2018 ICSEE International Conference on the Science of Electrical Engineering

Broadcasting Information subject to State Masking

Michael Dikshtein, Shlomo Shamai (Shitz)
Department of EE, Technion, Haifa 32000, Israel, {michaeldic@campus,sshlomo@ee}.technion.ac.il

***Abstract*—We study the problem of coding over a general discrete memoryless broadcast channel controlled by random parameters. The parameters are available at the transmitter in a non-causal manner and are subject to a state masking constraint on the receivers. We derive inner and outer bounds on the achievable region and show that for the special case of Gaussian broadcast channel with private messages, these bounds are tight.**

***Index Terms*—Dirty paper coding, Gelf'and-Pinsker scheme, noncausal CSI, Broadcast channel, state masking.**

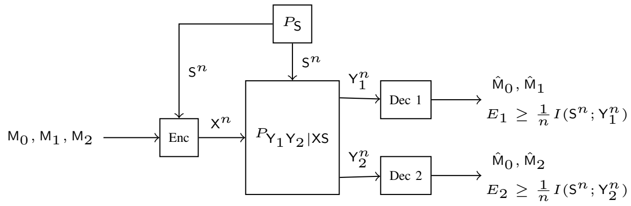
P_{S}
S^n
S^n
$\mathsf{M}_0, \mathsf{M}_1, \mathsf{M}_2$
Enc
X^n
$P_{\mathsf{Y}_1\mathsf{Y}_2|\mathsf{X}\mathsf{S}}$
Y_1^n
Y_2^n
Dec 1
Dec 2
$\hat{\mathsf{M}}_0, \hat{\mathsf{M}}_1$
$E_1 \geq \frac{1}{n} I(\mathsf{S}^n; \mathsf{Y}_1^n)$
$\hat{\mathsf{M}}_0, \hat{\mathsf{M}}_2$
$E_2 \geq \frac{1}{n} I(\mathsf{S}^n; \mathsf{Y}_2^n)$

Fig. 1. System model for general BC subject to state masking constraints.

I. Introduction

We consider a discrete memoryless broadcast channel (DMBC) with random parameters and channel side information (CSI) known in a noncausal manner to the transmitter subject to a state masking criterion at the receivers, depicted in Figure 1.

The single-letter expression for the capacity of the point to point discrete memoryless channel (DMC) with noncausal CSI at the encoder (the G-P channel) was derived in the seminal work of Gel'fand and Pinsker [1]. One of the most interesting special cases of the G-P channel is the Gaussian additive noise and interference setting in which the additive interference plays the role of the state sequence, which is known non-causally to the transmitter. Costa showed in [2] that the capacity of this channel is equal to the capacity of the same channel without additive interference. The capacity achieving scheme of [2] (which is that of [1] applied to the Gaussian case) is termed "writing on dirty paper" (WDP). Cohen and Lapidoth [3] showed that any interference sequence can be totally removed when the channel noise is ergodic and Gaussian.

The DMBC was first introduced by Cover [4]. The capacity region of the DMBC is still an open problem. The largest known inner bound on the capacity region of the DMBC with private messages was derived by Marton [5]. Liang [6] derived an inner bound on the capacity region of the DMBC with an additional common message. The best outer bound for DMBC with a common message is due to Nair and El Gamal [7]. There are however some special cases where the capacity region is fully characterized. For example the capacity region of the degraded DMBC was established by Gallager [8]. The capacity region of the Gaussian BC was derived by Bergmans [9]. An interesting result is the capacity region of the Gaussian MIMO BC which was established by Weingarten et al. [10]. The authors introduced a new notion of *an enhanced channel* and used it jointly with the Entropy Power Inequality (EPI) to show their result. The capacity achieving scheme relies on the dirty paper coding technique. Liu and Viswanath [11] developed *an extremal inequality* proof technique and showed that it can be used to establish a converse result in various Gaussian MIMO multiterminal networks, including the Gaussian MIMO BC with private messages. Recently, Geng and Nair [12] developed a different technique to characterize the capacity region of Gaussian MIMO BC with common and private messages.

Degraded DMBC with causal and noncausal side information was introduced by Steinberg [13]. Inner and outer bounds were derived on the capacity region. For the special case in which the nondegraded user is informed about the channel parameters, it was shown that the bounds are tight, thus deriving the capacity region for that case. The general DMBC with noncausal CSI at the encoder was studied by Steinberg and Shamai [14]. An inner bound was derived and it was shown to be tight for the Gaussian BC with independent additive interference at both channels. Outer bounds for DMBC with CSI at the encoder were derived in [15].

The problem of state-masking and information rate trade-off was introduced in [16]. In that work, the state sequence was treated as an undesired information that leaks to the receiver and is known to the transmitter. The measure of ability of the receiver to learn about the state from the received sequence was defined as the normalized block-wise mutual information between the state sequence S^n and the received sequence Y^n, that is, $I(\mathsf{S}^n;\mathsf{Y}^n)/n$.

The concept of state amplification is a dual problem to state masking. Kim et al. [17] considered the problem of transmitting data at rate R over a DMC with random parameters and CSI at the encoder and simultaneously conveying the information about the channel state itself to the receiver. They defined the channel state uncertainty reduction rate to be $\Delta \triangleq \frac{1}{n}(H(S^n) - \log|L_n|)$, where $|L_n|$ is the receiver list size in list decoding of the state, and found the (R, Δ) achievable region.

