Reliability of the Gaussian Broadcast Channel with Common Message and Feedback

Youlong Wu
Comm. and Electr. Department
Telecom ParisTech
Paris, France
youlong.wu@telecom-paristech.fr

Paolo Minero
Dept. of Electrical Engineering
Notre Dame University
Notre Dame, Indiana
pminero@nd.edu

Michèle Wigger
Comm. and Electr. Department
Telecom ParisTech
Paris, France
michele.wigger@telecom-paristech.fr

***Abstract*—We consider the two-user memoryless Gaussian broadcast channel (BC) with feedback and common message only. We show that linear-feedback schemes with message points, in the spirit of Schalkwijk&Kailath's scheme for point-to-point channels or Ozarow&Leung's scheme for BCs with private messages, are strictly suboptimal for this setup. In fact even with perfect feedback, the maximum rate achieved by these schemes is strictly smaller than capacity (which is the same with and without feedback).**

In contrast, rate-limited feedback suffices for bursty-feedback schemes to achieve double-exponential decay of the probability of error when the feedback rate R_{FB} is at least equal to the forward rate R.

***Index Terms*—Broadcast channel, Feedback, Capacity, Reliability, Linear schemes**

I. Introduction

We consider the two-user Gaussian broadcast channel (BC) where the transmitter sends a single common message to both receivers. For this setup, even perfect feedback cannot increase capacity. Feedback can however potentially reduce the minimum probability of error for a given blocklength n.

In fact, for Gaussian point-to-point channels [1], [2] or for memoryless Gaussian networks such as the multiple-access channel (MAC) [3] and the BC with private messages [9], perfect feedback allows to have a double-exponential decay of the probability of error in the blocklength. These super-exponential decays of the probability of error are achieved by Schalkwijk-Kailath type schemes that first map the message(s) into real message point(s) and then send as their channel inputs linear combinations of the message point(s) and the past feedback signals. We call such schemes *linear-feedback schemes with message points* or (with some abuse of notation) *linear-feedback schemes* for short. Such schemes are known to achieve the (sum-)capacity of Gaussian point-to-point channels (with or without memory) [1], [2] and of the two-user memoryless Gaussian MAC [3]. For $K \geq 3$-user Gaussian MACs they are optimal among a large class of schemes [4], [5], and for Gaussian BCs with private messages, they achieve the largest sum-rates known to date [6], [7], [8].

In this paper we show that while performing well (or optimally) in the above mentioned examples, linear-feedback schemes with message points are strictly suboptimal for the two-user memoryless Gaussian BC with common message only. In fact, for the BC with common message, the largest rate achieved by linear-feedback schemes with message points is strictly smaller than the capacity, which is the same with and without feedback. As a consequence, for this setup, linear-feedback schemes also fail to achieve double-exponential decay of the probability of error for rates close to capacity. We prove this result by showing that for any sequence of linear-feedback schemes that sends a common message at rate $R > 0$ with arbitrary small probability of error, it is possible to construct a sequence of linear-feedback schemes that send two independent private messages at rates $R_1 \geq R$ and $R_2 \geq R$ again with arbitrary small probability of error. Thus, intuitively, the class of linear-feedback schemes with message points cannot take advantage of the fact that both receivers are interested in the same message.

As we show, this is however only a shortcoming of the class of linear-feedback schemes with message points. In fact, we present a sequence of coding schemes that uses the feedback in a bursty way (that means the feedback signals are used only in very few transmissions as in [10]) and that can achieve double-exponential decay of the probability of error for all rates up to capacity. Moreover, in our scheme it suffices to have rate-limited feedback with feedback rate R_{fb} no smaller than the forward rate R.

The rest of the paper is organized as follows. In Section II we explain the channel model. In Section III the sub-optimality of linear-feedback coding schemes is established. In Section IV we present a bursty-feedback scheme achieving double-exponential decay of the probability of error.

II. System Model

We consider the two-receiver Gaussian broadcast channel. If X_i denotes the transmitter's channel input at time $i \in \{1, \ldots, n\}$, the channel output at Receiver $u \in \{1, 2\}$ at time i is

$$Y_{u,i} = X_i + Z_{u,i} \tag{1}$$

where $\{Z_{u,i}\}_{i=1}^n$ are independent and identically distributed (iid) centered bivariate Gaussians of covariance matrix $\begin{pmatrix} \sigma_1^2 & 0 \\ 0 & \sigma_2^2 \end{pmatrix}$. Without loss of generality we assume $\sigma_1^2 \geq \sigma_2^2$.

