Communication With Disturbance Constraints

Bernd Bandemer, *Member, IEEE* and Abbas El Gamal, *Fellow, IEEE*

***Abstract*— Motivated by the broadcast view of the interference channel, the new problem of communication with disturbance constraints is formulated. The rate–disturbance region is established for the single constraint case and the optimal encoding scheme turns out to be the same as the Han–Kobayashi scheme for the two user-pair interference channel. This result is extended to the Gaussian vector (multiple-input and multiple-output) case. For the case of communication with two disturbance constraints, inner and outer bounds on the rate–disturbance region for a deterministic model are established. The inner bound is achieved by an encoding scheme that involves rate splitting, Marton coding, and superposition coding, and is shown to be optimal in several nontrivial cases. This encoding scheme can be readily applied to discrete memoryless interference channels and motivates a natural extension of the Han–Kobayashi scheme to more than two user pairs.**

***Index Terms*— Capacity with constraints, interference channel, broadcast channel, wiretap channel, network information theory.**

I. Introduction

ALICE wishes to communicate a message to Bob while causing the least disturbance to nearby Dick, Diane, and Diego, who are not interested in the communication from Alice. Assume a discrete memoryless broadcast channel $p(y, z_1, \ldots, z_K|x)$ between Alice X, Bob Y, and their preoccupied friends $Z_1, \ldots, Z_K$ as depicted in Fig. 1. We measure the disturbance at side receiver Z_j by the amount of *undesired* information rate $(1/n)\, I(X^n; Z_j^n)$ originating from the sender X, and require this rate not to exceed $R_{\mathrm{d},j}$ in the limit. The problem is to determine the optimal trade-off between the message communication rate R and the disturbance rates $R_{\mathrm{d},j}$.

This communication with disturbance constraints problem is motivated by the broadcast side of the interference channel in which each sender wishes to communicate a message only to one of the receivers while causing the least disturbance to the other receivers. However, in this paper, which is an extended version of [1], we focus on studying the problem of communication with disturbance constraints itself.

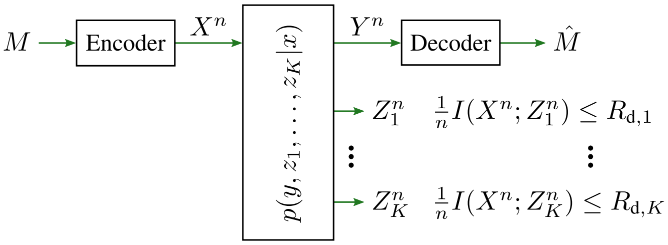

M
Encoder
X^n
$p(y, z_1, \ldots, z_K|x)$
Y^n
Decoder
$\hat{M}$
Z_1^n $\frac{1}{n}I(X^n; Z_1^n) \le R_{\mathrm{d},1}$
Z_K^n $\frac{1}{n}I(X^n; Z_K^n) \le R_{\mathrm{d},K}$

Fig. 1. Communication system with disturbance constraints.

The application of the coding scheme developed in this paper to deterministic interference channels with more than two user pairs is discussed in [2].

For a single disturbance constraint, we show that the optimal encoding scheme is rate splitting and superposition coding, which is the same as the Han–Kobayashi scheme for the two user-pair interference channel [3], [4]. This motivates us to study communication with more than one disturbance constraint with the hope of finding good coding schemes for interference channels with more than two user pairs. To this end, we establish inner and outer bounds on the rate–disturbance region for the deterministic channel model with two disturbance constraints that are tight in some nontrivial special cases. In the following section we provide needed definitions and present an extended summary of our results. The proofs are presented in subsequent sections, with some parts deferred to the Appendix.

II. Definitions and Main Results

Consider the discrete memoryless communication system with K disturbance constraints (henceforth referred to as DMC-K-DC) depicted in Fig. 1. The channel consists of $K+2$ finite alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}_j$, $j \in [1:K]$, and a collection of conditional pmfs $p(y, z_1, \ldots, z_K|x)$. A $(2^{nR}, n)$ code for the DMC-K-DC consists of the message set $[1:2^{nR}]$, an encoding function $x^n : [1 : 2^{nR}] \to \mathcal{X}^n$, and a decoding function $\hat{m} : \mathcal{Y}^n \to [1 : 2^{nR}]$. We assume that the message M is uniformly distributed over $[1:2^{nR}]$. A rate–disturbance tuple $(R, R_{\mathrm{d},1}, \ldots, R_{\mathrm{d},K}) \in \mathbb{R}_+^{K+1}$ is achievable for the DMC-K-DC if there exists a sequence of $(2^{nR}, n)$ codes such that

$$\begin{aligned}\lim_{n\to\infty} \mathrm{P}\{\hat{M} \neq M\} &= 0,\\ \limsup_{n\to\infty}\, (1/n)\, I(X^n; Z_j^n) &\le R_{\mathrm{d},j}, \quad j \in [1:K]. \qquad (1)\end{aligned}$$

The *rate–disturbance region* $\mathscr{R}$ of the DMC-K-DC is the closure of the set of all achievable tuples $(R, R_{\mathrm{d},1}, \ldots, R_{\mathrm{d},K})$.

Remark 1: Like the message rate R, the disturbance rates $R_{\mathrm{d},j}$, for $j \in [1:K]$, are measured in units of bits per channel use. (We use logarithms of base 2 throughout.)

Manuscript received November 7, 2011; revised October 16, 2012; accepted September 3, 2013. Date of publication May 9, 2014, date of current version July 10, 2014. This work was supported by the Defense Advanced Research Projects Agency–Information Theory of Mobile Ad-Hoc Networks. B. Bandemer was supported by an Eric and Illeana Benhamou Stanford Graduate Fellowship. This paper was presented at the 2011 IEEE International Symposium on Information Theory.

B. Bandemer was with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305 USA. He is now with Bosch Research and Technology Center, Palo Alto, CA 94304 USA (e-mail: bandemer@alumni.stanford.edu).

A. El Gamal is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305 USA (e-mail: abbas@ee.stanford.edu).

Communicated by Y. Steinberg, Associate Editor at Large.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2014.2322852

Remark 2: The measure of disturbance $(1/n)\, I(X^n; Z_j^n)$ can be expanded as $(1/n)\, H(Z_j^n) - (1/n)\, H(Z_j^n \,|\, X^n)$. The first term is the entropy rate of the received signal Z_j and is caused by both the transmission itself and by noise inherent to the channel. Subtracting the second term separates out the noise part. (For channels with additive white noise, e.g., the Gaussian case, the second term is exactly the differential entropy of each noise sample.)

Remark 3: Our results remain essentially the same if disturbance is measured by $(1/n)\, H(Z_j^n)$ instead of $(1/n)\, I(X^n; Z_j^n)$, in the sense that the optimal coding schemes and converse proof techniques are unchanged. The rate–disturbance region, however, would need to be appropriately transformed. If the channel is deterministic, the two disturbance measures coincide.

Remark 4: The disturbance constraint in (1) is reminiscent of the information leakage rate constraint for the wiretap channel [5], [6], namely

$$\limsup_{n\to\infty}\ (1/n)\, I(M; Z_j^n) \le R_{\text{leak},j}, \quad j \in [1\!:\!K]. \tag{2}$$

Note that by the data processing inequality, $I(M; Z_j^n) \le I(X^n; Z_j^n)$, hence the disturbance constraint is more restrictive than the leakage constraint. Consequently, the rate–disturbance region of a channel $p(y, z_1, \ldots, z_K|x)$ is contained in its rate–leakage region, if the right-hand side values of the constraints remain constant, $R_{\text{leak},j} = R_{\text{d},j}$ for $j \in [1:K]$. However, replacing the leakage rate constraint (2) with the disturbance rate constraint (1) significantly changes the optimal coding scheme. In the wiretap channel, the key component of the optimal encoding scheme is randomized encoding, which helps control the leakage rate $(1/n)\, I(M; Z_j^n)$. Such randomization reduces the achievable transmission rate for a given disturbance constraint, hence is not desirable in our setting.

The rate–disturbance region is not known in general. In this paper we establish the following results.

A. Rate–Disturbance Region for a Single Disturbance Constraint

Consider the case with a single disturbance constraint, i.e., $K = 1$, and relabel Z_1 as Z and $R_{\text{d},1}$ as R_d. We fully characterize the rate–disturbance region for this case.

Theorem 1: The rate–disturbance region $\mathscr{R}$ of the DMC-1-DC is the set of rate pairs (R, R_d) such that

$$\begin{aligned} R &\le I(X;Y), \\ R_\text{d} &\ge I(X; Z \,|\, U), \\ R - R_\text{d} &\le I(X; Y \,|\, U) - I(X; Z \,|\, U), \end{aligned}$$

for some pmf $p(u, x)$ with $|\mathcal{U}| \le |\mathcal{X}| + 1$.

Let $\mathscr{R}(U, X)$ be the rate region defined by the rate constraints in the theorem for a fixed joint pmf $(U, X) \sim p(u, x)$. This rate region is illustrated in Fig. 2. The rate–disturbance region is simply the union of these regions over all $p(u, x)$ and is convex without the need for a time-sharing random variable.

The proof of Theorem 1 is given in Subsections III-A and III-B. Achievability is established using rate splitting and superposition coding. Receiver Y decodes the satellite codeword while receiver Z distinguishes only the cloud center. Note that this encoding scheme is identical to each transmitter's operation in the Han–Kobayashi scheme for the two user-pair interference channel [3], [4].

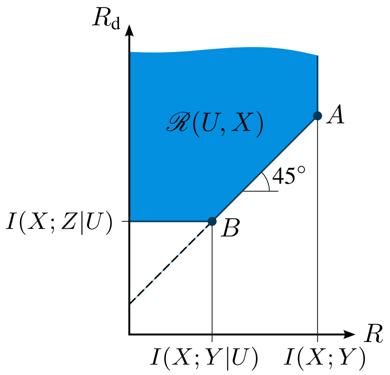


Fig. 2. Example of $\mathscr{R}(U, X)$, the constituent region of $\mathscr{R}$.

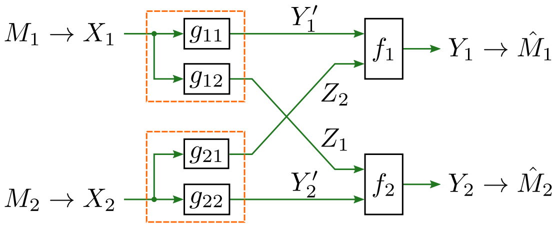


Fig. 3. Injective deterministic interference channel with two user pairs.

We now consider three interesting special cases.

1) Deterministic Channel: Assume that Y and Z are deterministic functions of X. We show that the rate–disturbance region in Theorem 1 reduces to the following.

Corollary 1: The rate–disturbance region for the deterministic channel with one disturbance constraint is the set of rate pairs (R, R_d) such that

$$\begin{aligned} R &\le H(Y), \\ R - R_\text{d} &\le H(Y \,|\, Z), \end{aligned}$$

for some pmf $p(x)$.

Clearly, this region is convex. Alternatively, the region can be written as the set of rate pairs (R, R_d) such that

$$\begin{aligned} R &\le H(Y \,|\, Q), \\ R_\text{d} &\ge I(Y; Z \,|\, Q), \end{aligned}$$

for some joint pmf $p(q, x)$ with $|\mathcal{Q}| \le 2$. Corollary 1 and the alternative description of the region are established by substituting $U = Z$ in the region of Theorem 1 and simplifying the resulting region as detailed in Subsection III-C.

Remark 5: Consider the injective deterministic interference channel with two user pairs depicted in Fig. 3. Here, g_{ij} is a function that models the link from transmitter i to receiver j, for $i, j \in \{1, 2\}$. The combining functions f_j are assumed to be injective in each argument. This setting is a special case of the channel investigated in [7]. This can be seen by merging g_{11} and f_1 of Fig. 3 into a function f_1' that maps (X_1, Z_2) to Y_1. Likewise, define the function f_2' as the merger of g_{22} and f_2. The modified combining functions f_1' and f_2' are

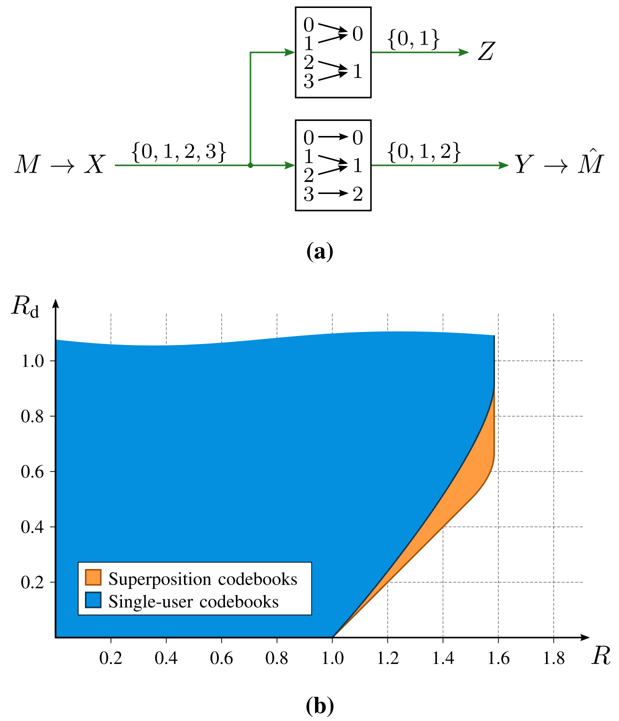


Fig. 4. Deterministic example with one disturbance constraint. (a) Channel block diagram. (b) Rate–disturbance region.

injective in Z_2 and Z_1, respectively, and therefore satisfy the assumptions in [7]. It follows that the Han–Kobayashi scheme where the transmitters use superposition codebooks generated according to $p(z_1)\, p(x_1|z_1)$ and $p(z_2)\, p(x_2|z_2)$ achieves the capacity region of the channel in Fig. 3.