Courtade [18] considered a joint scenario, with two-encoder source coding setting where one source is to be amplified, while the other source is to be masked. Koyluoglu et al.

978-1-5386-6378-3/18/$31.00 ©2018 IEEE

[19] considered a state-dependent BC with state sequence known in noncausal manner to Alice (the transmitter) and its goal is to effectively convey the state to Bob (receiver 1) while "masking" it from Eve (receiver 2). Liu and Chen [20] considered the problem of message transmission and state estimation over Gaussian BC, where both received signals interfered by same additive Gaussian state. Grover and Sahai [21] related the problem of state masking to Witsenhausen's Counter-example [22]. Tutuncuoglu et al. [23] studied the problem of state amplification and state masking in an energy harvesting binary channel. They considered a situation where the binary encoder is connected to a battery source B_i which tries to harvest energy E_i at every time slot i and were interested in how much the decoder, that has no knowledge of the battery state B_i nor the energy process E_i, can learn about the energy arrival process E^n. A privacy-constrained information extraction problem was recently considered by Asoodeh et al. [24]. In their setting, they divided the information to be conveyed into private information and public information and also used the mutual information measures to determine the trade-off between public information transmission and private data leakage. A good tutorial on channel coding in the presence of CSI that also covers the state masking setting can be found in [25].

In this work, we extend the state masking scenario to a broadcast channel corrupted by state which is known non-causally to the encoder. In our setting the encoder wishes to reliably transmit common and private information over state-dependent channel to two receivers, while simultaneously minimizing the amount of information each receiver can learn about the state sequence s^n. We develop inner and outer bounds and show that they are tight for a special case of state-dependent Gaussian BC with private messages.

II. Notations and Problem Formulation

Throughout the paper, random variables are denoted using a sans-serif font, e.g., X, their realizations are denoted by the respective lower case letters, e.g., x, and their alphabets are denoted by the respective calligraphic letter, e.g., $\mathcal{X}$. Let $\mathcal{X}^n$ stand for the set of all n-tuples of elements from $\mathcal{X}$. An element from $\mathcal{X}^n$ is denoted by $x^n = (x_1, x_2, \ldots, x_n)$ and substrings by $x_i^j = (x_i, x_{i+1}, \ldots, x_j)$. The cardinality of a finite set, say $\mathcal{X}$, is denoted by $|\mathcal{X}|$. The probability distribution function of X, the joint distribution function of X and Y, and the conditional distribution of X given Y are denoted by P_{X}, $P_{\mathsf{X,Y}}$ and $P_{\mathsf{X|Y}}$ respectively. The expectation of X is denoted by $\mathbb{E}[\mathsf{X}]$. The probability of an event $\mathcal{E}$ is denoted as $\mathbb{P}\{\mathcal{E}\}$. The set of jointly ϵ-typical n-tuples (x^n, y^n) is defined as $\mathcal{T}_\epsilon^{(n)}(P_{\mathsf{XY}})$ [26].

A set of consecutive integers starting at 1 and ending in 2^{nR} are denoted as $\mathcal{I}_R \triangleq \{1, 2, \ldots, 2^{nR}\}$.

Let $\mathcal{X}, \mathcal{S}, \mathcal{Y}_1, \mathcal{Y}_2$ be finite sets, and let P_S be a probability mass function (pmf) on $\mathcal{S}$. We consider a 2-receiver discrete memoryless broadcast channel with random parameters $(\mathcal{S}, P_{\mathsf{S}}, \mathcal{X}, P_{\mathsf{Y}_1,\mathsf{Y}_2|\mathsf{X},\mathsf{S}}, \mathcal{Y}_1 \times \mathcal{Y}_2)$ that consists of an input alphabet $\mathcal{X}$, a state alphabet $\mathcal{S}$ and two output alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$ and a probability transition function $P_{\mathsf{Y}_1,\mathsf{Y}_2|\mathsf{X},\mathsf{S}}$, where the states S_i, $i = 1, 2, \ldots$, are random taking values in $\mathcal{S}$ and drawn from a discrete memoryless source (DMS) $P_{\mathsf{S}^n}(s^n) = \prod_{i=1}^n P_{\mathsf{S}}(s_i)$. The channel is assumed to be memoryless and without feedback. Thus, probabilities on n-tuples are given by:

$$P_{\mathsf{Y}_1^n\mathsf{Y}_2^n|\mathsf{X}^n\mathsf{S}^n}(y_1^n, y_2^n|x^n, s^n) = \prod_{i=1}^n P_{\mathsf{Y}_1\mathsf{Y}_2|\mathsf{XS}}(y_{1i}, y_{2i}|x_i, s_i).$$

The channel input signal is subject to an average input cost constraint $\frac{1}{n}\sum_{i=1}^n \phi(\mathsf{X_i}) \le \Gamma$, where $\phi : \mathcal{X} \to \mathbb{R}^+$ is the input cost function and $\Gamma > 0$ is a given constant.

A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code for the broadcast channel with state sequence S^n known non-causally at the encoder consists of

- Three message sets $\mathcal{I}_{R_0}$, $\mathcal{I}_{R_1}$ and $\mathcal{I}_{R_2}$.
- An encoder that assigns a codeword $x^n(m_0, m_1, m_2, s^n)$ to each message-state quadruple $(m_0, m_1, m_2, s^n) \in \mathcal{I}_{R_0} \times \mathcal{I}_{R_1} \times \mathcal{I}_{R_2} \times \mathcal{S}^n$.
- Two decoders, where decoder 1 assigns an estimate $\hat{m}_{01} \in \mathcal{I}_{R_0}$ and $\hat{m}_1 \in \mathcal{I}_{R_1}$ to each received sequence y_1^n, and decoder 2 assigns an estimate $\hat{m}_{02} \in \mathcal{I}_{R_0}$ and $\hat{m}_2 \in \mathcal{I}_{R_2}$ to each received sequence y_2^n.

