-DPC}(\mathbf{S})$ by finding the properties of the covariance matrices that achieve the boundary of $\mathcal{R}_{12}^{\rm S-DPC}(\mathbf{S})$, see Lemma 1. According to Lemma 1, the boundary of $\mathcal{R}_{12}^{\rm S-DPC}(\mathbf{S})$ can be achieved by using the covariance matrices $\mathbf{K}_1^*, \mathbf{K}_2^*$ satisfying (17)-(18). On the other hand, using these covariance matrices, we can also achieve the boundary points of $\mathcal{R}_{12}^{\rm NS-DPC}(\mathbf{S})$, which are actually on the boundary of the capacity region $\mathcal{C}^{\rm NS}(\mathbf{S})$ as well, and are the private message sum rate capacity points for a given common message rate. To see this point, we define $\mu' = \mu_1 + \mu_2, \mu_0' = 1 + \mu_1 + \mu_2$ and $\gamma = \frac{\lambda+\mu_2}{1+\mu_1+\mu_2}$, i.e., $\bar{\gamma} = 1 - \gamma = \frac{\lambda+\mu_1}{1+\mu_1+\mu_2}$. Thus, the conditions in (17)-(18) can be written as

$$\mu'(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1 = \mu_0'\gamma(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mu_0'\bar{\gamma}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} + \mathbf{M}_S \quad (54)$$
$$\mu'(\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} + \mathbf{M}_2 = \mu'(\mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1 \quad (55)$$

which are the necessary conditions that the following problem needs to satisfy

$$\max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\rm NS-DPC}(\mathbf{S})} \mu_0' R_0 + \mu'(R_1 + R_2) \quad (56)$$

On the other hand, due to (52)-(53), we know that the solution of (56) gives us the private message sum rate capacity for a given common message rate, i.e., the points that achieve the maximum in (56) are on the boundary of the capacity region $\mathcal{C}^{\rm NS}(\mathbf{S})$. Furthermore, the maximum value in (56) can also be achieved by using the other possible encoding order, i.e.,

$$\max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\rm NS-DPC}(\mathbf{S})} \mu_0' R_0 + \mu'(R_1 + R_2)$$
$$= \max_{(R_0,R_1,R_2)\in\mathcal{R}_{21}^{\rm NS-DPC}(\mathbf{S})} \mu_0' R_0 + \mu'(R_1 + R_2) \quad (57)$$

Thus, this discussion reveals that there is a one-to-one correspondence between any rate triple on the boundary of $\mathcal{R}_{12}^{\rm S-DPC}(\mathbf{S})$ and the private messages sum rate capacity points on $\mathcal{C}^{\rm NS}(\mathbf{S})$. Hence, the boundary of $\mathcal{R}_{12}^{\rm S-DPC}(\mathbf{S})$, similarly $\mathcal{R}_{21}^{\rm S-DPC}(\mathbf{S})$, can be constructed by considering the private messages sum rate capacity points on $\mathcal{C}^{\rm NS}(\mathbf{S})$. This connection between the private messages sum rate capacity points and the boundaries of $\mathcal{R}_{12}^{\rm S-DPC}(\mathbf{S})$, $\mathcal{R}_{21}^{\rm S-DPC}(\mathbf{S})$ intuitively explains the two facts suggested by Theorem 1: i) The achievable rate region for the Gaussian MIMO broadcast channel with common and confidential messages is invariant with respect to the encoding order, i.e., $\mathcal{R}_{12}^{\rm S-DPC}(\mathbf{S}) = \mathcal{R}_{21}^{\rm S-DPC}(\mathbf{S})$ because the boundaries of these two regions correspond to those points on the DPC region for the Gaussian MIMO broadcast channel with common and private messages, for which encoding order does not matter either. ii) We can obtain the entire capacity region of the Gaussian MIMO broadcast channel with common and confidential messages, although the capacity region of its non-confidential counterpart is not known completely. The reason is that the boundary of the capacity region of the Gaussian MIMO broadcast channel with common and confidential messages comes from those points on the boundary of the DPC region of its non-confidential counterpart, which are known to be private message sum rate optimal.

V. Conclusions

We study the Gaussian MIMO broadcast channel with common and confidential messages, and obtain the entire capacity region. We show that a variant of the S-DPC scheme proposed in [5] is capacity-achieving. We provide the converse proof by using channel enhancement [6] and an extremal inequality from [7]. We also investigate the connections between the Gaussian MIMO broadcast channel with common and confidential messages and its non-confidential counterpart to provide further insight into capacity result we obtained.

References

[1] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2007. Also available at [arXiv:0710.1920].

[2] A. Khisti and G. Wornell. Secure transmission with multiple antennas II: The MIMOME channel. *IEEE Trans. Inf. Theory*, to appear. Also available at http://allegro.mit.edu/bin/pubs-search.php.

[3] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory*, 55(9):4033–4039, Sep. 2009.

[4] H. D. Ly, T. Liu, and Y. Liang. Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages. Submitted to *IEEE Trans. Inf. Theory*, Jul. 2009. Also available at http://www.ece.tamu.edu/∼tieliu/publications.html.

[5] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz). Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, to appear. Also available at [arXiv:0903.3786].

[6] 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.

[7] H. Weingarten, T. Liu, , S. Shamai (Shitz), Y. Steinberg, and P. Viswanath. The capacity region of the degraded multiple-input multiple-output compound broadcast channel. *IEEE Trans. Inf. Theory*, 55(11):5011–5023, Nov. 2009.

[8] 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.

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

[10] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.

[11] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz). MIMO Gaussian broadcast channels with confidential and common messages. *IEEE ISIT* 2010, to appear. Also available at [arXiv:1001.2806v1].

[12] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Mar. 2009. Also available at [arXiv:0903.3096].

[13] E. Ekrem and S. Ulukus. Capacity region of Gaussian MIMO broadcast channels with common and confidential messages. submitted to IEEE Trans. Inf. Theory, Feb. 2010. Also available at [arXiv:1002.5026].

[14] 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.