The transmitter wishes to convey a common message M to both receivers, where M is uniformly distributed over

the message set $\mathcal{M} \triangleq \{1, ..., \lfloor e^{nR} \rfloor\}$, independently of the noise sequences $\{Z_{1,i}\}$ and $\{Z_{2,i}\}$. Here, n is the blocklength and $R > 0$ the rate of transmission. It is assumed that the transmitter obtains feedback from both receivers. That means, after each channel use i, each Receiver u feeds back a signal $V_{u,i} \in \mathcal{V}_{u,i}$ to the transmitter, where the feedback alphabet $\mathcal{V}_{u,i}$ is a design parameter of the scheme. We consider two scenarios for the feedback: *rate-limited* feedback or *perfect* feedback. In the case of rate-limited feedback, the signals from Receiver u have to satisfy:

$$\sum_{i=1}^{n} H(V_{u,i}) \leq nR_{\text{fb}}, \qquad u \in \{1, 2\}, \tag{2}$$

where R_{fb} denotes the symmetric feedback rate. In the case of perfect feedback, we have no constraint on the feedback signals $\{V_{u,i}\}$, and it is thus optimal to choose $\mathcal{V}_{u,i} = \mathbb{R}$ and

$$V_{u,i} = Y_{u,i}, \tag{3}$$

because this way any processing that can be done at the receivers can also be done at the transmitter.

An encoding strategy is comprised of a sequence of encoding functions $\{f_i^{(n)}\}_{i=1}^n$ of the form

$$f_i^{(n)} \colon \mathcal{M} \times \mathcal{V}_{1,1} \times \cdots \times \mathcal{V}_{1,i-1} \times \mathcal{V}_{2,1} \times \cdots \times \mathcal{V}_{2,i-1} \to \mathbb{R} \tag{4}$$

that is used to produce the channel inputs as

$$X_i = f_i^{(n)}(M, V_1^{i-1}, V_2^{i-1}), \qquad i \in \{1, \ldots, n\}, \tag{5}$$

where for each positive integer k we define $V_1^k := (V_{1,1}, \ldots, V_{1,k})$ and $V_2^k := (V_{2,1}, \ldots, V_{2,k})$. We impose an expected average block-power constraint P on the channel input sequence. This means, we only allow for encoding functions that produce channel inputs $X_1, \ldots, X_n$ satisfying

$$\frac{1}{n}\mathbb{E}\Big[\sum_{i=1}^{n} X_i^2\Big] \leq P. \tag{6}$$

Each Receiver $u \in \{1, 2\}$ decodes the message M by means of a decoding function $g_u^{(n)}$ of the form

$$g_u^{(n)} \colon \mathbb{R}^n \to \mathcal{M}. \tag{7}$$

That means, Receiver u produces as its guess

$$\hat{M}_u = g_u^{(n)}(Y_u^n) \tag{8}$$

where $Y_u^n := (Y_{u,1}, \ldots, Y_{u,n})$.

An error occurs in the communication whenever

$$(\hat{M}_1 \neq M) \text{ or } (\hat{M}_2 \neq M), \tag{9}$$

and thus the average probability of error is

$$P_e^{(n)} \triangleq \Pr\Big[\hat{M}_1 \neq M \text{ or } \hat{M}_2 \neq M\Big]. \tag{10}$$

We say that *a rate $R > 0$ is achievable* for the described setup if for every $\epsilon > 0$ there exists a sequence of encoding and decoding functions $\big\{\{f_i^{(n)}\}_{i=1}^n, g_1^{(n)}, g_2^{(n)}\big\}_{n=1}^{\infty}$ as in (4) and (7) and satisfying the power constraint (6) such that for sufficiently large block lengths n the probability of error $P_e^{(n)} < \epsilon$. The supremum of all achievable rates is called the *capacity*. In the case of rate-limited feedback we denote it $C_{\text{rate-fb}}$ and in the case of perfect feedback $C_{\text{perf-fb}}$. It is well known that even with perfect feedback the capacity is the same as without feedback. Thus, irrespective of $R_{\text{fb}} \geq 0$:

$$C_{\text{rate-fb}} = C_{\text{perf-fb}} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2}\right). \tag{11}$$

In this paper we are also interested in the decay rate of the probability of error. We say that the probabilities of error $P_e^{(n)}$ of a sequence of schemes decays to 0 double-exponentially, if

$$\varliminf_{n\to\infty} -\frac{1}{n}\log\log P_e^{(n)} > 0. \tag{12}$$

Throughout the paper $\log(\cdot)$ denotes the natural logarithm.

III. Sub-Optimality of Linear-Feedback Schemes for Perfect Feedback

In this section we restrict attention to perfect feedback and to the class of *linear-feedback schemes with message points*.