Let $(\hat{\mathsf{M}}_{01}, \hat{\mathsf{M}}_1)$ and $(\hat{\mathsf{M}}_{02}, \hat{\mathsf{M}}_2)$ denote the outputs of decoder 1 and decoder 2, respectively. We assume that the message triple $(\mathsf{M}_0, \mathsf{M}_1, \mathsf{M}_2)$ is uniformly distributed over $\mathcal{I}_{R_0} \times \mathcal{I}_{R_1} \times \mathcal{I}_{R_2}$. The average probability of error is defined as

$$P_e^{(n)} = \mathbb{P}\left\{\bigcup_{k=1}^{2}\{(\hat{\mathsf{M}}_{0k}, \hat{\mathsf{M}}_k) \neq (\mathsf{M}_0, \mathsf{M}_k)\}\right\}. \tag{1}$$

The average probability of error at each receiver is defined as

$$P_{e,k}^{(n)} = \mathbb{P}\left\{(\hat{\mathsf{M}}_{0k}, \hat{\mathsf{M}}_k) \neq (\mathsf{M}_0, \mathsf{M}_k)\right\}, \quad k = 1, 2. \tag{2}$$

Obviously the average probability $P_e^{(n)}$ tends to zero as $n \to \infty$, iff both $P_{e,1}^{(n)}$ and $P_{e,2}^{(n)}$ tend to zero as $n \to \infty$.

We are interested in the interplay between reliable coding at rate triples (R_0, R_1, R_2) which we would like to keep as high as possible and the (normalized) mutual informations $I(\mathsf{S}^n; \mathsf{Y}_1^n)/n$ and $I(\mathsf{S}^n; \mathsf{Y}_2^n)/n$, which we would like to make as small as possible.

Definition 1. For a given $\Gamma > 0$, a quintuple $(R_0, R_1, R_2, E_1, E_2)$ is said to be achievable if for every $\epsilon > 0$ and sufficiently large n, there exists a sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ codes such that the following conditions are simultaneously satisfied:

$$\frac{1}{n}\sum_{i=1}^n \phi(X_i) \le \Gamma, \tag{3a}$$

$$P_e^{(n)} \le \epsilon, \tag{3b}$$

$$\frac{1}{n}I(\mathsf{S}^n; \mathsf{Y}_k^n) \le E_k + \epsilon, \quad k = 1, 2. \tag{3c}$$

Definition 2. The achievable region $\mathcal{R}$ is the closure of the set of all achievable quintuples $\{(R_0, R_1, R_2, E_1, E_2)\}$.

Definition 3. The achievable region $\mathcal{R}_0$ is the set of all zero-rates achievable pairs $\{(R_0, R_1, R_2, E_1, E_2)\} = \{(0, 0, 0, E_1, E_2)\}$.

III. Main Results

As mentioned before, the capacity region of the general DMBC is unknown even for channels without state. In this section we present inner and outer bounds on the achievable region. We begin with the inner bound. The inner bound on the rate-triple (R_0, R_1, R_2) is essentially the same as was given in [14], but our proof is simpler, and we also contribute a bound on the equivocation rate-pair (E_1, E_2). The main idea behind the proof is integration of Marton and GP coding, where for each message, a subcodebook is generated, whose size is large enough such that for every state sequence s^n a jointly typical auxiliary codeword can be found in the subcodebook.

Proposition 1. *An achievable region $\mathcal{R}$ consists of a quintuple $(R_0, R_1, R_2, E_1, E_2)$ that satisfies the following conditions*

$$R_0 \le \min\{I(\mathsf{W};\mathsf{Y}_1), I(\mathsf{W};\mathsf{Y}_2)\} - I(\mathsf{W};\mathsf{S}), \tag{4a}$$

$$R_0 + R_1 \le I(\mathsf{W},\mathsf{U};\mathsf{Y}_1) - I(\mathsf{W},\mathsf{U};\mathsf{S}), \tag{4b}$$

$$R_0 + R_2 \le I(\mathsf{W},\mathsf{V};\mathsf{Y}_2) - I(\mathsf{W},\mathsf{V};\mathsf{S}), \tag{4c}$$

$$\begin{aligned} R_0 + R_1 + R_2 \le{}& I(\mathsf{W},\mathsf{U};\mathsf{Y}_1) - I(\mathsf{W},\mathsf{U};\mathsf{S}) + I(\mathsf{W},\mathsf{V};\mathsf{Y}_2) \\ &- I(\mathsf{W},\mathsf{V};\mathsf{S}) - \min\{I(\mathsf{W};\mathsf{Y}_1), I(\mathsf{W};\mathsf{Y}_2)\} \\ &- I(\mathsf{W};\mathsf{S}) - I(\mathsf{U};\mathsf{V}|\mathsf{W},\mathsf{S}), \end{aligned} \tag{4d}$$

$$E_1 \le I(\mathsf{S};\mathsf{W},\mathsf{U},\mathsf{Y}_1), \tag{4e}$$

$$E_2 \le I(\mathsf{S};\mathsf{W},\mathsf{V},\mathsf{Y}_2), \tag{4f}$$

for some pmf $P_{\mathsf{SWUXY_1Y_2}} = P_{\mathsf{S}} P_{\mathsf{WUVX|S}} P_{\mathsf{Y_!Y_2|XS}}$.