On the other hand, Corollary 1 shows that the *same* encoding scheme achieves the disturbance-constrained capacity for the channels $X_1 \to (Y_1', Z_1)$ and $X_2 \to (Y_2', Z_2)$, shown as dashed boxes in Fig. 3. Here, Y_1' and Y_2' are the desired receivers, and Z_1 and Z_2 are the side receivers associated with disturbance constraints. Note that decodability of the desired messages at receivers Y_1 and Y_2 in the interference channel certainly implies decodability at Y_1' and Y_2' in the channels with disturbance constraint, respectively.

Example 1: Consider the deterministic channel depicted in Fig. 4(a) and its rate–disturbance region in Fig. 4(b). Note that rates $R \leq 1$ can be achieved with zero disturbance rate by restricting the transmission to input symbols $\{0, 1\}$ (or $\{2, 3\}$), which map to different symbols at Y, but are indistinguishable at Z. On the other hand, for sufficiently large R_d, the disturbance constraint becomes inactive and R is bounded only by the unconstrained capacity $\log(3)$. In addition to the optimal region achieved by superposition coding, the figure also shows the strictly suboptimal region achieved by simple non-layered random codes (i.e., single-user codebooks).

2) Gaussian Channel: Consider the problem of communication with one disturbance constraint for the Gaussian channel

$$Y = X + W_1,$$
$$Z = X + W_2,$$

where the noise is $W_1 \sim \mathcal{N}(0, 1)$ and $W_2 \sim \mathcal{N}(0, N)$. Assume an average power constraint P on the transmitted signal X.

The case $N \leq 1$ is quite straightforward. Since Y is a degraded version of Z, the disturbance rate is the same as the data rate R, and the rate-disturbance region is the set of rate pairs (R, R_d) such that

$$R \leq \mathrm{C}(P),$$
$$R_\mathrm{d} \geq R,$$

where $\mathrm{C}(x) = (1/2)\log(1 + x)$ for $x \geq 0$.

If $N > 1$, Z is a degraded version of Y, and the rate–disturbance region reduces to the following.

Corollary 2: The rate–disturbance region of the Gaussian channel with parameters $P > 0$ and $N > 1$ is the set of rate pairs (R, R_d) such that

$$R \leq \mathrm{C}(\alpha P),$$
$$R_\mathrm{d} \geq \mathrm{C}(\alpha P/N),$$

for some $\alpha \in [0, 1]$.

Achievability is proved by using Gaussian codes with power αP. The converse follows by defining $\alpha^\star \in [0, 1]$ such that $R = \mathrm{C}(\alpha^\star P)$ and applying the vector entropy power inequality to $Z^n = Y^n + \tilde{W}_2^n$, where $\tilde{W}_2 \sim \mathcal{N}(0, N - 1)$ is the excess noise. The details are given in Subsection III-D. Note that this is a degenerate form of the Han–Kobayashi scheme because the constraint from the multiple access side of the interference channel is not taken into consideration.

3) Vector Gaussian Channel: Now consider the vector Gaussian channel with one disturbance constraint

$$Y = X + W_1,$$
$$Z = X + W_2,$$

where $X \in \mathbb{R}^n$ and the noise is $W_1 \sim \mathcal{N}(0, K_1)$ and $W_2 \sim \mathcal{N}(0, K_2)$ for some positive semidefinite covariance matrices $K_1, K_2 \in \mathbb{R}^{n \times n}$. Assume an average transmit power constraint $\mathrm{tr}(K_x) \leq P$, where $K_x = \mathbb{E}(XX^\mathrm{T})$ is the covariance matrix of X. This case is not degraded in general.

Theorem 2: The rate–disturbance region of the Gaussian vector channel with parameters P, K_1, and K_2 is the convex hull of the set of pairs (R, R_d) such that

$$R \leq \tfrac{1}{2} \log \frac{|K_u + K_v + K_1|}{|K_1|},$$
$$R - R_\mathrm{d} \leq \tfrac{1}{2} \log \frac{|K_v + K_1|}{|K_v + K_2|} \frac{|K_2|}{|K_1|},$$
$$R_\mathrm{d} \geq \tfrac{1}{2} \log \frac{|K_v + K_2|}{|K_2|}.$$

for some positive semidefinite matrices $K_u, K_v \in \mathbb{R}^{n \times n}$ with $\mathrm{tr}(K_u + K_v) \leq P$.

Achievability of this rate–disturbance region follows by applying Theorem 1. Using the discretization procedure in [8], it can be shown that the theorem continues to hold with the power constraint additionally applied to the set of permissible input distributions. The claimed region then follows by considering the special case where the input distribution

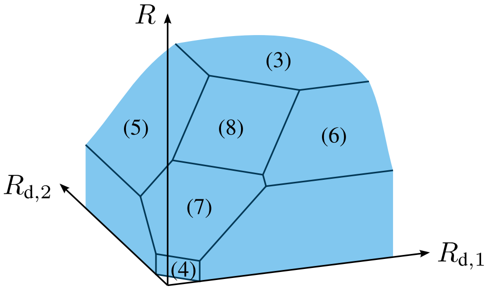


Fig. 5. Region $\mathscr{R}(U, X)$ for Theorem 3. Each face is annotated by the inequality that defines it.

$p(u, x)$ is jointly Gaussian. To prove the converse, we use an extremal inequality in [9] to show that Gaussian input distributions are sufficient. The details of the proof are given in Subsection III-E.

B. Inner and Outer Bounds for the Deterministic Channel With Two Disturbance Constraints

The correspondence between optimal encoding for the channel with one disturbance constraint and the Han–Kobayashi scheme for the interference channel with two user pairs suggests that the optimal coding scheme for K disturbance constraints may provide an efficient (if not optimal) scheme for the interference channel with $K + 1$ user pairs. This is particularly the case for extensions of the two user-pair injective deterministic interference channel for which Han–Kobayashi is optimal [7] (see Remark 5). As such, we restrict our attention to the deterministic version of the DMC-2-DC in which the channel outputs Y, Z_1, and Z_2 are arbitrary deterministic functions of the channel input X.

First, we establish the following inner bound on the rate–disturbance region.

Theorem 3 (Inner Bound): The rate–disturbance region $\mathscr{R}$ of the deterministic channel with two disturbance constraints is inner-bounded by the set of rate triples $(R, R_{\mathrm{d},1}, R_{\mathrm{d},2})$ such that

$$\begin{aligned} R &< H(Y), && (3)\\ R_{\mathrm{d},1} + R_{\mathrm{d},2} &> I(Z_1; Z_2 \mid U), && (4)\\ R - R_{\mathrm{d},1} &< H(Y \mid Z_1, U), && (5)\\ R - R_{\mathrm{d},2} &< H(Y \mid Z_2, U), && (6)\\ R - R_{\mathrm{d},1} - R_{\mathrm{d},2} &< H(Y \mid Z_1, Z_2, U) - I(Z_1; Z_2 \mid U), && (7)\\ 2R - R_{\mathrm{d},1} - R_{\mathrm{d},2} &< H(Y \mid Z_1, Z_2, U) + H(Y \mid U) \\ &\qquad - I(Z_1; Z_2 \mid U), && (8) \end{aligned}$$

for some pmf $p(u, x)$.

The inner bound is convex. The expression $I(Z_1; Z_2 \mid U)$ appears in three of the inequalities. As in Marton coding for the 2-receiver broadcast channel with a common message, it is the penalty incurred in encoding independent messages via dependent sequences. The region $\mathscr{R}(U, X)$ defined by the inequalities in the theorem for a fixed $p(u, x)$ is illustrated in Fig. 5.

Remark 6: The right-hand side of condition (8) can be equivalently expressed as

$$\begin{aligned} &H(Y \mid Z_1, Z_2, U) + H(Y \mid U) - I(Z_1; Z_2 \mid U)\\ &\qquad = H(Y \mid Z_1, U) + H(Y \mid Z_2, U) - I(Z_1; Z_2 \mid U, Y), \end{aligned}$$

This shows that the condition is stricter than the sum of conditions (5) and (6).

The encoding scheme for Theorem 3 involves rate splitting, Marton coding, and superposition coding. The message is split into four parts. Three of these parts are encoded as in Marton coding for the broadcast channel with a common message, with auxiliary random variables chosen according to U and the channel outputs Z_1 and Z_2. The fourth message part is encoded using superposition coding. The analysis of the probability of error, however, is complicated by the fact that receiver Y wishes to decode all parts of the message as detailed in Subsection IV-A. Receivers Z_1 and Z_2 each observe a satellite codeword from a superposition codebook.

Remark 7: The encoding scheme underlying the inner bound of Theorem 3 can be readily extended to the general (non-deterministic) DMC-2-DC.

To complement the inner bound, we establish the following outer bound on the rate–disturbance region of the deterministic channel with two disturbance constraints.

Theorem 4 (Outer Bound): If a rate triple $(R, R_{\mathrm{d},1}, R_{\mathrm{d},2})$ is achievable for the deterministic channel with two disturbance constraints, then it must satisfy the conditions

$$\begin{aligned} R &\le H(Y \mid Q),\\ R_{\mathrm{d},1} &\ge I(Y; Z_1 \mid Q),\\ R_{\mathrm{d},2} &\ge I(Y; Z_2 \mid Q), \end{aligned}$$

for some pmf $p(q, x)$ with $|\mathcal{Q}| \le 3$.

The proof of this outer bound is given in Subsection IV-B. Note that this outer bound is very similar in form to the alternative description of Corollary 1 for the single-constraint deterministic case.

The inner bound in Theorem 3 and the outer bound in Theorem 4 coincide in some special cases. To discuss these, we introduce the following notation. Since all channel outputs are functions of X, they can be equivalently thought of as set partitions of the input alphabet $\mathcal{X}$. Set partitions form a partially ordered set (poset) under the refinement relation. Since this poset is a complete lattice [10], the following concepts are well-defined. For two set partitions (functions) f and g, let $f \preccurlyeq g$ denote that f is a refinement of g (equivalently, g is degraded with respect to f), let $f \wedge g$ be the intersection of the two set partitions (the function that returns both f and g), and let $f \vee g$ denote the finest set partition of which both f and g are refinements (the Gács–Körner–Witsenhausen common part of f and g, see [11], [12]).

The inner bound of Theorem 3 coincides with the outer bound of Theorem 4 if Z_1 or Z_2 is a degraded version of $Y \wedge (Z_1 \vee Z_2)$, i.e., if the output Y together with the common part of Z_1 and Z_2 determine Z_1 or Z_2 completely.

Theorem 5: The rate–disturbance region $\mathscr{R}$ of the deterministic channel with two disturbance constraints is given by the

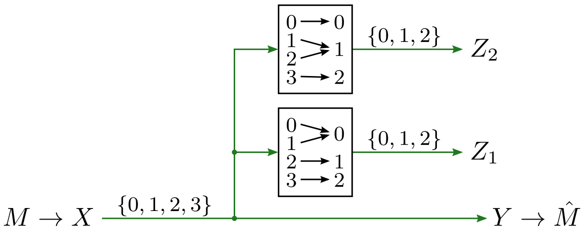


Fig. 6. Deterministic channel with two disturbance constraints.

outer bound of Theorem 4 if

$$Y \wedge (Z_1 \vee Z_2) \preccurlyeq Z_1, \quad \text{or}$$
$$Y \wedge (Z_1 \vee Z_2) \preccurlyeq Z_2.$$

The theorem is proved by specializing Theorem 3 as detailed in Subsection IV-C. In the case where Z_1 or Z_2 is a degraded version of Y alone, achievability follows by setting $U = \emptyset$ in Theorem 3. Otherwise, we let $U = Z_1 \vee Z_2$. This is intuitive, since U corresponds to the common-message step in the Marton encoding scheme.

Example 2: Consider the deterministic channel depicted in Fig. 6. The desired receiver output Y is a refinement of both side receiver outputs Z_1 and Z_2, and hence, Theorem 5 applies. Fig. 7(a) depicts the rate–disturbance region, numerically approximated by evaluating each grid point in a regular grid over the distributions $p(x)$ and subsequently taking the convex hull. Fig. 7(b) contrasts the single-constraint case (where $R_{\text{d},2}$ is set to infinity, and thus inactive) with the case where both side receivers are under the same disturbance rate constraint ($R_{\text{d},1} = R_{\text{d},2}$). As expected, imposing an additional disturbance constraint can significantly reduce the achievable message rate. Finally, Fig. 7(c) illustrates the trade-off between the disturbance rates $R_{\text{d},1}$ and $R_{\text{d},2}$ at the two side receivers, for a fixed data rate R.

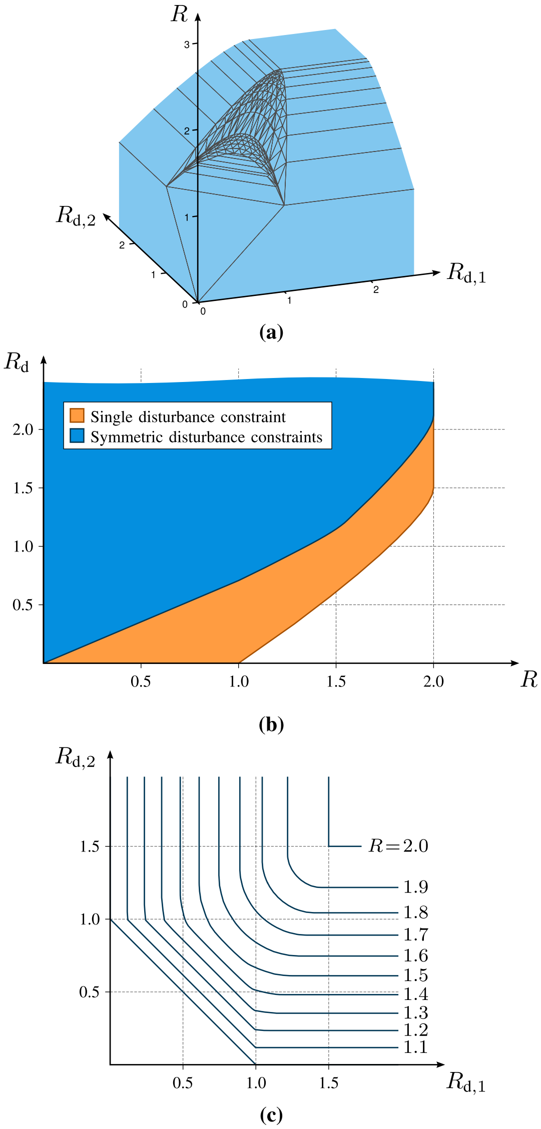
We conclude this section by considering another case in which we can fully characterize the rate–disturbance region of the deterministic channel with two disturbance constraints. If Z_1 is a degraded version of Z_2 (or vice versa), the region $\mathscr{R}$ of Theorem 3 is optimal and simplifies to the following.