A. Linear-Feedback Schemes with Message Points

Definition 1. *We say that a scheme is a linear-feedback scheme with message points (or for short a* linear-feedback scheme*), if the sequence of encoding functions $\{f_i^{(n)}\}_{i=1}^n$ is of the composite form*

$$f_i^{(n)} = L_i^{(n)} \circ \Phi^{(n)} \tag{13}$$

with

$$\Phi^{(n)} \colon M \mapsto \Theta \in \mathbb{R} \tag{14a}$$

$$L_i^{(n)} \colon (\Theta, Y_1^{i-1}, Y_2^{i-1}) \mapsto X_i, \tag{14b}$$

where $\Phi^{(n)}$ is an arbitrary mapping and $L_i^{(n)}$ is a linear *mapping on the respective domains.*

We denote the maximum rate achievable with a sequence of linear-feedback schemes $C_{\text{perf-fb}}^{(\text{Lin})}$.

For comparison, in this section we also discuss the scenario where the transmitter wishes to send two independent private messages M_1 and M_2 of rates R_1 and R_2 to Receivers 1 and 2, respectively. A *linear-feedback scheme* for this setup with private messages consists of a sequence of encoding functions $\{f_{\text{priv},i}^{(n)}\}$ that is of the composite form

$$f_{\text{priv},i}^{(n)} = L_{\text{priv},i}^{(n)} \circ \begin{pmatrix} \Phi_{\text{priv},1}^{(n)} \\ \Phi_{\text{priv},2}^{(n)} \end{pmatrix} \tag{15}$$

with

$$\Phi_{\text{priv},u}^{(n)} \colon M_u \mapsto \Theta_u \in \mathbb{R}, \qquad u \in \{1, 2\}, \tag{16a}$$

$$L_{\text{priv},i}^{(n)} \colon (\Theta_1, \Theta_2, Y_1^{i-1}, Y_2^{i-1}) \mapsto X_i, \tag{16b}$$

where $\Phi_{\text{priv},1}^{(n)}$ and $\Phi_{\text{priv},2}^{(n)}$ are arbitrary mappings and $L_{\text{priv},i}^{(n)}$ is a *linear* mapping on the respective domains. We denote the set of all rate pairs (R_1, R_2) that are achievable with a linear-feedback scheme $\mathcal{C}_{\text{priv, perf-fb}}^{(\text{Lin})}$.

B. Results

Proposition 1. *For a given power constraint P, if a sequence of linear-feedback schemes with message points achieves a common rate $R > 0$, then there exists a sequence of linear-feedback schemes with message points that achieves the symmetric private rates (R, R):*

$$0 \le R \le C_{\text{perf-fb}}^{(\text{Lin})} \qquad \Rightarrow \qquad (R,R) \in \mathcal{C}_{\text{priv, perf-fb}}^{(\text{Lin})}. \tag{17}$$

Proof: A sketch of the proof is given in Appendix A. ■

Theorem 1. *Linear-feedback schemes with message points cannot achieve the capacity of the Gaussian BC with common message:*

$$C_{\text{perf-fb}}^{(\text{Lin})} \le \frac{1}{2}\log\left(1+\frac{\alpha P}{(1-\alpha)P+\sigma_1^2}\right) < C_{\text{perf-fb}} \tag{18}$$

where α is the unique solution in the open interval $(0,1)$ to

$$\alpha\frac{\sigma_1^2\sigma_2^2}{\sigma_1^2+\sigma_2^2} = (1-\alpha)^2 P + (1-\alpha)\sigma_1^2. \tag{19}$$

Proof: Follows from Proposition 1 and by the outer bound on the capacity region for the Gaussian BC with private messages and perfect feedback in [9]. ■

IV. Double-Exponential Decay of Probability of Error with Rate-Limited Feedback

In this section we again allow for general coding schemes and we consider rate-limited feedback.

Theorem 2. *If the feedback rate $R_{\text{fb}} \ge R$, then it is possible to have a double-exponential decay of the probability of error.*

Proof: In Section IV-A we present a bursty-feedback scheme achieving the desired performance; it is based on the scheme in [10], see also [11]. Its analysis is omitted. ■

A. Bursty-feedback scheme

Fix a positive rate R and assume that

$$R_{\text{fb}} \ge R. \tag{20}$$

Also, fix a large blocklength n and $\delta > 0$ such that

$$R < C(1-\delta). \tag{21}$$

Choose a small $\epsilon > 0$ and define $n_2 = \epsilon n$ and $n_1 = n - n_2 - 1$. Notice that if n has been chosen sufficiently large,

$$\frac{n}{n_1} < 1+\delta. \tag{22}$$

We choose a no-feedback code $\mathcal{C}_1$ for the BC with common message. The parameters of the code are: blocklength n_1, rate $\frac{n}{n_1}R$, expected average block-power constraint P, and probability of error

$$P_{e,1}^{(n)} \le e^{-n(\zeta - o(1))} \tag{23}$$

for some $\zeta > 0$ and some function $o(1)$ that tends to 0 as $n \to \infty$. Notice that such a code exists because, by (21) and (22), the rate of the code $\frac{n}{n_1}R < C(1-\delta^2)$ and the error exponent of the BC with common message without feedback is positive for all rates below capacity.[1]