We give an outline of the proof in Section IV-A while the full proof can be found in the extended version of this paper [27].

Next, we provide the outer bound on $\mathcal{R}$.

Proposition 2. *If a rate quintuple $(R_0, R_1, R_2, E_1, E_2)$ is achievable for the DM-BC with random parameters and CSI known non-causally at the transmitter, then there exists a distribution $P_{\mathsf{WUVX|S}}$ such that the following inequalities are satisfied:*

$$R_0 \le \min\{I(\mathsf{W};\mathsf{Y}_1|\mathsf{S}), I(\mathsf{W};\mathsf{Y}_2|\mathsf{S})\} \tag{5a}$$

$$\begin{aligned} R_0 + R_1 \le{}& \min\{I(\mathsf{W};\mathsf{Y}_1|\mathsf{S}), I(\mathsf{W};\mathsf{Y}_2|\mathsf{S})\} \\ &+ I(\mathsf{U};\mathsf{Y}_1|\mathsf{W},\mathsf{S}) \end{aligned} \tag{5b}$$

$$\begin{aligned} R_0 + R_2 \le{}& \min\{I(\mathsf{W};\mathsf{Y}_1|\mathsf{S}), I(\mathsf{W};\mathsf{Y}_2|\mathsf{S})\} \\ &+ I(\mathsf{V};\mathsf{Y}_2|\mathsf{W},\mathsf{S}) \end{aligned} \tag{5c}$$

$$\begin{aligned} R_0 + R_1 + R_2 \le{}& \min\{I(\mathsf{W};\mathsf{Y}_1|\mathsf{S}), I(\mathsf{W};\mathsf{Y}_2|\mathsf{S})\} \\ &+ I(\mathsf{U};\mathsf{Y}_1|\mathsf{W},\mathsf{S}) + I(\mathsf{X};\mathsf{Y}_2|\mathsf{W},\mathsf{U},\mathsf{S}) \end{aligned} \tag{5d}$$

$$\begin{aligned} R_0 + R_1 + R_2 \le{}& \min\{I(\mathsf{W};\mathsf{Y}_1|\mathsf{S}), I(\mathsf{W};\mathsf{Y}_2|\mathsf{S})\} \\ &+ I(\mathsf{X};\mathsf{Y}_1|\mathsf{W},\mathsf{V},\mathsf{S}) + I(\mathsf{V};\mathsf{Y}_2|\mathsf{W},\mathsf{S}) \end{aligned} \tag{5e}$$

$$E_k \ge I(\mathsf{S};\mathsf{Y}_k) \quad k = 1, 2, \tag{5f}$$

where $P_{\mathsf{SWUVXY_1Y_2}} = P_{\mathsf{S}} P_{\mathsf{WUVX|S}} P_{\mathsf{Y_1Y_2|XS}}$.

We give an outline of the proof in Section IV-B while the full proof can be found in the extended version of this paper [27].

In some practical applications the transmitter is solely intended to minimize the leakage without transmitting any information. This scenario is also simpler to analyze in the zero rate triple case $(R_0, R_1, R_2) = (0, 0, 0)$. In such a scenario our goal is to minimize $I(S^n; Y_1^n)/n$ and $I(S^n; Y_2^n)/n$.

Let $\mathcal{E}_0(\mathsf{X})$ be the set of equivocation rate pairs (E_1, E_2) such that $E_k \ge I(\mathsf{S};\mathsf{Y}_k)$, $k = 1, 2$. Following is a characterization of the achievability region for $(R_0, R_1, R_2) = (0, 0, 0)$.

Theorem 1. *The achievable zero-rates region $\mathcal{R}_0$ of the DM-BC with random parameters $p(y_1, y_2|x, s)$ is the convex hull of the union of the regions $\mathcal{E}_0(\mathsf{X})$ over all $p(x|s)$.*

Proof: The theorem follows from the inner bound in Proposition 1 and the outer bound in Proposition 2, and respectively (4) and (5) by the following choice of auxiliary random variables: $\mathsf{W} = \emptyset$, $\mathsf{U} = \emptyset$ and $\mathsf{V} = \emptyset$. In this case, the encoder simply generates X^n given S^n according to $\prod_{i=1}^n P_{\mathsf{X|S}}(x_i|s_i)$. Since this creates a memoryless "channel" from S to $(\mathsf{Y}_1, \mathsf{Y}_2)$ we get that $I(\mathsf{S}^n; \mathsf{Y}_k^n)/n = I(\mathsf{S};\mathsf{Y})$. ■

IV. Proofs Outline

In this section we provide an outline to the proofs of Proposition 1 and Proposition 2.