Corollary 3: The rate–disturbance region $\mathscr{R}$ of the deterministic channel with two disturbance constraints with $Z_1 \preccurlyeq Z_2$ or $Z_2 \preccurlyeq Z_1$ is the set of rate triples $(R, R_{\text{d},1}, R_{\text{d},2})$ such that

$$\begin{aligned} R &\leq H(Y), \\ R - R_{\text{d},1} &\leq H(Y \,|\, Z_1), \\ R - R_{\text{d},2} &\leq H(Y \,|\, Z_2). \end{aligned}$$

for some pmf $p(x)$.

Achievability follows as a special case of Theorem 3. The encoding scheme carefully avoids introducing an ordering between the side receiver signals Z_1 and Z_2, but such ordering is naturally given by the channel here. Consequently, the corollary follows by setting the auxiliary U equal to the output at the degraded side receiver. This turns the encoding scheme into superposition coding with three layers. The details are given in Subsection IV-D.



(a)

(b)

(c)

Fig. 7. Rate–disturbance region for Example 2. (a) Rate–disturbance region. (b) Single disturbance constraint ($R_{\text{d},1} = R_\text{d}$, $R_{\text{d},2} = \infty$) and symmetric disturbance constraint ($R_{\text{d},1} = R_{\text{d},2} = R_\text{d}$). (c) Contour lines of the rate–disturbance region at constant rate R.

Note that the region of Corollary 3 is akin to the deterministic case with one disturbance constraint in Corollary 1. In both cases, the side receiver signals need not be degraded with respect to Y.

III. Proofs for a Single Disturbance Constraint

A. Achievability Proof of Theorem 1

Codebook Generation: Fix a pmf $p(u, x)$.

1) Split the message M into two independent messages M_0 and M_1 with rates R_0 and R_1, respectively. Hence $R = R_0 + R_1$.
2) For each $m_0 \in [1 : 2^{nR_0}]$, independently generate a sequence $u^n(m_0)$ according to $\prod_{i=1}^{n} p(u_i)$.
3) For each $(m_0, m_1) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$, independently generate a sequence $x^n(m_0, m_1)$ according to $\prod_{i=1}^{n} p(x_i \,|\, u_i(m_0))$.

Encoding: To send message $m = (m_0, m_1)$, transmit $x^n(m_0, m_1)$.

Decoding: Upon receiving y^n, find the unique $(\hat{m}_0, \hat{m}_1)$ such that $(u^n(\hat{m}_0), x^n(\hat{m}_0, \hat{m}_1), y^n) \in \mathcal{T}_\varepsilon^{(n)}(U, X, Y)$.

Analysis of the Probability of Error: We are using a superposition code over the channel from X to Y. Using the law of large numbers and the packing lemma in [8], it can be shown that the probability of error tends to zero as $n \to \infty$ if

$$R_1 < I(X; Y \,|\, U) - \delta(\varepsilon), \tag{9}$$

$$R_0 + R_1 < I(X; Y) - \delta(\varepsilon). \tag{10}$$

Analysis of Disturbance Rate: We analyze the disturbance rate averaged over codebooks $\mathcal{C}$.

$$\begin{aligned} I(X^n; Z^n \,|\, \mathcal{C}) &\le H(Z^n, M_0 \,|\, \mathcal{C}) - H(Z^n \,|\, X^n, \mathcal{C}) \\ &= H(M_0) + H(Z^n \,|\, M_0, \mathcal{C}) - H(Z^n \,|\, X^n) \\ &\overset{(a)}{\le} nR_0 + H(Z^n \,|\, U^n) - nH(Z \,|\, X) \\ &\le nR_0 + nH(Z \,|\, U) - nH(Z \,|\, X, U) \\ &= nR_0 + nI(X; Z \,|\, U) \\ &\le nR_{\mathrm{d}}, \end{aligned} \tag{11}$$

where (a) follows since U^n is a function of the codebook $\mathcal{C}$ and M_0. Substituting $R = R_0 + R_1$ and using Fourier–Motzkin elimination on inequalities (9), (10), and (11) yields the desired (R, R_{d}) region.

To complete the achievability proof, it remains to show that there exists a sequence of codes that satisfies *both* the probability of error and the disturbance constraint criteria. More generally, the random coding argument needs to be extended to the case with two simultaneous objectives. This extension is straightforward as long as one of the objective functions is non-negative and tends to zero. Then, the Markov inequality implies that a very large fraction of the code sequences satisfies this objective, hence there must be a sequence among them that additionally satisfies the second objective. The argument is detailed in Appendix A. This concludes the proof of achievability.

B. Converse of Theorem 1

Consider a sequence of codes with $P_e^{(n)} \to 0$ as $n \to \infty$ and the joint pmf that it induces on (M, X^n, Y^n, Z^n) assuming $M \sim \mathrm{Unif}[1:2^{nR}]$. Define the time-sharing random variable $Q \sim \mathrm{Unif}[1:n]$, independent of everything else. We use the identification $U = (Q, Y_{Q+1}^n, Z^{Q-1})$, and let $X = X_Q$, $Y = Y_Q$, and $Z = Z_Q$. Note that (X, Y, Z) is consistent with the channel. Then

$$R \le I(X; Y) + \varepsilon_n,$$

as in the converse proof for point-to-point channel capacity, which uses the same identifications of random variables. On the other hand,

$$\begin{aligned} nR_{\mathrm{d}} &\ge I(X^n; Z^n) \\ &= H(Z^n) - H(Z^n \,|\, X^n) \\ &= \sum_{i=1}^n \Big(H(Z_i \,|\, Z^{i-1}) - H(Z_i \,|\, X_i) \Big) \\ &\ge \sum_{i=1}^n H(Z_i \,|\, Z^{i-1}, Y_{i+1}^n) - nH(Z \,|\, X) \\ &= nH(Z \,|\, U) - nH(Z \,|\, X, U) \\ &= nI(X; Z \,|\, U). \end{aligned}$$

Finally,

$$\begin{aligned} &n(R_{\mathrm{d}} - R) \\ &\ge I(X^n; Z^n) - nR \\ &\overset{(a)}{\ge} H(Z^n) - H(Z^n \,|\, X^n) - I(M; Y^n) - n\varepsilon_n \\ &\overset{(b)}{=} \sum_{i=1}^n \Big(H(Z_i \,|\, Z^{i-1}) - I(M; Y_i \,|\, Y_{i+1}^n) \Big) - nH(Z \,|\, X) - n\varepsilon_n \\ &= \sum_{i=1}^n \Big(H(Z_i \,|\, Z^{i-1}, Y_{i+1}^n) + I(Y_{i+1}^n; Z_i \,|\, Z^{i-1}) \\ &\qquad - H(Y_i \,|\, Y_{i+1}^n) + H(Y_i \,|\, M, Y_{i+1}^n) \Big) - nH(Z \,|\, X) - n\varepsilon_n \\ &\overset{(c)}{=} \sum_{i=1}^n \Big(H(Z_i \,|\, Z^{i-1}, Y_{i+1}^n) + I(Y_i; Z^{i-1} \,|\, Y_{i+1}^n) \\ &\qquad - H(Y_i \,|\, Y_{i+1}^n) + H(Y_i \,|\, X_i) \Big) - nH(Z \,|\, X) - n\varepsilon_n \\ &= \sum_{i=1}^n \Big(H(Z_i \,|\, Z^{i-1}, Y_{i+1}^n) - H(Y_i \,|\, Z^{i-1}, Y_{i+1}^n) \\ &\qquad + H(Y_i \,|\, X_i, Z^{i-1}, Y_{i+1}^n) \Big) - nH(Z \,|\, X) - n\varepsilon_n \\ &= \sum_{i=1}^n \Big(H(Z_i \,|\, Z^{i-1}, Y_{i+1}^n) - I(X_i; Y_i \,|\, Z^{i-1}, Y_{i+1}^n) \Big) \\ &\qquad - nH(Z \,|\, X) - n\varepsilon_n \\ &\overset{(d)}{=} nH(Z \,|\, U) - nI(X; Y \,|\, U) - nH(Z \,|\, X, U) - n\varepsilon_n \\ &= nI(X; Z \,|\, U) - I(X; Y \,|\, U) - n\varepsilon_n, \end{aligned}$$

where (a) uses Fano's inequality, (b) single-letterizes the noise term $H(Z^n \,|\, X^n)$ with equality due to memorylessness of the channel, (c) applies Csiszár's sum identity to the second term and channel memorylessness to the fourth term, and (d) uses the previous definitions of auxiliary random variables. Finally, the cardinality bound on $\mathcal{U}$ is established using the convex cover method in [8].

C. Proof of Corollary 1

Using the deterministic nature of the channel, the region in Theorem 1 reduces to the set of rate pairs (R, R_{d}) such that

$$R \le H(Y), \tag{12}$$

$$R_{\mathrm{d}} \ge H(Z \,|\, U), \tag{13}$$

$$R_{\mathrm{d}} \ge R + H(Z \,|\, U) - H(Y \,|\, U), \tag{14}$$

for some pmf $p(u, x)$. Now fixing a rate R and a pmf $p(x)$ and varying $p(u|x)$ to minimize R_{d}, the right hand sides of (13) and (14) are lower bounded by

$$H(Z \mid U) \geq 0,$$

and

$$\begin{aligned}
R + H(Z \mid U) - H(Y \mid U) \\
&= R + H(Z \mid U) - H(Y, Z \mid U) + H(Z \mid Y, U) \\
&= R - H(Y \mid Z, U) + H(Z \mid Y, U) \\
&\geq R - H(Y \mid Z).
\end{aligned}$$

Note that the particular choice $U = Z$ simultaneously achieves both lower bounds with equality and is therefore sufficient. The rate–disturbance region thus reduces to Corollary 1.

For a fixed pmf $p(x)$, this region has exactly two relevant corner points: $P_1 = (H(Y|Z), 0)$ and $P_2 = (H(Y), I(Y; Z))$. As we vary $p(x)$, there is one corner point P_1 that dominates all other P_1 points. The pmf $p(x)$ for this dominant P_1 can be constructed by maximizing $H(Y|Z)$ as follows. For each $z \in \mathcal{Z}$, define $\mathcal{Y}_z \subseteq \mathcal{Y}$ to be the set of symbols y that are compatible with z, i.e., that can occur simultaneously with z as channel outputs. Let $z^\star$ be one of the symbols z that maximize $|\mathcal{Y}_z|$. For each element of $\mathcal{Y}_{z^\star}$, choose exactly one x that is compatible with it and $z^\star$. Finally, place equal probability mass on each of the chosen x values, and zero mass on all others. This pmf on X yields the dominant corner point P_1, namely $(\log(|\mathcal{Y}_{z^\star}|), 0)$. Moreover, for this distribution, P_2 coincides with P_1. Therefore, the net contribution (modulo convexification) of each pmf $p(x)$ to the rate–disturbance region amounts to its corner point P_2. This implies the alternative description of the region. Lastly, the cardinality bound on $\mathcal{Q}$ in the alternative description follows from the convex cover method in [8].

D. Proof of Corollary 2

Achievability is straightforward using a random Gaussian codebook with power control, and upper-bounding the disturbance rate at receiver Z by white Gaussian noise. The converse can be seen as follows. Clearly, $R \leq \mathrm{C}(P)$. Let $\alpha^\star \in [0, 1]$ be such that $R = \mathrm{C}(\alpha^\star P)$. Then

$$\begin{aligned}
n\,\mathrm{C}(\alpha^\star P) = nR &\leq I(X^n; Y^n) + n\varepsilon_n \\
&= h(Y^n) - h(Y^n \mid X^n) + n\varepsilon_n,
\end{aligned}$$

and therefore,

$$\begin{aligned}
h(Y^n) &\geq \tfrac{n}{2}\log(2\pi e) + n\,\mathrm{C}(\alpha^\star P) - n\varepsilon_n \\
&= \tfrac{n}{2}\log\left(2\pi e(1 + \alpha^\star P)\right) - n\varepsilon_n
\end{aligned}$$

Since $N < 1$, we can write the physically degraded form of the channel as $Y = X + W_1$, $Z = Y + \tilde{W}_2$, where $\tilde{W}_2 \sim \mathcal{N}(0, N - 1)$ is the excess noise that receiver Z experiences in addition to receiver Y. Applying the vector entropy power inequality to $Z^n = Y^n + \tilde{W}_2^n$, we conclude

$$\begin{aligned}
\tfrac{1}{n}h(Z^n) &\geq \tfrac{1}{2}\log\left(2^{\frac{2}{n}h(Y^n)} + 2^{\frac{2}{n}h(\tilde{W}_2^n)}\right) \\
&\geq \tfrac{1}{2}\log\left(2^{-2\varepsilon_n} \cdot 2\pi e(1 + \alpha^\star P) + 2\pi e(N - 1)\right) \\
&\geq \tfrac{1}{2}\log\left(2\pi e(N + \alpha^\star P)\right) - \varepsilon_n,
\end{aligned}$$

and finally,

$$\begin{aligned}
R_{\mathrm{d}} &\geq \tfrac{1}{n} I(X^n; Z^n) \\
&= \tfrac{1}{n}h(Z^n) - \tfrac{1}{2}\log(2\pi e N) \\
&\geq \mathrm{C}(\alpha^\star P/N) - \varepsilon_n.
\end{aligned}$$

E. Proof of Theorem 2

Recall the shape of $\mathscr{R}(U, X)$ depicted in Fig. 2. The coordinates of the corner points A and B are given by

$$\begin{aligned}
A(U, X):\quad R &= h(X + W_1) - h(W_1), && (15)\\
R_{\mathrm{d}} &= h(X + W_2 \mid U) + h(X + W_1) \\
&\quad - h(X + W_1 \mid U) - h(W_2), && (16)\\
B(U, X):\quad R &= h(X + W_1 \mid U) - h(W_1), && (17)\\
R_{\mathrm{d}} &= h(X + W_2 \mid U) - h(W_2). && (18)
\end{aligned}$$

Proof of Achievability: We specialize Theorem 1. Consider the specific $p(u, x)$ constructed as follows. For given positive semidefinite matrices $K_u, K_v \in \mathbb{R}^{n \times n}$ with $\operatorname{tr}(K_u + K_v) \leq P$, let

$$\begin{aligned}
U &\sim \mathcal{N}(0, K_u), \\
V &\sim \mathcal{N}(0, K_v), \\
X &= U + V,
\end{aligned}$$

where U and V are independent. Then, the terms in Theorem 1 evaluate to

$$\begin{aligned}
I(X; Y) &= h(Y) - h(W_1) = \tfrac{1}{2}\log\frac{|K_u + K_v + K_1|}{|K_1|}, \\
I(X; Y \mid U) &= h(Y \mid U) - h(W_1) = \tfrac{1}{2}\log\frac{|K_v + K_1|}{|K_1|}, \\
I(X; Z \mid U) &= h(Z \mid U) - h(W_2) = \tfrac{1}{2}\log\frac{|K_v + K_2|}{|K_2|}.
\end{aligned}$$

Simplifying the right hand sides and introducing time-sharing leads to the desired result.

