Identification over quantum broadcast channels

Johannes Rosenberger[1] · **Christian Deppe**[1] · **Uzi Pereg**[1,2,3,4]

Abstract

Identification over quantum broadcast channels is considered. As opposed to the information transmission task, the decoder only identifies whether a message of his choosing was sent or not. This relaxation allows for a double-exponential code size. An achievable identification region is derived for a quantum broadcast channel, and a full characterization for the class of classical-quantum broadcast channels. The identification capacity region of the single-mode pure-loss bosonic broadcast channel is obtained as a consequence. Furthermore, the results are demonstrated for the quantum erasure broadcast channel, where our region is suboptimal, but improves on the best previously known bounds.

1 Introduction

Modern data systems have an ever-growing gap between the available information storage and the bit-per-second rates, which are limited by the noisy transmission

✉ Johannes Rosenberger
johannes.rosenberger@tum.de

Christian Deppe
christian.deppe@tum.de

Uzi Pereg
uzipereg@technion.ac.il

1   Department of Computer Engineering, School of Computation, Information and Technology,
     Technical University of Munich, Munich, Germany

2   Munich Center for Quantum Science and Technology, Munich, Germany

3   Department of Electrical and Computer Engineering, Technion - Israel Institute of Technology,
   Haifa, Israel

4   Helen Diller Quantum Center, Technion - Israel Institute of Technology, Haifa, Israel

medium [1]. Quantum communication is thus expected to enter the sixth generation of cellular networks (6G) in order to achieve performance gains [2–4].

Data volumes are even larger when limiting a system to identifying alerts, rather than recovering information. In Shannon's transmission task [5], a transmitter sends a message over a noisy channel, and the receiver needs to find which message was sent. In some modern event-triggered applications, however, the receiver may simply perform a binary decision on whether a particular message of interest was sent or not. This setting is known as identification via channels [6]. Identification (ID) is relevant for various applications such as watermarking [7–9] and sensor communication [10]. In vehicle-to-X communication [11], a vehicle may announce information about its future movements to the surrounding road users. Every road user is interested in one specific movement that interferes with its plans, and it checks only if this movement is announced or not.

The ID capacity of a classical-quantum channel was determined by Löber [12] and Ahlswede and Winter [13] (see also [14]). The ID capacity turns out to have the same value as the transmission capacity for most classical-input single-user channels that we know of. However, the units are different. Specifically, the ID code size grows doubly exponentially in the block length, provided that the encoder has access to a source of randomness. Thereby, identification codes achieve an exponential advantage in throughput compared to transmission codes. This is attained by letting the encoding and decoding sets overlap. General results for ID are surveyed in [15]. Löber [12] considered a simultaneous identification scenario, in which the same measurement is performed in order to perform identification for multiple receivers. This is also relevant to a network that consists of chains [16]. In Boche et al. [17] considered identification over the classical-quantum channel under channel uncertainty and secrecy constraints. For quantum-quantum channels, even the single-user identification capacity is unknown so far, except for special channels [14]. In general, it can exceed the transmission capacity of a quantum channel [14] and was recently shown to exceed the simultaneous identification capacity [18]. For example, the transmission capacity and the simultaneous identification capacity of the noiseless qubit channel are both one [18, 19], but the identification capacity of the noiseless qubit channel is 2 and equals the entanglement-assisted transmission capacity [14]. The best lower bounds equal the amount of common randomness that can be generated over a channel, and thus, entanglement also increases the identification capacity [14].

The broadcast channel is a fundamental multi-user communication model, whereby a single transmitter sends messages to two receivers [20]. In the traditional transmission setting, the capacity region of the discrete memoryless broadcast channel is generally unknown, even in the classical case. The best known lower bound is due to Marton [21], and the best known upper bound was proven by Nair and El Gamal [22]. The two bounds coincide in special cases such as more capable, less noisy or degraded broadcast channel [23]. On the other hand, the ID capacity region of the classical broadcast channel was fully characterized by Bracher and Lapidoth [24, 25], for uniformly distributed messages. Namely, the ID capacity region is known for *any* classical discrete memoryless broadcast channel, without special requirements on the channel. The derivation in [24, 25] is based on a pool-selection technique that differs from the standard arguments. Related settings were also considered in [26–28]. The authors of the
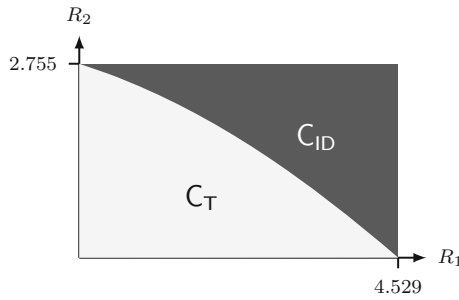
Fig. 1 The transmission and ID capacity regions of the pure-loss bosonic broadcast channel, with coherent-state encoding, mean photon-number input constraint $N_A = 10$, and transmissivity $\eta = 0.8$. The transmission capacity region C_T corresponds to the light gray area, and the ID capacity region C_{ID} comprises additionally the dark gray rectangular area

present paper have recently considered ID over the classical compound multiple-input multiple-output (MIMO) broadcast channel [29, 30].