A. Inner Bound

Fix the conditional pmf $P_{\mathsf{WUVX|S}}$ and let $n \to \infty$. Randomly and independently generate $2^{n(R_0+\tilde{R}_0)}$ sequences $w^n(m_0, l_0)$, $m_0 \in \mathcal{I}_{R_0}$, $l_0 \in \mathcal{I}_{\tilde{R}_0}$, according to $\prod_{i=1}^n P_{\mathsf{W}}(w_i)$. For each (m_0, l_0), generate $2^{n(R_2+\tilde{R}_2)}$ independent sequences $v^n(m_0, l_0, m_2, l_2)$, $m_2 \in \mathcal{I}_{R_2}$, $l_2 \in \mathcal{I}_{\tilde{R}_2}$, according to $\prod_{i=1}^n P_{\mathsf{V|W}}(v_i|w_i(m_0, l_0))$. Similarly, for each (m_0, l_0), generate $2^{n(R_1+\tilde{R}_{1s}+\tilde{R}_{12})}$ independent sequences $u^n(m_0, l_0, m_1, l_{1s}, l_{12})$, $m_1 \in \mathcal{I}_{R_1}$, $l_{1s} \in \mathcal{I}_{\tilde{R}_{1s}}$, $l_{12} \in \mathcal{I}_{\tilde{R}_{12}}$, according to $\prod_{i=1}^n P_{\mathsf{U|W}}(u_i|w_i(m_0, l_0))$. Let (m_0', m_1', m_2') be the message triple to be sent with the state sequence s^n observed. First the encoder finds $\tilde{l}_0$, such that $(s^n, w^n(m_0', \tilde{l}_0)) \in \mathcal{T}_{\epsilon'}^{(n)}$. It can be shown that at least one such $\tilde{l}_0$ exists if $\tilde{R}_0 > I(\mathsf{W};\mathsf{S})$. Then, given $w^n(m_0', \tilde{l}_0)$, the encoder finds $\tilde{l}_2$, such that $(s^n, w^n(m_0', \tilde{l}_0), v^n(m_0', \tilde{l}_0, m_2', \tilde{l}_2)) \in \mathcal{T}_{\epsilon''}^{(n)}$. It can be shown that at least one such $\tilde{l}_2$ exists if $\tilde{R}_2 > I(\mathsf{V};\mathsf{S}|\mathsf{W})$. Similarly, given $w^n(m_0', \tilde{l}_0)$, the encoder finds $\tilde{l}_{1s}$, such that $(s^n, w^n(m_0', \tilde{l}_0), u^n(m_0', \tilde{l}_0, m_1', \tilde{l}_{1s}, l_{12})) \in \mathcal{T}_{\epsilon''}^{(n)}$ for every l_{12}. It can be shown that at least one such $\tilde{l}_{1s}$ exists if $\tilde{R}_{1s} > I(\mathsf{U};\mathsf{S}|\mathsf{W})$. Then, given $w^n(m_0', \tilde{l}_0)$, $v^n(m_0', \tilde{l}_0, m_2', \tilde{l}_2)$ and $\tilde{l}_{1s}$, the encoder finds $\tilde{l}_{12}$, such that $(s^n, w^n(m_0', \tilde{l}_0), v^n(m_0', \tilde{l}_0, m_2', \tilde{l}_2), u^n(m_0', \tilde{l}_0, m_1', \tilde{l}_{1s}, \tilde{l}_{12})) \in \mathcal{T}_{\epsilon'''}^{(n)}$. It can be shown that at least one such $\tilde{l}_{12}$ exists if $\tilde{R}_{1s} > I(\mathsf{U};\mathsf{V}|\mathsf{W},\mathsf{S})$. Finally, for each quadruple (m_0, m_1, m_2, s^n) generate a sequence $x^n(m_0, m_1, m_2, s^n)$ according to $\prod_{i=1}^n P_{\mathsf{X|WUVS}}(x_i|w_i, u_i, v_i)$. In order to transmit (m_0, m_1, m_2) given s^n send $x^n(m_0, m_1, m_2, s^n)$.

Decoders 1 and 2 use joint typicality decoding of (w^n, u^n, y_1^n) and (w^n, v^n, y_2^n) respectively. It can be shown with probability approaching 1 as $n \to \infty$ the following rates are achievable

$$\begin{aligned} R_0 &\le \min\{I(\mathsf{W};\mathsf{Y}_1), I(\mathsf{W};\mathsf{Y}_2)\} - I(\mathsf{W};\mathsf{S}),\\ R_0+R_2 &\le I(\mathsf{W},\mathsf{V};\mathsf{Y}_2) - I(\mathsf{W},\mathsf{V};\mathsf{S}),\\ R_0+R_1 &\le I(\mathsf{W},\mathsf{U};\mathsf{Y}_1)-I(\mathsf{W};\mathsf{S})-I(\mathsf{U};\mathsf{V},\mathsf{S}|\mathsf{W})\\ &= I(\mathsf{W},\mathsf{U};\mathsf{Y}_1)-I(\mathsf{W},\mathsf{U};\mathsf{S})-I(\mathsf{U};\mathsf{V}|\mathsf{W},\mathsf{S}).\end{aligned} \tag{6}$$

As for the upper bound on the mutual information between S^n and Y_1^n,

$$\begin{aligned} I(\mathsf{S}^n;\mathsf{Y}_1^n) &\le I(\mathsf{S}^n;\mathsf{W}^n,\mathsf{U}^n,\mathsf{Y}_1^n)\\ &\le I(\mathsf{S}^n;\mathsf{W}^n,\mathsf{U}^n|\mathsf{M}_0,\mathsf{M}_1) + I(\mathsf{S}^n;\mathsf{Y}_1^n|\mathsf{W}^n,\mathsf{U}^n)\\ &\overset{(a)}{\le} H(\mathsf{W}^n|\mathsf{M}_0) + H(\mathsf{U}^n|\mathsf{W}^n,\mathsf{M}_0,\mathsf{M}_1)\\ &\quad - H(\mathsf{U}^n|\mathsf{W}^n,\mathsf{M}_0,\mathsf{M}_1,\mathsf{S}^n) + nI(\mathsf{S};\mathsf{Y}_1|\mathsf{W},\mathsf{U})\\ &\overset{(b)}{\le} n(\tilde{R}_0 + \tilde{R}_{1s} + \tilde{R}_{12} - \tilde{R}_{12} + I(\mathsf{S};\mathsf{Y}_1|\mathsf{W},\mathsf{U}))\\ &= nI(\mathsf{S};\mathsf{Y}_1,\mathsf{W},\mathsf{U}) \end{aligned} \tag{7}$$