For completeness, the coordinates of A and B for given matrices K_u, K_v are

$$\begin{aligned}
A(K_u, K_v):\quad R &= \tfrac{1}{2}\log\frac{|K_u + K_v + K_1|}{|K_1|}, && (19)\\
R_{\mathrm{d}} &= \tfrac{1}{2}\log\frac{|K_v + K_2|}{|K_2|}\frac{|K_u + K_v + K_1|}{|K_v + K_1|}, && (20)\\
B(K_u, K_v):\quad R &= \tfrac{1}{2}\log\frac{|K_v + K_1|}{|K_1|}, && (21)\\
R_{\mathrm{d}} &= \tfrac{1}{2}\log\frac{|K_v + K_2|}{|K_2|}. && (22)
\end{aligned}$$

The constituent region $\mathscr{R}(U, X)$ for fixed K_u and K_v is depicted in Fig. 8. □

Proof of Converse: The converse proof of Theorem 1 continues to hold and we only need to show that Gaussian input distributions are sufficient. We proceed as follows. Since the rate–disturbance region is convex, its boundary can be fully characterized by maximizing $R - \lambda R_{\mathrm{d}}$ for each $\lambda > 0$. We write

$$\begin{aligned}
R - \lambda R_{\mathrm{d}} &\leq \max_{(R, R_{\mathrm{d}}) \in \mathscr{R}} \{R - \lambda R_{\mathrm{d}}\} \\
&= \max_{(U,X)} \max_{(R, R_{\mathrm{d}}) \in \mathscr{R}(U,X)} \{R - \lambda R_{\mathrm{d}}\},
\end{aligned}$$

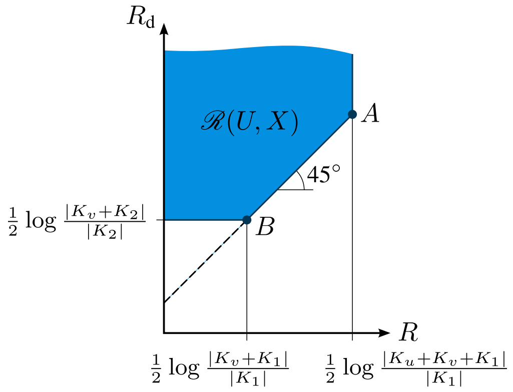

$R_{\rm d}$
$\mathscr{R}(U,X)$
A
$45°$
B
$\frac{1}{2}\log\frac{|K_v+K_2|}{|K_2|}$
R
$\frac{1}{2}\log\frac{|K_v+K_1|}{|K_1|}$
$\frac{1}{2}\log\frac{|K_u+K_v+K_1|}{|K_1|}$

Fig. 8. Constituent region for Gaussian superposition codebook with parameters K_u and K_v.

where the outer optimization is over the joint distribution of (U, X) and the inner optimization is over the region achieved by that distribution. The inner optimization can be solved explicitly as follows. For ease of presentation, assume for the moment that the power constraint is of the form $K_x \preceq S$ for some positive semidefinite matrix S. (That is, valid K_x are precisely those that result in the matrix $S - K_x$ being positive semidefinite.)

First, consider $\lambda \le 1$. For any distribution $(U, X) \sim p(u, x)$, point $A(U, X)$ achieves a value of the inner optimization at least as large as point $B(U, X)$, or any point on the line between them. Using the coordinates of $A(U, X)$ in (15) and (16), we can write

$$\begin{aligned}
&R - \lambda R_{\rm d}\\
&\le \max_{(U,X)} \{\lambda\,(h(X + W_1 \,|\, U) - h(X + W_2 \,|\, U))\\
&\qquad\qquad + (1-\lambda)h(X + W_1) - h(W_1) + \lambda h(W_2)\}\\
&\overset{(a)}{\le} \lambda \cdot \max_{(U,X)} \{h(X + W_1 \,|\, U) - h(X + W_2 \,|\, U)\}\\
&\qquad\qquad +(1-\lambda)\cdot \max_{(U,X)} \{h(X+W_1)\} - h(W_1) + \lambda h(W_2)\\
&\overset{(b)}{\le} \lambda \cdot \max_{K_x \preceq S} \left\{ \tfrac{1}{2}\log\frac{|K_x + K_1|}{|K_x + K_2|} \right\}\\
&\quad +(1-\lambda)\cdot \max_{K_x \preceq S} \left\{ \tfrac{1}{2}\log\left((2\pi e)^n |K_x + K_1|\right)\right\}\\
&\quad -\tfrac{1}{2}\log\left((2\pi e)^n |K_1|\right) + \tfrac{\lambda}{2}\log\left((2\pi e)^n |K_2|\right).
\end{aligned}$$

In (a), the two maximizations are taken independently. In step (b), the first maximization is achieved by a Gaussian X that is independent of U, due to a theorem proved by Liu and Viswanath [9, Th. 8]. The optimization is now only over covariances matrices. Let $K^\star$ be an optimizer of this first maximization. The second maximization is also achieved by a Gaussian X, and is optimized by $K_x = S$ since $f(K_x) = |K_x + K_1|$ is matrix monotone. It follows that

$$\begin{aligned}
R - \lambda R_{\rm d} &\le \tfrac{\lambda}{2}\log\frac{|K^\star + K_1|}{|K^\star + K_2|} + \tfrac{1-\lambda}{2}\log\left((2\pi e)^n |S + K_1|\right)\\
&\quad -\tfrac{1}{2}\log\left((2\pi e)^n |K_1|\right) + \tfrac{\lambda}{2}\log\left((2\pi e)^n |K_2|\right)\\
&= \tfrac{1}{2}\log\frac{|S + K_1|}{|K_1|} - \tfrac{\lambda}{2}\log\frac{|K^\star + K_2|}{|K^\star + K_1|}\,\frac{|S + K_1|}{|K_2|}.
\end{aligned}$$

But this upper bound is achieved with equality by Gaussian superposition codebooks, namely through the point $A(K_u, K_v)$ as specified by equations (19) and (20), with $K_u = S - K^\star$ and $K_v = K^\star$.

Now, consider $\lambda > 1$. The argument proceeds analogously to the previous case. For completeness' sake, the details are as follows. We can write the inner optimization explicitly using the coordinates of $B(U, X)$ in (17) and (18) as

$$\begin{aligned}
R - \lambda R_{\rm d} &\le \max_{(U,X)} \{h(X + W_1 \,|\, U) - \lambda h(X + W_2 \,|\, U)\}\\
&\qquad\qquad + \lambda h(W_2) - h(W_1)\\
&\overset{(a)}{\le} \max_{K_x \preceq S} \left\{ \tfrac{1}{2}\log\left((2\pi e)^n |K_x + K_1|\right)\right.\\
&\qquad\qquad \left. - \tfrac{\lambda}{2}\log\left((2\pi e)^n |K_x + K_2|\right)\right\}\\
&\quad +\tfrac{\lambda}{2}\log\left((2\pi e)^n |K_2|\right) - \tfrac{1}{2}\log\left((2\pi e)^n |K_1|\right).
\end{aligned}$$

The optimum in (a) is achieved by a Gaussian X (independent of U) by virtue of [9, Th. 8], while the other two terms are independent of the optimization variable. Let $K^\star$ be an optimizer. Then

$$R - \lambda R_{\rm d} \le \tfrac{1}{2}\log\frac{|K^\star + K_1|}{|K_1|} - \tfrac{\lambda}{2}\log\frac{|K^\star + K_2|}{|K_2|}.$$

This upper bound is achieved with equality by Gaussian superposition codebooks through the point $B(K_u, K_v)$ as given by equations (21) and (22) with $K_u = 0$ and $K_v = K^\star$. This is a power control strategy, similar to the scalar Gaussian case.

We have thus shown that under a power constraint $K_x \preceq S$, Gaussian superposition codes are optimal. The conclusion extends to the sum power constraint $\mathrm{tr}(K_x) \le P$ by observing that

$$\{K_x : \mathrm{tr}(K_x) \le P\} = \bigcup_{\substack{S:\, S \succeq 0\\ \mathrm{tr}(S) \le P}} \{K_x : K_x \preceq S\}.$$

In other words, the sum power constraint can be expressed as a union of constraints of the type $K_x \preceq S$, for each of which Gaussian superposition codes are optimal. Therefore, a Gaussian superposition code must be optimal overall. □

IV. Proofs for Two Disturbance Constraints

A. Proof of Theorem 3

Codebook Generation: Fix a pmf $p(u, x)$. Split the rate as $R = R_0 + R_1 + R_2 + R_3$. Define the auxiliary rates $\tilde{R}_1 \ge R_1$ and $\tilde{R}_2 \ge R_2$, let $\varepsilon' > 0$, and define the set partitions

$$\begin{aligned}
[1\,{:}\,2^{n\tilde{R}_1}] &= \mathcal{L}_1(1) \cup \cdots \cup \mathcal{L}_1(2^{nR_1}),\\
[1\,{:}\,2^{n\tilde{R}_2}] &= \mathcal{L}_2(1) \cup \cdots \cup \mathcal{L}_2(2^{nR_2}),
\end{aligned}$$

where $\mathcal{L}_1(\cdot)$ and $\mathcal{L}_2(\cdot)$ are indexed sets of size $2^{n(\tilde{R}_1 - R_1)}$ and $2^{n(\tilde{R}_2 - R_2)}$, respectively.

1) For each $m_0 \in [1\,{:}\,2^{nR_0}]$, generate $u^n(m_0)$ according to $\prod_{i=1}^n p(u_i)$.
2) For each $l_1 \in [1\,{:}\,2^{n\tilde{R}_1}]$, generate $z_1^n(m_0, l_1)$ according to $\prod_{i=1}^n p(z_{1i} \,|\, u_i(m_0))$. Likewise, for each $l_2 \in [1\,{:}\,2^{n\tilde{R}_2}]$, generate $z_2^n(m_0, l_2)$ according to $\prod_{i=1}^n p(z_{2i} \,|\, u_i(m_0))$.
3) For each (m_0, m_1, m_2), let $\mathcal{S}(m_0, m_1, m_2)$ be the set of all pairs (l_1, l_2) from the product set

TABLE I
MESSAGE SUBSETS FOR DECODING ERROR EVENTS

Message subset	m_0	m_1	m_2	m_3
$\mathcal{M}_0$	1	1	1	1
$\mathcal{M}_1$	1	1	1	$\neq 1$
$\mathcal{M}_2$	1	$\neq 1$	1	any
$\mathcal{M}_3$	1	1	$\neq 1$	any
$\mathcal{M}_4$	1	$\neq 1$	$\neq 1$	any
$\mathcal{M}_5$	$\neq 1$	any	any	any

$\mathcal{L}_1(m_1) \times \mathcal{L}_2(m_2)$ such that $(z_1^n(m_0, l_1), z_2^n(m_0, l_2)) \in \mathcal{T}_{\varepsilon'}^{(n)}(Z_1, Z_2 \,|\, u^n(m_0))$.

4) For each (m_0, l_1, l_2) and $m_3 \in [1 : 2^{nR_3}]$, generate $x^n(m_0, l_1, l_2, m_3)$ according to

$$\prod_{i=1}^{n} p(x_i \,|\, u_i(m_0), z_{1i}(l_1), z_{2i}(l_2))$$

if $(l_1, l_2) \in \mathcal{S}(m_0, m_1, m_2)$. Otherwise, we draw from $\mathrm{Unif}(\mathcal{X}^n)$.

5) Choose $(l_1^{(m_0,m_1,m_2)}, l_2^{(m_0,m_1,m_2)})$ uniformly from $\mathcal{S}(m_0, m_1, m_2)$. If $\mathcal{S}(m_0, m_1, m_2)$ is empty, choose $(1, 1)$.