Now, choose a second code $\mathcal{C}_2$ for the BC with common message and no feedback. The parameters of code $\mathcal{C}_2$ are: blocklength n_2, rate R/ϵ, expected average block-power constraint P/γ, where

$$\gamma \triangleq P_{e,1}^{(n)}, \tag{24}$$

and probability of error

$$P_{e,2}^{(n)} \le \exp(-\exp(n(\zeta - o(1)))). \tag{25}$$

That such a code exists can be proved using arguments from [12].

Transmission takes place in 2 phases.

1) First phase with channel uses $i = 1, \dots, n_1$: During the first n_1 channel uses, the transmitter sends the codeword in $\mathcal{C}_1$ corresponding to message M.

After observing the channel outputs $Y_u^{n_1}$, Receiver $u \in \{1,2\}$ makes a tentative decision $\hat{M}_{u,1}$ about M. It then sends its tentative decision $\hat{M}_{u,1}$ to the transmitter over the feedback channel:

$$V_{u,n_1} = \hat{M}_{u,1}. \tag{26}$$

All other feedback signals from Receiver u are deterministically 0 and therefore, by (20), the scheme satisfies the feedback rate constraint (2).

2) Second phase with channel uses $i = n_1+1, \dots, n$: In channel use n_1+1 the transmitter sends a signal to indicate whether both receivers' tentative decisions were correct. Specifically,

$$X_{n_1+1} = \begin{cases} \sqrt{P/\gamma} & \text{if } \hat{M}_{1,1} \ne M \text{ or } \hat{M}_{2,1} \ne M \\ 0 & \text{if } \hat{M}_{1,1} = \hat{M}_{2,1} = M. \end{cases} \tag{27}$$

Moreover, if one of the two tentative decisions was wrong,

$$(\hat{M}_{1,1} \ne M) \text{ or } (\hat{M}_{2,1} \ne M),$$

then during channel uses $i = n_1+2, \dots, n$ the transmitter sends the codeword from $\mathcal{C}_2$ that corresponds to M.

Each Receiver u first detects the signal X_{n_1+1}. Define

$$\Gamma \triangleq \frac{\sqrt{P/\gamma}}{2}. \tag{28}$$

If $Y_{u,n_1+1} < \Gamma$, Receiver u decides that its tentative decision was correct, and produces as its guess $\hat{M}_u = \hat{M}_{u,1}$. If instead $Y_{u,n_1+1} \ge \Gamma$, it decides that its tentative decision $\hat{M}_{u,1}$ was wrong and discards it. It then produces a new guess $\hat{M}_{u,2}$ by decoding the code $\mathcal{C}_2$ applied in the second phase solely based on the outputs $Y_{u,n_1+2}, \dots, Y_{u,n}$, and produces as its final guess $\hat{M}_u = \hat{M}_{u,2}$.

[1] The positiveness of the error exponent for the Gaussian BC with common message and without feedback follows from the fact that without feedback the probability of error for the Gaussian BC with common messages is at most twice the probability of error to the weaker receiver.

APPENDIX A
PROOF OF PROPOSITION 1

Let δ be a small positive number. Fix a sequence of linear-feedback schemes $\left\{\left(\Phi^{(n)}, \{L_i^{(n)}\}_{i=1}^n, g_1^{(n)}, g_2^{(n)}\right)\right\}_{n=1}^{\infty}$ that send a common message to the two receivers and that satisfy the power constraint (6) with P replaced by $(P-\delta)$. Based on this sequence, we construct a sequence of linear-feedback schemes $\left\{\left(\Phi_{\text{priv},1}^{(n)}, \Phi_{\text{priv},2}^{(n)}, \{L_{\text{priv},i}^{(n)}\}_{i=1}^n, g_{\text{priv},1}^{(n)}, g_{\text{priv},2}^{(n)}\right)\right\}_{n=1}^{\infty}$ that send two independent private messages at rates

$$R_1 \geq R \qquad \text{and} \qquad R_2 \geq R, \tag{29}$$

and that for large blocklengths n satisfy the power constraint (6). Since $\delta > 0$ can be chosen arbitrarily small, and by continuity considerations, this establishes the proposition.