where (a) follows from the memorylessness of the channel $P_{\mathsf{Y}_2|\mathsf{W},\mathsf{U},\mathsf{S}}$. In (b) we used the fact that the sizes of each bin of $\mathcal{C}_0$ and $\mathcal{C}_1$ are $2^{n\tilde{R}_0}$ and $2^{n(\tilde{R}_{1s}+\tilde{R}_{12})}$, respectively. Furthermore, given $(w^n(m_0,l_0), m_0, m_1, s^n)$, u^n is uniform over $\mathcal{I}_{\tilde{R}_{12}}$. The upper bound for $I(\mathsf{S}^n;\mathsf{Y}_2^n)$ follows from similar considerations.

B. Outer bound

The outer bound on the achievable rates region can be shown by providing the state sequence s^n as side information to the receivers, defining the following auxiliary random variables for each $i \in [1:n]$

$$\mathsf{W}_i \triangleq (\mathsf{M}_0, \mathsf{Y}_1^{i-1}, \mathsf{S}^{i-1}, \mathsf{Y}_{2,i+1}^n, \mathsf{S}_{i+1}^n), \quad \mathsf{U}_i = \mathsf{M}_1, \quad \mathsf{V}_i \triangleq \mathsf{M}_2, \tag{8}$$

and a proper use of Csiszár and Körner sum identity [28].

As for the lower bound on the equivocation rates E_k, $k = 1,2$, we use the memorylessness property of the source P_S to show

$$I(\mathsf{S}^n;\mathsf{Y}_k^n) \ge \sum_{i=1}^n I(\mathsf{S}_i;\mathsf{Y}_{k,i}) \ge nI(\mathsf{S};\mathsf{Y}_k). \tag{9}$$

V. State-Dependent Gaussian BC

In this section we consider a scalar additive white Gaussian noise BC with additive state. The channel outputs corresponding to the inputs $(\mathsf{X},\mathsf{S}_1,\mathsf{S}_2)$ are:

$$\mathsf{Y}_k = \mathsf{X} + \mathsf{S}_k + \mathsf{Z}_k, \quad k = 1,2 \tag{10}$$

where $\mathsf{Z}_k \sim \mathcal{N}(0,N_k)$, $k \in \{1,2\}$ are additive Gaussian noises, $\mathsf{S}_k \sim \mathcal{N}(0,Q_k), k \in \{1,2\}$ are additive Gaussian random variables, both known noncausally at the transmitter. The Gaussian random variables $\mathsf{Z}_1, \mathsf{Z}_2, \mathsf{S}_1$ and S_2 are mutually independent and the equivocation rates are measured between the outputs and the state $\mathbf{S} = (\mathsf{S}_1,\mathsf{S}_2)$. The input X is power constrained to P, such that, $\frac{1}{n}\sum_{i=1}^n \mathsf{X}_i^2 \le P$. We further assume that $N_2 > N_1$ without loss of generality. Denote $P' \triangleq (1-\rho_1^2-\rho_2^2)P$.

Theorem 2. *The rate-leakage region of the Gaussian State-Dependent Broadcast Channel with private messages is the quadruple (R_1,R_2,E_1,E_2) such that*

$$R_1 \le \frac{1}{2}\log\left(1+\frac{\gamma P'}{N_1}\right), \tag{11}$$

$$R_2 \le \frac{1}{2}\log\left(1+\frac{\overline{\gamma}P'}{\gamma P'+N_2}\right), \tag{12}$$

$$E_k = \frac{1}{2}\log\frac{P+2\rho_k\sqrt{PQ_k}+Q_k+N_k}{P'+N_k}, \quad k=1,2. \tag{13}$$

for some $\gamma \in [0,1]$ and ρ_1, ρ_2 satisfying $\rho_1^2+\rho_2^2 \le 1$.

Proof: We start with the converse part, using Proposition 2 with $W = \emptyset$. Define the correlation coefficients between the state and the input sequences as $\rho_1 \triangleq \frac{\mathbb{E}[\mathsf{XS}_1]}{\sqrt{PQ_1}}$ and $\rho_2 \triangleq \frac{\mathbb{E}[\mathsf{XS}_2]}{\sqrt{PQ_2}}$. Define the state variable $\mathbf{S} \triangleq (\mathsf{S}_1,\mathsf{S}_2)$. And now proceed to lower bound the equivocation measures,

$$I(\mathbf{S};\mathsf{Y}_1) = h(\mathbf{S}) - h(\mathbf{S}|\mathsf{Y}_1). \tag{14}$$

The conditional differential entropy can be upper bounded as

$$h(\mathbf{S}|\mathsf{Y}_1) \le \frac{1}{2}\log(2\pi e)^2\frac{Q_1Q_2(P'+1)}{P+2\rho_1\sqrt{PQ_1}+Q_1+N_1}, \tag{15}$$

and

$$h(\mathbf{S}) = \frac{1}{2}\log(2\pi e)^2 Q_1Q_2. \tag{16}$$

The upper bound on E_2 follows by similar considerations.