Encoding: To send message $m = (m_0, m_1, m_2, m_3)$, transmit the sequence

$$x^n(m_0, l_1^{(m_0,m_1,m_2)}, l_2^{(m_0,m_1,m_2)}, m_3).$$

Decoding: Let $\varepsilon > \varepsilon'$. Upon receiving y^n, define the tuple

$$\begin{aligned} T(m_0, m_1, m_2, m_3) &= \Big(u^n(m_0), z_1^n(m_0, l_1^{(m_0,m_1,m_2)}), z_2^n(m_0, l_2^{(m_0,m_1,m_2)}), \\ &\qquad x^n(m_0, l_1^{(m_0,m_1,m_2)}, l_2^{(m_0,m_1,m_2)}, m_3), y^n\Big) \end{aligned}$$

Declare that $\hat{m} = (\hat{m}_0, \hat{m}_1, \hat{m}_2, \hat{m}_3)$ has been sent if it is the unique message such that

$$T(\hat{m}_0, \hat{m}_1, \hat{m}_2, \hat{m}_3) \in \mathcal{T}_{\varepsilon}^{(n)}(U, Z_1, Z_2, X, Y).$$

Analysis of the Probability of Error: Without loss of generality, assume that $m_0 = m_1 = m_2 = m_3 = 1$ is transmitted. Define the following events.

$$\begin{aligned} &\mathcal{E}_{\mathrm{e}1}: \quad \mathcal{S}(1, 1, 1) \text{ is empty,} \\ &\mathcal{E}_{\mathrm{e}2}: \quad \mathcal{S}(1, 1, 1) \text{ contains two distinct pairs with} \\ &\qquad\qquad \text{equal first or second component,} \\ &\mathcal{E}_i: \quad \{T(m_0, m_1, m_2, m_3) \in \mathcal{T}_{\varepsilon}^{(n)}(U, Z_1, Z_2, X, Y) \text{ for} \\ &\qquad\qquad \text{some } (m_0, m_1, m_2, m_3) \in \mathcal{M}_i\}, \qquad i \in \{0, \ldots, 5\}, \end{aligned}$$

where the message subsets $\mathcal{M}_i$ are specified in Table I. Defining the "encoding error" event $\mathcal{E}_{\mathrm{e}} = \mathcal{E}_{\mathrm{e}1} \cup \mathcal{E}_{\mathrm{e}2}$ and the "decoding error" event $\mathcal{E}_{\mathrm{d}} = \mathcal{E}_0^c \cup \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \cup \mathcal{E}_4 \cup \mathcal{E}_5$, the probability of error can be upper-bounded as

$$\mathrm{P}(\mathcal{E}) \le \mathrm{P}(\mathcal{E}_{\mathrm{e}} \cup \mathcal{E}_{\mathrm{d}}) \le \mathrm{P}(\mathcal{E}_{\mathrm{e}}) + \mathrm{P}(\mathcal{E}_{\mathrm{d}} \,|\, \mathcal{E}_{\mathrm{e}}^c).$$

The motivation for introducing $\mathcal{E}_{\mathrm{e}2}$ as an "error" is to simplify the analysis of the second probability term.

We bound $\mathrm{P}(\mathcal{E}_{\mathrm{e}})$ by the following lemma. Let $r_1 = \tilde{R}_1 - R_1$ and $r_2 = \tilde{R}_2 - R_2$.

Lemma 1: $\mathrm{P}(\mathcal{E}_{\mathrm{e}}) \to 0$ as $n \to \infty$ if

$$r_1 + r_2 > I(Z_1; Z_1 \,|\, U) + \delta(\varepsilon'), \tag{23}$$

$$r_1/2 + r_2 < I(Z_1; Z_2 \,|\, U) - \delta(\varepsilon'), \tag{24}$$

$$r_1 + r_2/2 < I(Z_1; Z_2 \,|\, U) - \delta(\varepsilon'). \tag{25}$$

Proof Sketch: First, consider $\mathcal{E}_{\mathrm{e}1}$. As in the proof of Marton's inner bound for the broadcast channel, the mutual covering lemma [8] implies $\mathrm{P}(\mathcal{E}_{\mathrm{e}1}) \to 0$ as $n \to \infty$ if (23) holds.

Now consider $\mathcal{E}_{\mathrm{e}2}$, for which we need to control the number of typical pairs that can occur in the same "row" or "column" of the product set $\mathcal{L}_1(m_1) \times \mathcal{L}_2(m_2)$, i.e., for the same l_1 or l_2 coordinate. The probability $\mathrm{P}(\mathcal{E}_{\mathrm{e}2})$ tends to zero provided that (24) and (25) hold.

This is akin to the birthday problem [13], where k samples are drawn uniformly and independently from $[1\!:\!N]$, and the interest is in samples that have the same value (collisions). It is well-known that for the probability of collision to be p_c, the number of samples required is roughly $k \approx \sqrt{-2N \ln(1 - p_c)}$, which scales with $\sqrt{N}$. In our case, the number of samples is the cardinality of the set $\mathcal{S}(m_0, m_1, m_2)$, which is roughly $k = 2^{n(r_1 + r_2 - I(Z_1; Z_2 \,|\, U))}$. The samples are categorized into $N_1 = 2^{nr_1}$ and $N_2 = 2^{nr_2}$ classes along rows and columns, respectively. To achieve a probability of collision $p_c \to 0$ along both dimensions, we need $k \ll \min\{\sqrt{N_1}, \sqrt{N_2}\}$, which yields exactly the conditions (24) and (25).

A rigorous proof is given in Appendix B. □

We bound the probability $\mathrm{P}(\mathcal{E}_{\mathrm{d}} \,|\, \mathcal{E}_{\mathrm{e}}^c)$ by the following lemma.

Lemma 2: $\mathrm{P}(\mathcal{E}_{\mathrm{d}} \,|\, \mathcal{E}_{\mathrm{e}}^c) \to 0$ as $n \to \infty$ if the conditions of Lemma 1 hold, and

$$R_3 < H(Y \,|\, Z_1, Z_2, U) - \delta(\varepsilon), \tag{26}$$

$$\tilde{R}_1 + R_3 < H(Y \,|\, Z_2, U) + I(Z_1; Z_2 \,|\, U) - \delta(\varepsilon), \tag{27}$$

$$\tilde{R}_2 + R_3 < H(Y \,|\, Z_1, U) + I(Z_1; Z_2 \,|\, U) - \delta(\varepsilon), \tag{28}$$

$$\tilde{R}_1 + \tilde{R}_2 + R_3 < H(Y \,|\, U) + I(Z_1; Z_2 \,|\, U) - \delta(\varepsilon), \tag{29}$$

$$R_0 + \tilde{R}_1 + \tilde{R}_2 + R_3 < H(Y) + I(Z_1; Z_2 \,|\, U) - \delta(\varepsilon). \tag{30}$$

Proof Sketch: The events of which $\mathcal{E}_{\mathrm{d}}$ is composed are illustrated in Fig. 9, which also depicts the structure of the codebook for $m_0 = 1$. The product sets $\mathcal{L}_1(m_1) \times \mathcal{L}_2(m_2)$, for each (m_1, m_2), are represented by shaded squares. In each product set, the sequence pair selected in step 5 of the codebook generation procedure is shown with its superposed x^n codewords, as created in step 4. The correct codeword $x^n(1, l_1^{(1,1,1)}, l_2^{(1,1,1)}, 1)$ is shown as a white circle which is connected to the received sequence y^n. The codewords that may be mistakenly detected at the receiver are shown as black circles. The product sets associated with decoding error events $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$, and $\mathcal{E}_4$ are labeled 1, 2, 3, and 4, respectively.

We bound the probability of each sub-event of $\mathcal{E}_{\mathrm{d}}$. First, note that by the conditional typicality lemma in [8], $\mathrm{P}(\mathcal{E}_0^c) \to 0$ as $n \to \infty$ (this relies on $\varepsilon' < \varepsilon$). The probabilities of the events

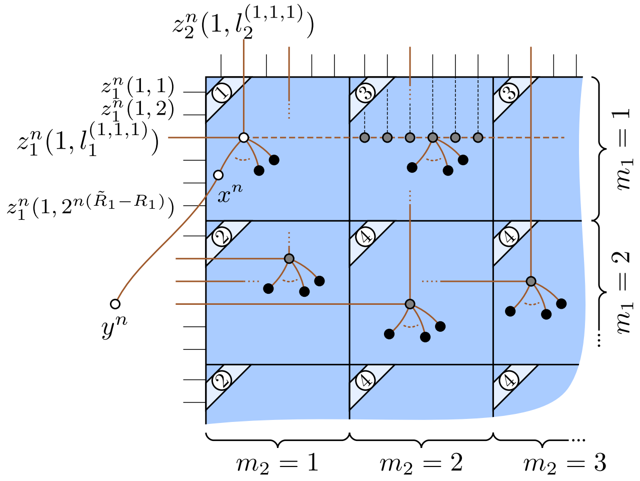


Fig. 9. Illustration of decoding error events, for $m_0 = 1$.

$\mathcal{E}_1$ through $\mathcal{E}_5$ conditioned on $\mathcal{E}_\mathrm{e}^c$ tend to zero as $n \to \infty$ under conditions (26) through (30), correspondingly.

The events $\mathcal{E}_2$ and $\mathcal{E}_3$ require the most careful analysis, since the true codeword $x^n(1, l_1^{(1,1,1)}, l_2^{(1,1,1)}, 1)$ and the codewords with which it may be confused can be statistically dependent by sharing the same z_1^n or z_2^n sequence (see dashed line and circles on it in Fig. 9). Moreover, even when the chosen pairs in two different product sets do not share one of the two coordinates (see, for example, the chosen pairs for $(m_1, m_2) = (1, 1)$ and $(2, 1)$ in Fig. 9), statistical dependence could potentially occur. This can be caused by the selection procedure in step 5 of codebook generation, since the indices $(l_1^{(m_0,m_1,m_2)}, l_2^{(m_0,m_1,m_2)})$ statistically depend on all sequences in the product set. We use the following lemma to show that the event $\mathcal{E}_{\mathrm{e}2}^c$ prevents this dependence leakage from occurring.

Lemma 3 (Independence Lemma): Consider a finite set $\mathcal{A}$ and a subset $\mathcal{A}' \subset \mathcal{A}$. Let p_A be an arbitrary pmf over $\mathcal{A}$. Let the random vector A^n be distributed proportionally to the product distribution $\prod_{l=1}^n p_A(a_l)$, restricted to the support set $\{a^n : a_k \in \mathcal{A}' \text{ for some } k\}$. Let I be drawn uniformly from $\{i : A_i \in \mathcal{A}'\}$. Let $J = I + 1$, if $I < n$, and $J = 1$ otherwise. Then, the random variables A_I and A_J are independent.

A proof is provided in Appendix C. The application of the lemma is what distinguishes this analysis from the conventional Marton inner bound for broadcast channels [14], [15]. There, analysis of the selection procedure can be altogether avoided since each receiver decodes only one of the two coordinates.

A detailed proof for the event $\mathcal{E}_3$ is given in Appendix D, the other events follow likewise. □

Analysis of Disturbance Rate: When viewed by receiver Z_1, the codeword for message $m = (m_0, m_1, m_2, m_3)$ appears as $z_1^n(m_0, l_1^{(m_0,m_1,m_2)})$. We can pessimistically assume that all sequences $z_1^n(m_0, l_1)$ as created in step 2 of codebook generation can be seen at the receiver for some message m. Therefore, the number of possible sequences at Z_1, and thus its disturbance rate, is upper-bounded by $H(Z_1^n) \le n(R_0 + \tilde{R}_1)$. Applying the same argument for Z_2, the proposed scheme achieves

$$R_0 + \tilde{R}_1 \le R_{\mathrm{d},1}, \tag{31}$$

$$R_0 + \tilde{R}_2 \le R_{\mathrm{d},2}. \tag{32}$$

Conclusion of the Proof: Collecting inequalities (23) through (32), recalling $R = R_0 + R_1 + R_2 + R_3$, and using the Fourier–Motzkin procedure to eliminate R_0, R_1, R_2, and R_3 leads to the $(R, R_{\mathrm{d},1}, R_{\mathrm{d},2})$ region claimed in the theorem.

Finally, the statement of Remark 6 follows from

$$\begin{aligned} -I(Z_1; Z_2 \,|\, U) + I(Z_1; Z_2 \,|\, U, Y) &= -H(Z_2 \,|\, U) + H(Z_2 \,|\, U, Z_1) + H(Z_2 \,|\, U, Y) \\ &\quad -H(Z_2 \,|\, U, Y, Z_1) \\ &= -I(Y; Z_2 \,|\, U) + I(Y; Z_2 \,|\, U, Z_1), \end{aligned}$$

which leads to the equality

$$\begin{aligned} &H(Y \,|\, Z_1, Z_2, U) + H(Y \,|\, U) - I(Z_1; Z_2 \,|\, U) \\ &\qquad + I(Z_1; Z_2 \,|\, U, Y) \\ &\quad = H(Y \,|\, Z_1, Z_2, U) + H(Y \,|\, U) - I(Y; Z_2 \,|\, U) \\ &\qquad + I(Y; Z_2 \,|\, U, Z_1) \\ &\quad = H(Y \,|\, Z_1, U) + H(Y \,|\, Z_2, U). \end{aligned}$$

B. Proof of Theorem 4

First, consider

$$\begin{aligned} nR &\le I(X^n; Y^n) + n\epsilon_n \\ &= \sum_{i=1}^n I(X^n; Y_i \,|\, Y^{i-1}) + n\epsilon_n \\ &= \sum_{i=1}^n I(X_i; Y_i \,|\, Y^{i-1}) + n\epsilon_n \\ &= nI(X; Y \,|\, Q) \\ &= nH(Y \,|\, Q). \end{aligned}$$

Furthermore,

$$\begin{aligned} nR_{\mathrm{d},1} &\ge I(X^n; Z_1^n) \\ &\ge I(Y^n; Z_1^n) \\ &= \sum_{i=1}^n I(Y_i; Z_1^n \,|\, Y^{i-1}) \\ &\ge \sum_{i=1}^n I(Y_i; Z_{1i} \,|\, Y^{i-1}) \\ &= nI(Y; Z_1 \,|\, Q), \end{aligned}$$

where $Y = Y_T$, $Z_1 = Z_{1T}$, and $Q = (Y^{T-1}, T)$ with $T \sim \mathrm{Unif}[1\,{:}\,n]$. The same argument leads to

$$nR_{\mathrm{d},2} \ge nI(Y; Z_2 \,|\, Q),$$

with the same random variable identifications, and the additional $Z_2 = Z_{2T}$. Finally, the cardinality bound on $\mathcal{Q}$ follows from the convex cover method in [8].