In the next subsection A-1 we state two lemmas on the sequence of linear-feedback schemes for common message. The construction of the desired sequence of linear-feedback schemes for private messages is explained in Subsection A-2.

1) About the Linear-Feedback Schemes with Common Message: We denote the message point, the channel inputs, and the channel outputs corresponding to the blocklength n scheme $(\Phi^{(n)}, \{L_i^{(n)}\}_{i=1}^n, g_1^{(n)}, g_2^{(n)})$ by $\Theta^{(n)}$, $X_1^{(n)}, \ldots, X_n^{(n)}$, $Y_{1,1}^{(n)}, \ldots, Y_{1,n}^{(n)}$, $Y_{2,1}^{(n)}, \ldots, Y_{2,n}^{(n)}$. By the definition of a linear-feedback coding scheme in (16), and defining

$$\mathbf{X}^{(n)} \triangleq \left(X_1^{(n)}, \ldots, X_n^{(n)}\right)^{\mathsf{T}}, \tag{30}$$

$$\mathbf{Y}_u^{(n)} \triangleq \left(Y_{u,1}^{(n)}, \ldots, Y_{u,n}^{(n)}\right)^{\mathsf{T}}, \qquad u \in \{1,2\}, \tag{31}$$

$$\mathbf{Z}_u \triangleq \left(Z_{u,1}, \ldots, Z_{u,n}\right)^{\mathsf{T}}, \qquad u \in \{1,2\}, \tag{32}$$

we can write

$$\mathbf{X}^{(n)} = \mathsf{A}^{(n)}\mathbf{Z}_1 + \mathsf{B}^{(n)}\mathbf{Z}_2 + \mathbf{d}^{(n)}\Theta^{(n)} \tag{33a}$$

$$\mathbf{Y}_1^{(n)} = (\mathsf{I} + \mathsf{A}^{(n)})\mathbf{Z}_1 + \mathsf{B}^{(n)}\mathbf{Z}_2 + \mathbf{d}^{(n)}\Theta^{(n)} \tag{33b}$$

$$\mathbf{Y}_2^{(n)} = \mathsf{A}^{(n)}\mathbf{Z}_1 + (\mathsf{I} + \mathsf{B}^{(n)})\mathbf{Z}_2 + \mathbf{d}^{(n)}\Theta^{(n)}. \tag{33c}$$

for some strictly-lower triangular n-by-n matrices $\mathsf{A}^{(n)}$ and $\mathsf{B}^{(n)}$ and an n-dimensional column-vector $\mathbf{d}^{(n)}$.[2] Notice that, since the schemes satisfy the average block-power constraint in (6) for power $P-\delta$,

$$\mathrm{tr}(\mathsf{A}\mathsf{A}^{\mathsf{T}})\sigma_1^2 + \mathrm{tr}(\mathsf{B}\mathsf{B}^{\mathsf{T}})\sigma_2^2 + \|\mathbf{d}^{(n)}\|^2 \mathsf{Var}\left(\Theta^{(n)}\right) \leq n(P-\delta), \tag{34}$$

where, for ease of notation, we dropped the superscript (n) for the matrices $\mathsf{A}^{(n)}$ and $\mathsf{B}^{(n)}$.

Lemma 1. *For each positive integer n there exist two n-dimensional row-vectors $\mathbf{v}_1^{(n)}$ and $\mathbf{v}_2^{(n)}$ of unit norms*

$$\|\mathbf{v}_1^{(n)}\|^2 = \|\mathbf{v}_2^{(n)}\|^2 = 1 \tag{35}$$

such that

$$R \leq \varliminf_{n\to\infty} -\frac{1}{2n}\log\left(\sigma_1^2\|\mathbf{v}_1^{(n)}(\mathsf{I}+\mathsf{A}^{(n)})\|^2 + \sigma_2^2\|\mathbf{v}_1^{(n)}\mathsf{B}^{(n)}\|^2\right) =: \Gamma_1 \tag{36}$$

and

$$R \leq \varliminf_{n\to\infty} -\frac{1}{2n}\log\left(\sigma_1^2\|\mathbf{v}_2^{(n)}\mathsf{A}^{(n)}\|^2 + \sigma_2^2\|\mathbf{v}_2^{(n)}(\mathsf{I}+\mathsf{B}^{(n)})\|^2\right) =: \Gamma_2. \tag{37}$$