The rates R_1 and R_2 can be upper bounded as

$$nR_1 \le I(\mathsf{X};\mathsf{Y}_1|\mathsf{V},\mathbf{S}) = h(\mathsf{X}+\mathsf{Z}_1|\mathsf{V},\mathbf{S}) - h(\mathsf{Z}_1) \tag{17}$$

$$nR_2 \le I(\mathsf{V};\mathsf{Y}_2|\mathbf{S}) = h(\mathsf{X}+\mathsf{Z}_2|\mathbf{S}) - h(\mathsf{X}+\mathsf{Z}_2|\mathsf{V},\mathbf{S}). \tag{18}$$

The first entropy term in (18) can be upper bounded as

$$h(\mathsf{X}+\mathsf{Z}_2|\mathbf{S}) \le \frac{1}{2}\log(2\pi e)(P'+N_2). \tag{19}$$

Similarly as in Bergmans's proof [9] to the converse of Gaussian BC, we first find lower and upper bounds for the second entropy term

$$h(\mathsf{X}+\mathsf{Z}_2|\mathsf{V},\mathbf{S}) \le h(\mathsf{X}+\mathsf{Z}_2|\mathbf{S}) \le \frac{1}{2}\log(2\pi e)(P'+N_2), \tag{20}$$

and

$$h(\mathsf{X}+\mathsf{Z}_2|\mathsf{V},\mathbf{S}) \ge h(\mathsf{X}+\mathsf{Z}_2|\mathsf{V},\mathsf{X},\mathbf{S}) = \frac{1}{2}\log(2\pi e N_2). \tag{21}$$

Hence, there must exist a $\gamma \in [0,1]$ such that

$$h(\mathsf{X}+\mathsf{Z}_2|\mathsf{V},\mathbf{S}) = \frac{1}{2}\log(2\pi e)(\gamma P'+N_2). \tag{22}$$

Now using the conditional EPI, we obtain

$$\begin{aligned} h(\mathsf{X}+\mathsf{Z}_2|\mathsf{V},\mathbf{S}) &= h(\mathsf{X}+\mathsf{Z}_1+\tilde{Z}_2|\mathsf{V},\mathbf{S})\\ &\ge \frac{1}{2}\log\left(2^{2h(\mathsf{X}+\mathsf{Z}_1|\mathsf{V},\mathbf{S})} + 2^{h(\tilde{Z}_2)}\right)\\ &= \frac{1}{2}\log\left(2^{2h(\mathsf{X}+\mathsf{Z}_1|\mathsf{V},\mathbf{S})} + 2\pi e(N_2-N_1)\right). \end{aligned} \tag{23}$$

This implies that

$$h(\mathsf{X}+\mathsf{Z}_1|\mathsf{V},\mathbf{S}) \leq \frac{n}{2}\log 2\pi e(\gamma P' + N_1). \tag{24}$$

By combining (17), (18), (22) and (24) we have shown that the outer bound on the capacity region consists of rate-pairs satisfying (11) and (12).

In order to prove the direct part, we use the achievability scheme that was proposed in [14], which integrates Marton coding and Gelfand-Pinsker coding. This scheme was shown to be optimal for Gaussian sources, in the sense that it cancels the state interference completely. In our model $\mathbf{S} = (\mathsf{S}_1, \mathsf{S}_2)$. We evaluate the mutual information terms in Proposition 1 by using the following choice of the auxiliary random variables:

$$W = \emptyset \qquad X_1' \sim \mathcal{N}(0,\gamma P') \qquad X_2' \sim \mathcal{N}(0,\overline{\gamma}P') \tag{25}$$

$$X = X_1' + X_2' + \beta_1\mathsf{S}_1 + \beta_2\mathsf{S}_2 \tag{26}$$

$$U = X_1' + \alpha_{10}X_2' + \alpha_{11}\mathsf{S}_1 + \alpha_{12}\mathsf{S}_2 \tag{27}$$

$$V = X_2' + \alpha_{21}\mathsf{S}_1 + \alpha_{22}\mathsf{S}_2 \tag{28}$$

with $\beta_1 = \rho_1\sqrt{\frac{P}{Q_1}}$, $\beta_1 = \rho_2\sqrt{\frac{P}{Q_2}}$, $\alpha_{10} = \frac{\gamma P'}{\gamma P'+N_1}$, $\alpha_{11} = \frac{(1+\beta_1)\gamma P'}{\gamma P'+N_1}$, $\alpha_{12} = \frac{\beta_2\gamma P'}{\gamma P'+N_1}$, $\alpha_{21} = \frac{\beta_1\overline{\gamma}P'}{P'+N_2}$ and $\alpha_{22} = \frac{(1+\beta_2)\overline{\gamma}P'}{P'+N_2}$. Hence,

$$I(\mathsf{U};\mathsf{Y}_1) - I(\mathsf{U};\mathsf{V},\mathsf{S}) = \frac{1}{2}\log\left(1+\frac{\gamma P'}{N_1}\right), \tag{29}$$

$$I(\mathsf{V};\mathsf{Y}_2) - I(\mathsf{V};\mathsf{S}) = \frac{1}{2}\log\left(1+\frac{\overline{\gamma}P'}{\gamma P'+N_2}\right). \tag{30}$$

The achievability of the equivocation rates follows by showing that

$$I(\mathsf{S};\mathsf{U}|\mathsf{Y}_1) = I(\mathsf{S};\mathsf{V}|\mathsf{Y}_2) = 0. \tag{31}$$

Subsituting (29) and (30) in the equations for (R_1, R_2, E_1, E_2) we obtain that (11), (12) and (13) are achievable and that meets the outer bound and thus we characterized the achievable region $\mathcal{R}$ for this channel. ■

VI. Conclusions

In this paper we addressed the problem of simultaneous communication and state masking over general DMBC with random parameters and parameters given as side information to the encoder. We developed inner and outer bounds on the achievable region containing rates and masking measures and showed that these bounds are tight for the state-dependent Gaussian BC with private messages. Moreover, the standard results as point-to-point masking [16] and state-dependent BC [14] (no masking demands), emerge as special cases of the bounds here. An extension to the MIMO Gaussian BC with private and common messages is under current study.