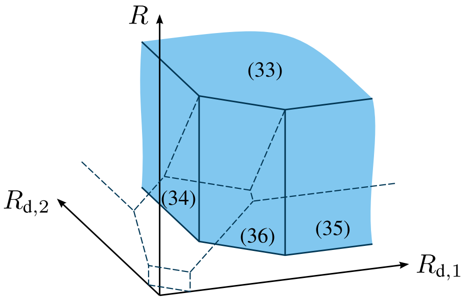


Fig. 10. Constituent region for Corollary 4, for a fixed $p(u, x)$. Each face is annotated by the inequality that defines it. For comparison, the constituent region of Theorem 3 is shown with dashed lines (see Fig. 5).

C. Proof of Theorem 5

First, we specialize Theorem 3 as follows.

Corollary 4: The rate–disturbance region $\mathscr{R}$ of the deterministic channel with two disturbance constraints is inner-bounded by the set of rate triples $(R, R_{\mathrm{d},1}, R_{\mathrm{d},2})$ such that

$$\begin{aligned} R &< H(Y), && (33)\\ R_{\mathrm{d},1} &> I(Y; Z_1, U), && (34)\\ R_{\mathrm{d},2} &> I(Y; Z_2, U), && (35)\\ R_{\mathrm{d},1} + R_{\mathrm{d},2} &> I(Y; Z_1, Z_2, U) + I(Y; U) + I(Z_1; Z_2 \,|\, U) &&\\ &= I(Y; Z_1, U) + I(Y; Z_2, U) &&\\ &\quad + I(Z_1; Z_2 \,|\, U, Y), && (36) \end{aligned}$$

for some pmf $p(u, x)$.

The two equivalent expressions in (36) originate from Remark 6. An example of the constituent regions of Corollary 4 for fixed $p(u, x)$ is depicted in Fig. 10. The figure also illustrates how the corollary follows from Theorem 3: Each constituent region of the corollary is a strict subset of the constituent region of the theorem, for the same $p(u, x)$.

Proof of Corollary 4: In Theorem 3, consider the case where (3) is met with equality, i.e., $R = H(Y)$. This yields a subset region which is still achievable. It simplifies to

$$\begin{aligned} R_{\mathrm{d},1} + R_{\mathrm{d},2} &> I(Z_1; Z_2 \,|\, U), && (37)\\ R_{\mathrm{d},1} &> I(Y; Z_1, U), && (38)\\ R_{\mathrm{d},2} &> I(Y; Z_2, U), && (39)\\ R_{\mathrm{d},1} + R_{\mathrm{d},2} &> I(Y; Z_1, Z_2, U) + I(Z_1; Z_2 \,|\, U), && (40)\\ R_{\mathrm{d},1} + R_{\mathrm{d},2} &> I(Y; Z_1, Z_2, U) + I(Y; U) + I(Z_1; Z_2 \,|\, U) &&\\ &= I(Y; Z_1, U) + I(Y; Z_2, U) + I(Z_1; Z_2 \,|\, U, Y). && (41) \end{aligned}$$

Clearly, conditions (37) and (40) are dominated by inequality (41), and the desired result follows. □

Proof of Achievability for Theorem 5: We further specialize Corollary 4. We choose $U = Z_1 \vee Z_2$, i.e., the common part of Z_1 and Z_2. This implies that condition (36) can be omitted, since $I(Z_1; Z_2 \,|\, U, Y) = 0$ for all $p(u, x)$ by assumption. Furthermore, U can be dropped from conditions (34) and (35) by virtue of being a function of Z_1 and Z_2. We conclude that

$$\begin{aligned} R &< H(Y), && (42)\\ R_{\mathrm{d},1} &> I(Y; Z_1), && (43)\\ R_{\mathrm{d},2} &> I(Y; Z_2), && (44) \end{aligned}$$

is achievable for all $p(x)$. Adding a time-sharing random variable Q completes the proof.

Note that in the special case where $Y \preccurlyeq Z_1$ or $Y \preccurlyeq Z_2$, the same conclusion holds with the choice $U = \emptyset$. □

D. Proof of Corollary 3

Proof of Achievability: We prove the result for $Z_1 \preccurlyeq Z_2$, the other case follows by symmetry. We specialize the achievable region of Theorem 3 by choosing $U = Z_2$. The rate–disturbance constraints are

$$\begin{aligned} R &< H(Y), && (45)\\ R_{\mathrm{d},1} + R_{\mathrm{d},2} &> 0, && (46)\\ R - R_{\mathrm{d},1} &< H(Y \,|\, Z_1), && (47)\\ R - R_{\mathrm{d},2} &< H(Y \,|\, Z_2), && (48)\\ R - R_{\mathrm{d},1} - R_{\mathrm{d},2} &< H(Y \,|\, Z_1), && (49)\\ 2R - R_{\mathrm{d},1} - R_{\mathrm{d},2} &< H(Y \,|\, Z_1) + H(Y \,|\, Z_2). && (50) \end{aligned}$$

Clearly, (46) is vacuous. Furthermore, (49) is dominated by (47), and (50) is dominated by the sum of (47) and (48). This completes the proof. □

Proof of Converse: The first inequality follows from Fano's inequality as

$$\begin{aligned} nR &\le I(X^n; Y^n) + n\epsilon_n\\ &= H(Y^n) + n\epsilon_n\\ &\le nH(Y) + n\epsilon_n, \end{aligned}$$

where $Y = Y_Q$ and $Q \sim \mathrm{Unif}[1\!:\!n]$. The other two inequalities follow as

$$\begin{aligned} n(R - R_{\mathrm{d},1}) &\le nR - I(X^n; Z_1^n)\\ &\le H(Y^n) - H(Z_1^n) + n\epsilon_n\\ &\le H(Y^n, Z_1^n) - H(Z_1^n) + n\epsilon_n\\ &= H(Y^n \,|\, Z_1^n) + n\epsilon_n\\ &\le nH(Y \,|\, Z_1) + n\epsilon_n, \end{aligned}$$

with $Z_1 = Z_{1Q}$, and likewise for $n(R - R_{\mathrm{d},2})$.

Acknowledgments

The authors would like to thank Pramod Viswanath and Yeow-Khiang Chia for helpful discussions, and the anonymous reviewers for feedback that has helped improve the paper. We used the Information Theoretic Inequalities Prover (Xitip) [16], [17] as a verification tool in some of our derivations.

Appendix

A. The Random Coding Argument for Two Figures of Merit

Consider a random sequence of codebooks $(\mathcal{C}^{(n)})$. With each codebook c, we associate a probability of error $P_e(c)$ and a secondary figure of merit $F(c) \geq 0$. Then we have the following.

Lemma 4: If

$$\mathbb{E}[P_e(\mathcal{C}^{(n)})] \leq \gamma_n,$$
$$\mathbb{E}[F(\mathcal{C}^{(n)})] \leq F_n,$$

where $\lim_{n\to\infty} \gamma_n = 0$, then for sufficiently large n, there exists a particular code $\mathcal{C}^{(n)}$ that satisfies

$$P_e(\mathcal{C}^{(n)}) \leq \zeta_n, \tag{51}$$
$$F(\mathcal{C}^{(n)}) \leq (1+\xi_n)F_n, \tag{52}$$

where $\zeta_n, \xi_n \to 0$ as $n \to \infty$.

Proof of Lemma 4: By Markov's inequality,

$$\mathrm{P}\{P_e(\mathcal{C}^{(n)}) < \gamma_n^{1/2}\} \geq 1 - \gamma_n^{1/2},$$
$$\mathrm{P}\{F(\mathcal{C}^{(n)}) < (1+\gamma_n^{1/3})F_n\} \geq 1 - 1/(1+\gamma_n^{1/3}).$$

Note that for any jointly distributed binary random variables A and B, $\mathrm{P}(A)+\mathrm{P}(B) > 1$ implies $\mathrm{P}(A,B) > 0$. For sufficiently large n,

$$\gamma_n^{1/2} + 1/(1+\gamma_n^{1/3}) < 1,$$

and thus,

$$\mathrm{P}\{P_e(\mathcal{C}^{(n)}) < \gamma_n^{1/2},\ F(\mathcal{C}^{(n)}) < (1+\gamma_n^{1/3})F_n\} > 0.$$

Hence a particular code $\mathcal{C}^{(n)}$ must exist that satisfies (51) and (52), where $\zeta_n = \gamma_n^{1/2}$ and $\xi_n = \gamma_n^{1/3}$. □

B. Proof of Lemma 1

The product bin $(m_1, m_2) = (1,1)$ for $m_0 = 1$ contains lm sequence pairs, where $l = 2^{nr_1}$ and $m = 2^{nr_2}$. Each pair $(Z_1^n(1,l_1), Z_2^n(1,l_2))$, for $l_1 \in [1:l]$ and $l_2 \in [1:m]$, has probability $p \doteq 2^{-nI(Z_1;Z_2\,|\,U)}$ to be jointly typical. Now fix one coordinate, say $l_1 = 1$. The corresponding "row" of the bin contains m sequences $Z_2^n(1,l_2)$, each of which has an independent probability of p to be jointly typical with $Z_1^n(1,1)$. Let K be the total number of typical sequences in this row. Then

$$\begin{aligned}
\mathrm{P}\{K=0\} &= (1-p)^m,\\
\mathrm{P}\{K=1\} &= mp(1-p)^{m-1},\\
\mathrm{P}\{K\geq 2\} &= 1-(1-p+mp)\underbrace{(1-p)^{m-1}}_{\geq 1-(m-1)p}\\
&\leq m^2p^2.
\end{aligned}$$

We have thus upper-bounded the probability to encounter two or more typical pairs in a single row. Consequently, the probability of two or more typical pairs occurring in *any* row is upper bounded by lm^2p^2. Substituting definitions leads to the desired inequality. The same argument can be made for columns of the bin.

C. Proof of Independence Lemma (Lemma 3)

For ease of notation, define the specialized modulo operator $[\![x]\!]$ as $x+1$ if $x < n$ and as 1 if $x = n$, the indicator function $\mathbf{1}_{\mathcal{A}'}(a) = 1$ if $a \in \mathcal{A}'$ and 0 otherwise, and the shorthand notations $Y = A_I$ and $Z = A_J$. Notice that

$$p(a^n) = \begin{cases} \frac{1}{c}\prod_{l=1}^n p_A(a_l) & \text{if } a_k \in \mathcal{A}' \text{ for some } k \in [1\!:\!n] \\ 0 & \text{otherwise,} \end{cases}$$

where c is a normalization constant, the exact value of which is not relevant. Further,

$$p(i\,|\,a^n) = \begin{cases} \frac{1}{\sum_{k=1}^n \mathbf{1}_{\mathcal{A}'}(a_k)} & \text{if } a_i \in \mathcal{A}' \\ 0 & \text{otherwise.} \end{cases}$$

The joint distribution of (A^n, I, J, Y, Z) is then

$$p(a^n, i, j, y, z) = \begin{cases} \frac{p(a^n)}{\sum_{k=1}^n \mathbf{1}_{\mathcal{A}'}(a_k)} & \begin{array}{l}\text{if } a_i \in \mathcal{A}',\, a_i = y,\\ a_j = z, \text{ and } j = [\![i+1]\!]\end{array} \\ 0 & \text{otherwise.} \end{cases}$$

Partially marginalizing, it follows that

$$p(y,z) = \sum_{i=1}^n \sum_{\substack{a^n:\ a_i\in\mathcal{A}'\\ a_i=y\\ a_{[\![i+1]\!]}=z}} \frac{p(a^n)}{\sum_{k=1}^n \mathbf{1}_{\mathcal{A}'}(a_k)}.$$

It is clear that $p(y,z) = p(y)\,p(z) = 0$ if $y \notin \mathcal{A}'$. On the other hand, for $y \in \mathcal{A}'$, we have

$$p(y,z) = \sum_{i=1}^n \sum_{\substack{a^n:\ a_i=y\\ a_{[\![i+1]\!]}=z}} \frac{\prod_{l=1}^n p_A(a_l)}{c\sum_{k=1}^n \mathbf{1}_{\mathcal{A}'}(a_k)}.$$

The fraction under the sum is invariant under permutations of a^n. Therefore,

$$\begin{aligned}
p(y,z) &= \frac{1}{c}\sum_{i=1}^n \sum_{\substack{a^n:\ a_1=y\\ a_2=z}} \frac{\prod_{l=1}^n p_A(a_l)}{\sum_{k=1}^n \mathbf{1}_{\mathcal{A}'}(a_k)}\\
&= \frac{n}{c}\sum_{a^n=(y,z,a_3^n)} \frac{\prod_{l=1}^n p_A(a_l)}{\sum_{k=1}^n \mathbf{1}_{\mathcal{A}'}(a_k)}\\
&= \frac{n\ p_A(y)\ p_A(z)}{c}\sum_{a_3^n\in\mathcal{A}^{n-2}} \frac{\prod_{l=3}^n p_A(a_l)}{1+\mathbf{1}_{\mathcal{A}'}(z)+\sum_{k=3}^n \mathbf{1}_{\mathcal{A}'}(a_k)},
\end{aligned}$$

where a_3^n are the last $n-2$ components of a^n. Observe that $p(y,z)$ separates into a function of z and a function of y. Independence is thus established.