Proof: Omitted. ∎

Lemma 2. *Let $\{\mathbf{v}_1^{(n)}\}$ and $\{\mathbf{v}_2^{(n)}\}$ be as in Lemma 1. If the limits Γ_1, Γ_2 in (36) and (37) are both positive, then for each positive integer n there exists a pair of indices $(j^{(n)}, k^{(n)})$ satisfying*

$$\lim_{n\to\infty} \frac{1}{n}\mathsf{E}\left[\left(X_{j^{(n)}}^{(n)}\right)^2\right] = 0 \tag{38a}$$

$$\lim_{n\to\infty} \frac{1}{n}\mathsf{E}\left[\left(X_{k^{(n)}}^{(n)}\right)^2\right] = 0 \tag{38b}$$

$$\lim_{n\to\infty} \frac{1}{2n}\log(|v_{1,j^{(n)}}^{(n)}|) > 0 \tag{38c}$$

$$\lim_{n\to\infty} \frac{1}{2n}\log(|v_{2,k^{(n)}}^{(n)}|) > 0, \tag{38d}$$

where $v_{1,j^{(n)}}^{(n)}$ denotes the $j^{(n)}$-th component of $\mathbf{v}_1^{(n)}$ and $v_{2,k^{(n)}}^{(n)}$ denotes the $k^{(n)}$-th component of $\mathbf{v}_2^{(n)}$.

Proof: Omitted. ∎

2) A Linear-Feedback Scheme for Private Messages: We are now ready to describe our sequence of linear-feedback schemes for private messages $\left\{\left(\phi_{\text{priv},1}^{(n)}, \phi_{\text{priv},2}^{(n)}, \{L_{\text{priv},i}^{(n)}\}_{i=1}^n, g_{\text{priv},1}^{(n)}, g_{\text{priv},2}^{(n)}\right)\right\}_{n=1}^{\infty}$. We denote the channel inputs produced by the blocklength-n scheme by $\{\bar{X}_i^{(n)}\}$ and the corresponding channel outputs by

$$\bar{Y}_{u,i}^{(n)} = \bar{X}_i^{(n)} + Z_{u,i}, \qquad u \in \{1,2\}. \tag{39}$$

To facilitate the description, we assume that the transmission starts at time $i = -1$ (instead of $i = 1$).

We describe our scheme for blocklength-$(n+4)$, which takes place in time-slots $i = -1, 0, \ldots, n+2$. As we shall see, the blocklength-$(n+4)$ encoding functions $\left\{L_{\text{priv},i}^{(n+4)}\right\}_{i=1}^{n+4}$ are constructed from the blocklength-n parameters $\mathsf{A}^{(n)}$ and $\mathsf{B}^{(n)}$ defined in the previous section.

Let $j^{(n)}$ and $k^{(n)}$ be two indices that satisfy the conditions in Lemma 2 and define

$$\bar{Z}_{1,i}^{(n+4)} := \begin{cases} Z_{1,i}, & \text{if } 1 \leq i \leq j^{(n)}, \\ Z_{1,i+1}, & \text{if } j^{(n)}+1 \leq i \leq k^{(n)}, \\ Z_{1,i+2}, & \text{if } k^{(n)}+1 \leq i \leq n \end{cases} \tag{40}$$

and

$$\bar{Z}_{2,i}^{(n+4)} := \begin{cases} Z_{2,i}, & \text{if } 1 \leq i \leq j^{(n)}-1, \\ Z_{2,i+1}, & \text{if } j^{(n)} \leq i \leq k^{(n)}-1, \\ Z_{2,i+2} & \text{if } k^{(n)} \leq i \leq n. \end{cases} \tag{41}$$

We assume that $j^{(n)} \leq k^{(n)}$; otherwise we exchange the roles of the subscripts 1 and 2 and in our scheme we reverse the roles of the two receivers.

[2] We do not use a superscript (n) for the noise samples because their law does not depend on the block length n.

Encoding is as follows. The transmitter first computes the two message points $\bar{\Theta}_1^{(n+4)}$ and $\bar{\Theta}_2^{(n+4)}$ as in [9]:

$$\bar{\Theta}_u^{(n+4)} := 1/2 - \frac{M_u - 1}{\lfloor 2^{(n+4)R_u} \rfloor}, \qquad u \in \{1, 2\}. \tag{42}$$

In the first two channel uses it then transmits:

$$\bar{X}_{-1}^{(n+4)} = \bar{\Theta}_1^{(n+4)} \sqrt{\frac{P}{\mathrm{Var}\big(\bar{\Theta}_1^{(n+4)}\big)}} \tag{43}$$

$$\bar{X}_0^{(n+4)} = \bar{\Theta}_2^{(n+4)} \sqrt{\frac{P}{\mathrm{Var}\big(\bar{\Theta}_2^{(n+4)}\big)}}. \tag{44}$$

The remaining inputs $\bar{X}_1^{(n+4)}, \ldots, \bar{X}_{n+2}^{(n+4)}$ are constructed from the inputs $X_1^{(n)}, \ldots, X_n^{(n)}$ in the scheme with common message.