Acknowledgment

The work of M. Dikshtein and S. Shamai (Shitz) has been supported by the European Union's Horizon 2020 Research And Innovation Programme, grant agreement no. 694630 and the Heron consortium via the Israel minister of economy and science.

References

[1] S. Gel'fand and M. Pinsker. Coding for channels with ramdom parameters. *Probl. Contr. Inf. Theory*, 9(1):19–31, January 1980.

[2] M. H. M. Costa. Writing on dirty paper. *IEEE Trans. Inform. Theory*, 29(3):439–441, May 1983.

[3] A. S. Cohen and A. Lapidoth. Generalized writing on dirty paper. In *Proc. IEEE Int. Symp. Inf. Theory*, page 227, Jun/Jul 2002.

[4] T. Cover. Broadcast channels. *IEEE Trans. Inform. Theory*, 18(1):2–14, Jan 1972.

[5] K. Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans. Inform. Theory*, 25(3):306–311, May 1979.

[6] Y. Liang. *Multiuser communications with relaying and user cooperation*. PhD thesis, University of Illinois, Urbana-Champaign, IL., 2005.

[7] C. Nair and A. El Gamal. An outer bound to the capacity region of the broadcast channel. *IEEE Trans. Inform. Theory*, 53(1):350–355, Jan 2007.

[8] R. G. Gallager. Capacity and coding for degraded broadcast channels. *Probl. Pered. Inform.*, 10(3):3–14, July-Sept 1974.

[9] P. Bergmans. A simple converse for broadcast channels with additive white Gaussian noise (corresp.). *IEEE Trans. Inform. Theory*, 20(2):279–280, Mar 1974.

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

[11] T. Liu and P. Viswanath. An extremal inequality motivated by multiterminal information-theoretic problems. *IEEE Trans. Inform. Theory*, 53(5):1839–1851, May 2007.

[12] Y. Geng and C. Nair. The capacity region of the two-receiver Gaussian vector broadcast channel with private and common messages. *IEEE Trans. Inform. Theory*, 60(4):2087–2104, April 2014.

[13] Y. Steinberg. Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information. *IEEE Trans. Inform. Theory*, 51(8):2867–2877, Aug 2005.

[14] Y. Steinberg and S. Shamai (Shitz). Achievable rates for the broadcast channel with states known at the transmitter. In *Proc. IEEE Int. Symp. Inf. Theory, 2005*, pages 2184–2188, Sept 2005.

[15] R. Khosravi-Farsani and F. Marvasti. Capacity bounds for multiuser channels with non-causal channel state information at the transmitters. In *2011 IEEE Information Theory Workshop*, pages 195–199, Oct 2011.

[16] N. Merhav and S. Shamai. Information rates subject to state masking. *IEEE Trans. Inform. Theory*, 53(6):2254–2261, June 2007.

[17] Y. H. Kim, A. Sutivong, and T. M. Cover. State amplification. *IEEE Trans. Inform. Theory*, 54(5):1850–1859, May 2008.

[18] T. A. Courtade. Information masking and amplification: The source coding setting. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 189–193, July 2012.

[19] O. O. Koyluoglu, R. Soundararajan, and S. Vishwanath. State amplification subject to masking constraints. *IEEE Trans. Inform. Theory*, 62(11):6233–6250, Nov 2016.

[20] W. Liu and B. Chen. Message transmission and state estimation over Gaussian broadcast channels. In *2009 43rd Annual Conference on Information Sciences and Systems*, pages 147–151, March 2009.

[21] P. Grover and A. Sahai. Witsenhausen's counterexample as assisted interference suppression. *International Journal of Systems, Control and Communications*, 2(1-3):197–237, 2010.

[22] H. S Witsenhausen. A counterexample in stochastic optimum control. *SIAM Journal on Control*, 6(1):131–147, 1968.

[23] K. Tutuncuoglu, O. Ozel, A. Yener, and S. Ulukus. State amplification and state masking for the binary energy harvesting channel. In *2014 IEEE Information Theory Workshop (ITW 2014)*, pages 336–340, Nov 2014.

[24] Shahab Asoodeh, Mario Diaz, Fady Alajaji, and Tamás Linder. Information extraction under privacy constraints. *Information*, 7(1), 2016.

[25] G. Keshet, Y. Steinberg, and N. Merhav. Channel coding in the presence of side information. *Foundations and Trends® in Communications and Information Theory*, 4(6):445–586, 2008.

[26] A. El Gamal and Y.H. Kim. *Network information theory.* Cambridge : Cambridge University Press, c2011., 2011.

[27] Michael Dikshtein and Shlomo Shamai. Broadcasting Information subject to State Masking, 2018; arXiv:1810.11781.

[28] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, 1978.