D. Proof of Lemma 2, Exemplified for $\mathcal{E}_3$

We analyze the probability of $\mathcal{E}_3$ as follows.

$$\begin{aligned}
\mathcal{E}_3 = \big\{&\big(U^n(1), Z_1^n(1, L_1^{(1,1,m_2)}), Z_2^n(1, L_2^{(1,1,m_2)}),\\
&X^n(1, L_1^{(1,1,m_2)}, L_2^{(1,1,m_2)}, m_3), Y^n\big) \in \mathcal{T}_\varepsilon^{(n)},\\
&\text{for some } m_2 \neq 1,\, m_3\big\}\\
\subseteq \big\{&\big(U^n(1), Z_1^n(1, L_1^{(1,1,m_2)}), Z_2^n(1, l_2),\\
&X^n(1, L_1^{(1,1,m_2)}, l_2, m_3), Y^n\big) \in \mathcal{T}_\varepsilon^{(n)},\\
&\text{for some } m_2 \neq 1,\, m_3,\, l_2 \notin \mathcal{L}_2(1)\big\},
\end{aligned}$$

Define the event $\mathcal{E}_{\mathrm{eq}} = \{L_1^{(1,1,m_2)} = L_1^{(1,1,1)}\}$, which allows us to write $\mathrm{P}(\mathcal{E}_3 \mid \mathcal{E}_{\mathrm{e}}^c) = \mathrm{P}(\mathcal{E}_3 \cap \mathcal{E}_{\mathrm{eq}} \mid \mathcal{E}_{\mathrm{e}}^c) + \mathrm{P}(\mathcal{E}_3 \cap \mathcal{E}_{\mathrm{eq}}^c \mid \mathcal{E}_{\mathrm{e}}^c)$. We consider both terms separately.

$$\begin{aligned}\mathcal{E}_3 \cap \mathcal{E}_{\mathrm{eq}} \subseteq \big\{&\big(U^n(1), Z_1^n(1, L_1^{(1,1,1)}), Z_2^n(1, l_2),\\ &X^n(1, L_1^{(1,1,1)}, l_2, m_3), Y^n\big) \in \mathcal{T}_\varepsilon^{(n)},\\ &\text{for some } l_2 \notin \mathcal{L}_2(1), m_3\big\}.\end{aligned}$$

Thus,

$$\begin{aligned}&\mathrm{P}(\mathcal{E}_3 \cap \mathcal{E}_{\mathrm{eq}} \mid \mathcal{E}_{\mathrm{e}}^c)\\ &\le \sum_{(u^n, z_1^n, y^n) \in \mathcal{T}_\varepsilon^{(n)}} \mathrm{P}\big\{U^n(1) = u^n, Z_1^n(1, L_1^{(1,1,1)}) = z_1^n,\\ &\qquad\qquad Y^n = y^n \mid \mathcal{E}_{\mathrm{e}}^c\big\}\\ &\quad\cdot \sum_{l_2 \notin \mathcal{L}_2(1)} \sum_{m_3=1}^{2^{nR_3}} \mathrm{P}\big\{(u^n, z_1^n, Z_2^n(1, l_2),\\ &\qquad\qquad X^n(1, L_1^{(1,1,1)}, l_2, m_3), y^n) \in \mathcal{T}_\varepsilon^{(n)} \mid \mathcal{E}_{\mathrm{e}}^c\big\}\\ &\le 2^{n(\tilde{R}_2 + R_3)}\ P^\star,\end{aligned}$$

where $P^\star$ is shorthand for the last $\mathrm{P}\{\cdot\}$ expression. Continue with

$$\begin{aligned}P^\star &= \sum_{\substack{(z_2^n, x^n) \in \mathcal{T}_\varepsilon^{(n)}(\\ Z_2, X \mid u^n, z_1^n, y^n)}} \mathrm{P}\big\{Z_2^n(1, l_2) = z_2^n, X^n(1, L_1^{(1,1,1)}, l_2, m_3) = x^n \mid\\ &\qquad\qquad U^n(1) = u^n, Z_1^n(1, L_1^{(1,1,1)}) = z_1^n,\\ &\qquad\qquad Y^n = y^n, \mathcal{E}_{\mathrm{e}}^c\big\}\\ &\overset{(a)}{=} \underbrace{\sum_{\substack{(z_2^n, x^n) \in \mathcal{T}_\varepsilon^{(n)}(\\ Z_2, X \mid u^n, z_1^n, y^n)}}}_{\doteq 2^{nH(X, Z_2 \mid Z_1, Y, U)}} \underbrace{p(z_2^n \mid u^n)}_{\doteq 2^{-nH(Z_2 \mid U)}} \underbrace{p(x^n \mid z_1^n, z_2^n, u^n)}_{\doteq 2^{-nH(X \mid Z_1, Z_2, U)}}\\ &\le 2^{n(H(X, Z_2 \mid Z_1, Y, U) - H(Z_2 \mid U) - H(X \mid Z_1, Z_2, U) + \delta(\varepsilon))}\\ &= 2^{n(-H(Y \mid Z_1, U) - I(Z_1; Z_2 \mid U) + \delta(\varepsilon))}.\end{aligned}$$

In step (a), we have used the fact that $l_2 \notin \mathcal{L}_2(1)$, and therefore, $Z_2^n(1, l_2)$ relates to a product set other than the first one. It is independent of the conditions $Y^n = y^n$ and $\mathcal{E}_{\mathrm{e}}^c$, both of which relate only to the product set $(1, 1)$ for $m_0 = 1$. A similar argument applies to the second term.

Substituting back in the previous chain of inequalities implies that $\mathrm{P}(\mathcal{E}_3 \cap \mathcal{E}_{\mathrm{eq}} \mid \mathcal{E}_{\mathrm{e}}^c) \to 0$ as $n \to \infty$ if inequality (28) holds.

Next, consider

$$\begin{aligned}\mathcal{E}_3 \cap \mathcal{E}_{\mathrm{eq}}^c \subseteq \big\{&\big(U^n(1), Z_1^n(1, l_1), Z_2^n(1, l_2), X^n(1, l_1, l_2, m_3),\\ &Y^n\big) \in \mathcal{T}_\varepsilon^{(n)}, \text{ for some } l_1 \in \mathcal{L}_1(1) \setminus \{L_1^{(1,1,1)}\},\\ &l_2 \notin \mathcal{L}_2(1), m_3\big\}\\ = \big\{&\big(U^n(1), Z_1^n(1, L_1^{(1,1,1)} + l_1), Z_2^n(1, l_2),\\ &X^n(1, L_1^{(1,1,1)} + l_1, l_2, m_3), Y^n\big) \in \mathcal{T}_\varepsilon^{(n)},\\ &\text{for some } l_1 \neq 0, l_2 \notin \mathcal{L}_2(1), m_3\big\},\end{aligned}$$

where the index l_1 in the last line can take values between 1 and $|\mathcal{L}_1(1)| - 1$, and the addition $L_1^{(1,1,1)} + l_1$ in the index is understood modulo the set $\mathcal{L}_1(1)$. We argue

$$\begin{aligned}&\mathrm{P}(\mathcal{E}_3 \cap \mathcal{E}_{\mathrm{eq}}^c \mid \mathcal{E}_{\mathrm{e}}^c)\\ &\le \sum_{(u^n, y^n) \in \mathcal{T}_\varepsilon^{(n)}} \mathrm{P}\big\{U^n(1) = u^n, Y^n = y^n \mid \mathcal{E}_{\mathrm{e}}^c\big\} \sum_{l_1 \neq 0} \sum_{l_2 \notin \mathcal{L}_2(1)}\\ &\quad \sum_{m_3=1}^{2^{nR_3}} \mathrm{P}\big\{(u^n, Z_1^n(1, L_1^{(1,1,1)} + l_1), Z_2^n(1, l_2),\\ &\qquad\qquad X^n(1, L_1^{(1,1,1)} + l_1, l_2, m_3), y^n) \in \mathcal{T}_\varepsilon^{(n)} \mid\\ &\qquad\qquad U^n(1) = u^n, Y^n = y^n, \mathcal{E}_{\mathrm{e}}^c\big\}\\ &\le 2^{n(\tilde{R}_1 - R_1 + \tilde{R}_2 + R_3)}\ P^{\star\star},\end{aligned}$$

where $P^{\star\star}$ represents the last $\mathrm{P}\{\cdot\}$ expression. Continue with

$$\begin{aligned}P^{\star\star} &\overset{(a)}{=} \sum_{\substack{(z_1^n, z_2^n, x^n) \in \mathcal{T}_\varepsilon^{(n)}\\ (Z_1, Z_2, X \mid u^n, y^n)}} \mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n, Z_2^n(1, l_2) = z_2^n,\\ &\qquad\qquad X^n(1, L_1^{(1,1,1)} + 1, l_2, m_3) = x^n \mid\\ &\qquad\qquad U^n(1) = u^n, Y^n = y^n, \mathcal{E}_{\mathrm{e}}^c\big\}\\ &= \sum_{\substack{(z_1^n, z_2^n, x^n) \in \mathcal{T}_\varepsilon^{(n)}(\\ Z_1, Z_2, X \mid u^n, y^n)}} \sum_{\substack{z_2^n(l_2'), \text{ for}\\ \text{all } l_2' \in \mathcal{L}_2(1)}} \mathrm{P}\big\{Z_2^n(1, l_2') = z_2^n(l_2')\\ &\qquad\qquad \text{for all } l_2' \in \mathcal{L}_2(1) \mid\\ &\qquad\qquad U^n(1) = u^n,\\ &\qquad\qquad Y^n = y^n, \mathcal{E}_{\mathrm{e}}^c\big\}\\ &\quad\cdot \mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n, Z_2^n(1, l_2) = z_2^n,\\ &\qquad\qquad X^n(1, L_1^{(1,1,1)} + 1, l_2, m_3) = x^n \mid\\ &\qquad\qquad U^n(1) = u^n, Y^n = y^n, Z_2^n(1, l_2') = z_2^n(l_2')\\ &\qquad\qquad \text{for all } l_2' \in \mathcal{L}_2(1), \mathcal{E}_{\mathrm{e}}^c\big\},\end{aligned} \tag{53}$$

where in (a), we are allowed to set $l_1 = 1$ without loss of generality due to symmetry. The index $L_1^{(1,1,1)} + 1$ is representative for all indices that are not selected in step 5 of the codebook generation procedure. We decompose the last probability term as

$$\begin{aligned}&\mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n \mid U^n(1) = u^n, Y^n = y^n,\\ &\qquad Z_2^n(1, l_2') = z_2^n(l_2') \text{ for all } l_2' \in \mathcal{L}_2(1), \mathcal{E}_{\mathrm{e}}^c\big\}\\ &\mathrm{P}\big\{Z_2^n(1, l_2) = z_2^n \mid U^n(1) = u^n, Y^n = y^n,\\ &\qquad Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n,\\ &\qquad Z_2^n(1, l_2') = z_2^n(l_2') \text{ for all } l_2' \in \mathcal{L}_2(1), \mathcal{E}_{\mathrm{e}}^c\big\}\\ &\mathrm{P}\big\{X^n(1, L_1^{(1,1,1)} + 1, l_2, m_3) = x^n \mid U^n(1) = u^n,\\ &\qquad Y^n = y^n, Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n,\\ &\qquad Z_2^n(1, l_2') = z_2^n(l_2') \text{ for all } l_2' \in \mathcal{L}_2(1),\\ &\qquad Z_2^n(1, l_2) = z_2^n, \mathcal{E}_{\mathrm{e}}^c\big\},\end{aligned} \tag{54}$$

and consider each factor separately. To analyze the first factor, note that

$$\begin{aligned}&Z_1^n(1, L_1^{(1,1,1)} + 1)\\ &- \big(U^n(1), Z_2^n(1, l_2') \text{ for all } l_2' \in \mathcal{L}_2(1), \mathcal{E}_{\mathrm{e}}^c, Z_1^n(1, L_1^{(1,1,1)})\big)\\ &- Y^n\end{aligned} \tag{55}$$

forms a Markov chain by codebook construction. Since $\mathcal{E}_{\mathrm{e}}$ includes the event $\mathcal{E}_{\mathrm{e}2}$, the middle term of the chain uniquely determines $Z_2^n(1, L_2^{(1,1,1)})$ on which the transmitted codeword is conditioned. Further,

$$\begin{aligned} &Z_1^n(1, L_1^{(1,1,1)} + 1)\\ &\quad - \big(U^n(1), Z_2^n(1, l_2') \text{ for all } l_2' \in \mathcal{L}_2(1), \mathcal{E}_{\mathrm{e}}^c\big)\\ &\quad - Z_1^n(1, L_1^{(1,1,1)}) \end{aligned} \tag{56}$$

forms another Markov chain. This follows from Lemma 3, where the left and right term in the chain play the role of A_J and A_I, respectively, and the middle term in the chain determines the set $\mathcal{A}'$ as

$$\mathcal{T}^\star = \bigcup_{l_2' \in \mathcal{L}_2(1)} \mathcal{T}_{\varepsilon'}^{(n)}(Z_1 \,|\, u^n, z_2^n(l_2')). \tag{57}$$

Since the event $\mathcal{E}_{\mathrm{e}}$ includes $\mathcal{E}_{\mathrm{e2}}$, it is ensured that I is drawn uniformly, as required by the lemma.

It is straightforward to verify that if $A - (B, C) - D$ and $A - B - C$ form Markov chains, then so does $A - B - D$. Hence, (55) and (56) imply the Markov chain

$$\begin{aligned} &Z_1^n(1, L_1^{(1,1,1)} + 1)\\ &\quad - \big(U^n(1), Z_2^n(1, l_2') \text{ for all } l_2' \in \mathcal{L}_2(1), \mathcal{E}_{\mathrm{e}}^c\big)\\ &\quad - Y^n, \end{aligned}$$

and the conditioning on $Y^n = y^n$ in the first factor of (54) can be omitted. We are left with

$$\begin{aligned} \mathrm{P}\big\{&Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n \,|\, U^n(1) = u^n,\\ &\underbrace{Z_2^n(1, l_2') = z_2^n(l_2') \text{ for all } l_2' \in \mathcal{L}_2(1), \mathcal{E}_{\mathrm{e}}^c}_{\mathcal{E}_{\mathrm{cond}}}\big\}. \end{aligned}$$

To simplify further, consider the conditional joint distribution of all sequences $Z_1^n(1, L_1^{(1,1,1)} + k)$ for $k \in [0 : |\mathcal{L}_1(1)| - 1]$ given $U^n(1) = u^n$. The effect of additionally conditioning on $\mathcal{E}_{\mathrm{cond}}$ relates to the typical sets $\mathcal{T}_{\varepsilon'}^{(n)}(Z_1 \,|\, u^n, z_2^n(l_2'))$ for $l_2' \in \mathcal{L}_2(1)$, and imposes that (a) the $k = 0$ sequence is in one of the typical sets, (b) no sequence is in more than one of the typical sets, and (c) none of typical sets contains more than one sequence. The latter two are exclusion constraints. We are interested in the marginal with respect to the $k = 1$ sequence, i.e., $Z_1^n(1, L_1^{(1,1,1)} + 1)$. If $z_1^n \in \mathcal{T}^\star$, where $\mathcal{T}^\star$ is the union of the typical sets as defined in (57), we have

$$\begin{aligned} &\mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n \,|\, U^n(1) = u^n, \mathcal{E}_{\mathrm{cond}}\big\}\\ &\qquad \le \mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n \,|\, U^n(1) = u^n\big\}, \end{aligned} \tag{58}$$

that is, conditioning on $\mathcal{E}_{\mathrm{cond}}$ makes it less probable for $Z_1^n(1, L_1^{(1,1,1)} + 1)$ to be within $\mathcal{T}^\star$ due to the exclusion constraints with respect to the subsets of $\mathcal{T}^\star$.