- At times $1, \ldots, j^{(n)} - 1$ the transmitter sends $X_1^{(n)}, \ldots, X_{j^{(n)}-1}$ but without the component from the message point.
- At time $j^{(n)}$ it sends $X_{j^{(n)}}^{(n)}$ but with the component from the message point replaced by $Z_{1,-1}/\sqrt{\sigma_1^2}$.
- At times $j^{(n)} + 1, \ldots, k^{(n)}$ it sends the inputs $X_{j^{(n)}}^{(n)}, \ldots, X_{k^{(n)}}^{(n)}$ but again without the message point.
- At time $k^{(n)} + 2$ it sends $X_{k^{(n)}}^{(n)}$ but with the component from the message point replaced by $Z_{2,0}/\sqrt{\sigma_2^2}$.
- Finally, at times $k^{(n)} + 3, \ldots, n + 2$ it sends the inputs $X_{k^{(n)}+1}^{(n)}, \ldots X_n^{(n)}$.

Defining

$$\mathbf{I}_1^{(n+4)} := \Big(\bar{Y}_{1,1}^{(n+4)}, \ldots, \bar{Y}_{1,j^{(n)}}^{(n+4)},\ \bar{Y}_{1,j^{(n)}+2}^{(n+4)}, \ldots, \bar{Y}_{1,k^{(n)}+1}^{(n+4)},\ \bar{Y}_{1,k^{(n)}+3}^{(n+4)}, \ldots, \bar{Y}_{1,n+2}^{(n+4)}\Big)^{\mathsf{T}} \tag{45}$$

and

$$\mathbf{I}_2^{(n+4)} := \Big(\bar{Y}_{2,1}^{(n+4)}, \ldots, \bar{Y}_{2,j^{(n)}-1}^{(n+4)},\ \bar{Y}_{2,j^{(n)}+1}^{(n+4)}, \ldots, \bar{Y}_{2,k^{(n)}}^{(n+4)},\ \bar{Y}_{2,k^{(n)}+2}^{(n+4)}, \ldots, \bar{Y}_{2,n+2}^{(n+4)}\Big)^{\mathsf{T}}, \tag{46}$$

the described encoding procedure yields:

$$\mathbf{I}_1^{(n+4)} = (\mathsf{I} + \mathsf{A}^{(n)})\bar{\mathbf{Z}}_1^{(n+4)} + \mathsf{B}^{(n)}\bar{\mathbf{Z}}_2^{(n+4)} + \mathbf{e}_{j^{(n)}} \frac{Z_{1,-1}}{\sqrt{\sigma_1^2}} \tag{47a}$$

and

$$\mathbf{I}_2^{(n+4)} = \mathsf{A}^{(n)}\bar{\mathbf{Z}}_1^{(n+4)} + (\mathsf{I} + \mathsf{B}^{(n)})\bar{\mathbf{Z}}_2^{(n+4)} + \mathbf{e}_{k^{(n)}} \frac{Z_{2,0}}{\sqrt{\sigma_2^2}}, \tag{47b}$$

where

$$\bar{\mathbf{Z}}_u^{(n+4)} := (\bar{Z}_{u,1}^{(n+4)}, \ldots, \bar{Z}_{u,n}^{(n+4)})^{\mathsf{T}}, \qquad u \in \{1, 2\} \tag{48}$$

and where, for $i \in \{1, \ldots, n\}$, $\mathbf{e}_i$ denotes the n-dimensional vector with i-th entry 1 and all other entries equal to 0.

Receiver 1 completely ignores its channel outputs $\bar{Y}_{1,0}^{(n+4)}, \bar{Y}_{1,j^{(n)}+1}^{(n+4)}, \bar{Y}_{1,k^{(n)}+2}^{(n+4)}$ and bases its decision solely on the vector $\mathbf{I}_1^{(n+4)}$ and on $\bar{Y}_{1,-1}^{(n+4)}$. Similarly, Receiver 2 bases its decision on $\mathbf{I}_2^{(n+4)}$ and on $\bar{Y}_{2,0}^{(n+4)}$. The decisions are taken as in the Ozarow-Leung scheme [9]. Specifically, Receiver 1 first produces the LMMSE estimate $\hat{Z}_{1,-1}^{(n+4)}$ of the noise $Z_{1,-1}$ based on $\mathbf{I}_1^{(n+4)}$ and guesses the message point $\bar{\Theta}_1^{(n+4)}$ as

$$\hat{\Theta}_1^{(n+4)} = \sqrt{\frac{\mathrm{Var}\big(\bar{\Theta}_1^{(n+4)}\big)}{P}} \Big(\bar{Y}_{1,-1}^{(n+4)} - \hat{Z}_{1,-1}^{(n+4)}\Big). \tag{49}$$

It finally decodes its desired Message M_1 using nearest-neighbor decoding from $\hat{\Theta}_1^{(n+4)}$. Receiver 2 decodes its Message M_2 in a similar way.

By (47) and because the indices $j^{(n)}$ and $k^{(n)}$ satisfy the conditions (38c) and (38d) in Lemma 2, it can be shown (details omitted) that the probability of error of the described scheme tends to 0 as $n \to \infty$, whenever

$$R_1 \le \Gamma_1 \quad \text{and} \quad R_2 \le \Gamma_2. \tag{50}$$

Also notice that the way we constructed the channel inputs,

$$\begin{aligned}
&\sum_{i=-1}^{n+2} \mathsf{E}\Big[\big|\bar{X}_i^{(n+4)}\big|^2\Big] \\
&\le 2P + \sum_{i=1}^{n} \mathsf{E}\Big[\big|X_i^{(n)}\big|^2\Big] + \mathsf{E}\Big[\big|\bar{X}_{j^{(n)}}^{(n+4)}\big|^2\Big] + \mathsf{E}\Big[\big|\bar{X}_{k^{(n)}}^{(n+4)}\big|^2\Big] \\
&\le 2P + n(P - \delta) + \mathsf{E}\Big[\big|X_{j^{(n)}}^{(n)}\big|^2\Big] + \mathsf{E}\Big[\big|X_{k^{(n)}}^{(n)}\big|^2\Big] + 2.
\end{aligned} \tag{51}$$

Thus, since $j^{(n)}$ and $k^{(n)}$ satisfy (38a) and (38b) in Lemma 2, the inputs $\{\bar{X}_i^{(n+4)}\}_{i=-1}^{n+2}$ are expected average block-power constrained to P for all sufficiently large n.

By Lemma 1 and rate constraints (50), we therefore conclude that the symmetric private rate pair $R_1 = R$ and $R_2 = R$ is achievable with a sequence of linear feedback schemes.

REFERENCES

[1] J. P. M. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback-I: no bandwidth constraint," *IEEE Trans. on Inf. Theory*, vol. 12, no. 2, pp. 183–189, Apr. 1966.

[2] Y.-H. Kim, "Feedback capacity of stationary Gaussian channels," *IEEE Trans. on Inf. Theory*, vol. 56, no. 1, pp. 57–85, January 2010.

[3] L. H. Ozarow, "The capacity of the white Gaussian multiple access channel with feedback," *IEEE Trans. on Inf. Theory*, vol. 30, no. 4, pp. 623–629, 1984.

[4] G. Kramer, "Feedback strategies for white Gaussian interference networks," *IEEE Trans. on Inf. Theory*, vol. 48, no. 6, pp. 1423–1438, 2002.

[5] E. Ardestanizadeh, M. Wigger, Y.-H. Kim, and T. Javidi, "Linear sum-capacity for Gaussian multiple access channels with feedback, *IEEE Transactions on Inf. Theory*, vol. 58, no. 1, pp. 224–236, Jan. 2012.

[6] E. Ardestanizadeh, P. Minero and M. Franceschetti, "LQG control approach to Gaussian broadcast channels with feedback," *IEEE Trans. on Inf. Theory*, vol. 58, no. 8, pp. 5267–5278, 2012.

[7] M. Gastpar, A. Lapidoth, Y. Steinberg, and M. Wigger, "Feedback can double the prelog of some memoryless Gaussian networks," submitted to *IEEE Trans. on Inf. Theory*. Online: http://arxiv.org/abs/1003.6082.

[8] M. Gastpar, A. Lapidoth, Y. Steinberg, and M. Wigger, "New achievable rates for the Gaussian broadcast channel with feedback," in *Proc. of 8th ISWCS*, 2011, Aachen, Germany, Nov. 6-9, 2011, pp. 579–583.

[9] L. H. Ozarow, and S. K. Leung-Yan-Cheong, "An achievable region and outer bound for the Gaussian broadcast channel with feedback," *IEEE Trans. on Inf. Theory*, vol. 30, no. 4, pp. 667–671, July 1984.

[10] R. Mirghaderi, A. Goldsmith, T. Weissman, "Achievable error exponents in the Gaussian channel with rate-limited feedback", submitted to *IEEE Trans. on Inf. Theory*. http://arxiv.org/abs/1007.1986.

[11] A. Sahai, S. C. Draper, and M. Gastpar, "Boosting reliability over AWGN networks with average power constraints and noiseless feedback," in *Proc. of ISIT 2005*, Adelaide, Australia, Sep. 2005.

[12] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell Systems Tech. Journal*, vol. 38, no. 3, pp. 611–656, 1959.