On the other hand, if $z_1^n \notin \mathcal{T}^\star$, we have

$$\begin{aligned} &\mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n \,|\, U^n(1) = u^n, \mathcal{E}_{\mathrm{cond}}\big\}\\ &\quad \overset{\text{(a)}}{\le} \mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n \,|\, U^n(1) = u^n,\\ &\qquad\qquad Z_1^n(1, L_1^{(1,1,1)} + 1) \notin \mathcal{T}^\star\big\}\\ &\quad \le \frac{\mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n \,|\, U^n(1) = u^n\big\}}{\mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) \notin \mathcal{T}^\star \,|\, U^n(1) = u^n\big\}}, \end{aligned} \tag{59}$$

where in step (a), we have pessimistically assumed that $\mathcal{E}_{\mathrm{cond}}$ excludes $Z_1^n(1, L_1^{(1,1,1)} + 1)$ from the entire set $\mathcal{T}^\star$. To bound (58) and (59) further, we need the following lemma, which is proved at the end of the section.

Lemma 5: For any $\widetilde{\mathcal{Z}_1^n} \subseteq \mathcal{Z}_1^n$, if the conditions in Lemma 1 hold, then

$$\begin{aligned} \lim_{n\to\infty} &\mathrm{P}\{Z_1^n(1, L_1^{(1,1,1)} + 1) \in \widetilde{\mathcal{Z}_1^n} \,|\, U_1^n(1) = u^n\}\\ &\qquad = \mathrm{P}\{Z_1^n(1, 1) \in \widetilde{\mathcal{Z}_1^n} \,|\, U_1^n(1) = u^n\}. \end{aligned}$$

The lemma states that the distribution of a nonselected Z_1^n sequence tends to the distribution of a sequence before the selection process. Applying the lemma to the right-hand side in (58) and the numerator in (59) immediately yields

$$\begin{aligned} \mathrm{P}\big\{&Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n \,|\, U^n(1) = u^n\big\}\\ &\overset{\text{(a)}}{\le} \mathrm{P}\big\{Z_1^n(1, 1) = z_1^n \,|\, U^n(1) = u^n\big\} + \varepsilon_n\\ &\doteq 2^{-nH(Z_1 \,|\, U)}, \end{aligned}$$

where in (a), $\varepsilon_n \to 0$ as $n \to \infty$. Applying the lemma to the denominator of (59) yields

$$\begin{aligned} \mathrm{P}\big\{&Z_1^n(1, L_1^{(1,1,1)} + 1) \notin \mathcal{T}^\star \,|\, U^n(1) = u^n\big\}\\ &\ge 1 - \mathrm{P}\big\{Z_1^n(1, 1) \in \mathcal{T}^\star \,|\, U^n(1) = u^n\big\} - \varepsilon_n\\ &\overset{\text{(a)}}{\ge} 1 - |\mathcal{T}^\star| \cdot 2^{n(-H(Z_1 \,|\, U) + \delta(\varepsilon'))} - \varepsilon_n\\ &\overset{\text{(b)}}{\ge} 1 - 2^{n(\tilde{R}_2 - R_2 - I(Z_1; Z_2 \,|\, U) + 2\delta(\varepsilon'))} - \varepsilon_n\\ &\overset{\text{(c)}}{\longrightarrow} 1 \quad \text{as } n \to \infty, \end{aligned}$$

where (a) follows from $\mathcal{T}^\star \subseteq \mathcal{T}_{\varepsilon'}^{(n)}(Z_1 \,|\, u^n)$, (b) uses

$$\begin{aligned} |\mathcal{T}^\star| &\le |\mathcal{L}_2(1)| \cdot 2^{n(H(Z_1 \,|\, U, Z_2) + \delta(\varepsilon'))}\\ &= 2^{n(\tilde{R}_2 - R_2 + H(Z_1 \,|\, U, Z_2) + \delta(\varepsilon'))}, \end{aligned}$$

and (c) relies on the conditions of Lemma 1, which ensure that $\tilde{R}_2 - R_2 < I(Z_1; Z_2 \,|\, U)$. Substituting into (58) and (59), we conclude that for all z_1^n,

$$\begin{aligned} \mathrm{P}\big\{Z_1^n(1, L_1^{(1,1,1)} + 1) &= z_1^n \,|\, U^n(1) = u^n, \mathcal{E}_{\mathrm{cond}}\big\}\\ &\le 2^{-n(H(Z_1 \,|\, U) - \delta(\varepsilon'))}, \end{aligned}$$

where $\delta(\varepsilon') \to 0$ as $n \to \infty$ and thus, we have bounded the first factor in (54).

The second factor in (54) simplifies as

$$\begin{aligned} \mathrm{P}\big\{&Z_2^n(1, l_2) = z_2^n \,|\, U^n(1) = u^n, Y^n = y^n,\\ &\qquad Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n, \mathcal{E}_{\mathrm{e}}^c\big\}\\ &\overset{\text{(a)}}{=} \mathrm{P}\big\{Z_2^n(1, l_2) = z_2^n \,|\, U^n(1) = u^n\big\}\\ &\doteq 2^{-nH(Z_2|U)}, \end{aligned}$$

where (a) follows from $l_2 \notin \mathcal{L}_2(1)$ and the fact that the conditions $Y^n = y^n$, $Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n$, and $\mathcal{E}_{\mathrm{e}}^c$ relate only to the product set $\mathcal{L}_1(1) \times \mathcal{L}_2(1)$ for $m_0 = 1$.

Similarly, the third factor in (54) evaluates to

$$\begin{aligned}
&\mathrm{P}\big\{X^n(1, L_1^{(1,1,1)} + 1, l_2, m_3) = x^n \mid U^n(1) = u^n, Y^n = y^n,\\
&\qquad Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n, Z_2^n(1, l_2) = z_2^n, \mathcal{E}_{\mathrm{e}}^c\big\}\\
&\quad = \mathrm{P}\big\{X^n(1, L_1^{(1,1,1)} + 1, l_2, m_3) = x^n \mid U^n(1) = u^n,\\
&\qquad Z_1^n(1, L_1^{(1,1,1)} + 1) = z_1^n, Z_2^n(1, l_2) = z_2^n\big\}\\
&\quad \doteq 2^{-nH(X|Z_1,Z_2,U)}.
\end{aligned}$$

Substituting the bounds for the three factors in (54) back into (53), and noting that

$$|\mathcal{T}_\varepsilon^{(n)}(Z_1, Z_2, X \mid u^n, y^n)| \doteq 2^{nH(X,Z_1,Z_2|Y,U)},$$

we conclude

$$\begin{aligned}
P^{\star\star} &\le 2^{n(H(X,Z_1,Z_2|Y,U)-H(Z_1|U)-H(Z_2|U)-H(X|Z_1,Z_2,U)+\delta(\varepsilon))}\\
&= 2^{n(-H(Y|U)-I(Z_1;Z_2|U)+\delta(\varepsilon))}.
\end{aligned}$$

Finally, this implies that $\mathrm{P}(\mathcal{E}_3 \cap \mathcal{E}_{\mathrm{eq}}^c \mid \mathcal{E}_{\mathrm{e}}^c) \to 0$ as $n \to \infty$ if

$$\tilde{R}_1 - R_1 + \tilde{R}_2 + R_3 \le H(Y|U) + I(Z_1; Z_2|U) - \delta(\varepsilon).$$

But this condition is an implication of (29) which stems from analyzing $\mathcal{E}_4$, and may thus be omitted.

To complete the proof, it remains to show Lemma 5.

Proof of Lemma 5: We express the term on the right hand side as follows.

$$\begin{aligned}
&\mathrm{P}\{Z_1^n(1,1) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\}\\
&\quad = \sum_{l_1^\star \in \mathcal{L}_1(1)} \mathrm{P}\{L_1^{(1,1,1)} = l_1^\star, Z_1^n(1,1) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\}\\
&\quad = \frac{1}{|\mathcal{L}_1(1)|} \sum_{l_1^\star \in \mathcal{L}_1(1)} \mathrm{P}\{Z_1^n(1,1) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n,\\
&\qquad\qquad L_1^{(1,1,1)} = l_1^\star\}\\
&\quad \overset{(a)}{=} \tfrac{1}{|\mathcal{L}_1(1)|}\ \mathrm{P}\{Z_1^n(1, L_1^{(1,1,1)}) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\}\\
&\qquad + \tfrac{|\mathcal{L}_1(1)|-1}{|\mathcal{L}_1(1)|}\ \mathrm{P}\{Z_1^n(1, L_1^{(1,1,1)} + 1) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\},
\end{aligned}$$

where (a) follows from symmetry, which implies that $\mathrm{P}\{Z_1^n(1, L_1^{(1,1,1)} + k) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\}$ for $k \neq 0$ is independent of k.

Hence,

$$\begin{aligned}
&\mathrm{P}\{Z_1^n(1, L_1^{(1,1,1)} + 1) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\}\\
&\qquad \le \tfrac{|\mathcal{L}_1(1)|}{|\mathcal{L}_1(1)|-1} \mathrm{P}\{Z_1^n(1,1) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\},\\
&\mathrm{P}\{Z_1^n(1, L_1^{(1,1,1)} + 1) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\}\\
&\qquad \ge \tfrac{|\mathcal{L}_1(1)|}{|\mathcal{L}_1(1)|-1} \mathrm{P}\{Z_1^n(1,1) \in \widetilde{\mathcal{Z}_1^n} \mid U_1^n(1) = u^n\} - \tfrac{1}{|\mathcal{L}_1(1)|-1},
\end{aligned}$$

Recall that $|\mathcal{L}_1(1)| = 2^{n(\tilde{R}_1 - R_1)}$, and therefore, by the conditions of Lemma 1, $|\mathcal{L}_1(1)| \to \infty$ as $n \to \infty$. This completes the proof of the lemma.

REFERENCES

[1] B. Bandemer and A. El Gamal, "Communication with disturbance constraints," in *Proc. ISIT*, St. Petersburg, Russia, Aug. 2011.

[2] B. Bandemer and A. El Gamal, "An achievable rate region for the 3-user-pair deterministic interference channel," in *Proc. 49th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2011.

[3] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.

[4] H.-F. Chong, M. Motani, H. K. Garg, and H. El Gamal, "On the Han–Kobayashi region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3188–3195, Jul. 2008.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[7] A. A. El Gamal and M. H. M. Costa, "The capacity region of a class of deterministic interference channels (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 28, no. 2, pp. 343–346, Mar. 1982.

[8] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[9] T. Liu and P. Viswanath, "An extremal inequality motivated by multiterminal information theoretic problems," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1839–1851, May 2007.

[10] R. P. Stanley, *Enumerative Combinatorics*, vol. 1, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[11] P. Gács and J. Körner, "Common information is far less than mutual information," *Problems Control Inform. Theory*, vol. 2, no. 2, pp. 149–162, 1973.

[12] H. S. Witsenhausen, "On sequences of pairs of dependent random variables," *SIAM J. Appl. Math.*, vol. 28, no. 1, pp. 100–113, Jan. 1975.

[13] R. von Mises, "Über Aufteilungs- und Besetzungs-Wahrscheinlichkeiten," *Revue Faculté Sci. l'Université d'Istanbul*, vol. 4, pp. 145–163, 1939.

[14] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 3, pp. 306–311, May 1979.

[15] A. El Gamal and E. C. van der Meulen, "A proof of Marton's coding theorem for the discrete memoryless broadcast channel (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 120–122, Jan. 1981.

[16] R. Pulikkoonattu. (2008, Jan.). Information theoretic inequalities prover 'Xitip' [Online]. Available: http://xitip.epfl.ch/

[17] R. W. Yeung and Y.-O. Yan. (2014, Jun. 15). *Information Theoretic Inequality Prover* [Online]. Available: http://user-www.ie.cuhk.edu.hk/~ITIP/

Bernd Bandemer (S'06–M'12) received the Dipl.-Ing. degree in Electrical and Computer Engineering in 2006 from Ilmenau University of Technology, Ilmenau, Germany and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, in 2012. From 2012 to 2013, he was a postdoctoral researcher at the Information Theory and Applications Center at the University of California in San Diego. In October 2013 he joined the Bosch Research and Technology Center in Palo Alto, CA, USA. His research interests include network information theory, wireless communications, machine learning and data mining.

Abbas El Gamal (S'71–M'73–SM'83–F'00) is the Hitachi America Professor in the School of Engineering and the Chair of the Department of Electrical Engineering at Stanford University. He received his B.Sc. Honors degree from Cairo University in 1972, and his M.S. in Statistics and Ph.D. in Electrical Engineering both from Stanford University in 1977 and 1978, respectively. From 1978 to 1980, he was an Assistant Professor of Electrical Engineering at USC. From 2004 to 2009, he was the Director of the Information Systems Laboratory at Stanford University. His research contributions have been in network information theory, FPGAs, and digital imaging devices and systems. He has authored or coauthored over 200 papers and holds 35 patents in these areas. He is coauthor of the book Network Information Theory (Cambridge Press 2011). He has received several honors and awards for his research contributions, including the 2012 Claude E. Shannon Award and the 2004 INFOCOM Paper Award. He is a member of the US National Academy of Engineering. He serves on the Board of Directors of the Information Theory Society and is currently President. He has cofounded and served on the board of directors and advisory boards of several semiconductor and biotechnology startup companies.