Quantum broadcast channels were studied in various settings [31–46]. Yard et al. [31] derived the superposition inner bound and determined the capacity region for the degraded classical-quantum broadcast channel. Wang et al. [34] used the previous characterization to determine the capacity region for Hadamard broadcast channels. Dupuis et al. [35, 36] developed the entanglement-assisted version of Marton's region. Quantum broadcast channels with conferencing decoders were recently considered in [47] as well, providing an information-theoretic perspective to the operation of quantum repeaters. In addition, security aspects were treated in [48, 49].

Optical communication forms the backbone of the Internet [50–53]. The Gaussian bosonic channel is a simple quantum-mechanical model for optical communication over free space or optical fibers [54, 55]. An optical communication system consists of a modulated source of photons, the optical channel, and an optical detector. For a single-mode bosonic broadcast channel, the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is a pair of modes with annihilation operators $\hat{b}_1$ and $\hat{b}_2$, corresponding to each receiver. Bosonic broadcast channels are considered in different settings in [56–63].

In this work, we consider identification over the quantum broadcast channel. We derive an achievable ID rate region for the general quantum broadcast channel and establish full characterization for the classical-quantum broadcast channel under a semi-average error criterion. We demonstrate our results and determine the ID capacity region of the quantum erasure broadcast channel. Furthermore, we establish the capacity region of the single-mode pure-loss bosonic broadcast channel with coherent-state encoding. The ID capacity region of the bosonic broadcast channel is depicted in Fig. 1 as the area below the solid blue line. For comparison, the transmission capacity region, as determined by Guha and Shapiro [56] subject to the minimum output-entropy conjecture, is indicated by the red dashed line. It can be seen that the ID capacity region is significantly larger than the transmission counterpart. We note that the ID result does not require the conjecture.

While the properties above are analogous to the classical setting [30], the analysis is more involved. To prove the direct part, we extend the pool-selection method due to Bracher and Lapidoth [24, 25] to the quantum setting. On the other hand, our converse proof is based on completely different arguments than in Bracher and Lapidoth's classical proof. Instead, we exploit recent observations made by Boche et al. [17] as they treated the classical-quantum compound channel, combined with the arguments of Ahlswede and Winter [13] in their seminal paper on ID for the single-user classical-quantum channel.

This paper is organized as follows: In Sect. 2, we introduce the notation, give basic definitions, and introduce the communication model. Section 3 contains our main results. In Sect. 4, we demonstrate our results for the pure-loss bosonic broadcast channel and the erasure broadcast channel. Section 5 provides the achievability proof for identification over the quantum broadcast channel in finite dimensions, and Sect. 6 provides the proof for the ID capacity region of the classical-quantum broadcast channel. Finally, the results are summarized in Sect. 7.

2 Preliminaries and related work

2.1 Notation

We use the following notation conventions.

2.1.1 Basic notation

$X, Y, \ldots$	Classical random variables
$\mathcal{X}, \mathcal{Y}, \ldots$	Finite sets (alphabets)
$x, y, \ldots$	Constants and classical values
$x^n = (x_1, x_2, \ldots, x_n) \in \mathcal{X}^n$	Sequence of length n
P_X	Probability mass function (PMF) of X
$\mathbb{E}[X]$	Expectation of a random variable X
$\mathcal{P}(\mathcal{X})$	Set of all PMFs with finite support over a set $\mathcal{X}$
$P^n(x^n) = \prod_{t=1}^{n} P(x_t)$	n-fold product distribution
$[N]$	$\{1, \ldots, \lceil N \rceil\}$
$A, B, \ldots$	Quantum systems
$\mathcal{H}_A$	Hilbert space A
$\rho_A \in \mathscr{D}(\mathcal{H}_A)$	Density operator on $\mathcal{H}_A$
$\mathscr{D}(\mathcal{H}_A)$	Set of density operators on $\mathcal{H}_A$
$\mathcal{N}_{A \to B} : \mathscr{D}(\mathcal{H}_A) \to \mathscr{D}(\mathcal{H}_B)$	Quantum channel (CPTP map)
$\{D_j : j \in [J]\}$	Positive operator-valued measure (POVM),
$\|\Phi_{AB}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} \|i\rangle_A \otimes \|i\rangle_B$	A maximally entangled state of dimension d

2.1.2 Information measures

$H(X) = \sum\limits_{x \in \text{supp } P_X} -P_X(x) \log_2 P_X(x)$	Classical entropy
$I(X;Y) = H(X) + H(Y) - H(XY)$	Classical mutual information
$H(A)_\rho = H(\rho_A) = -\text{Tr}[\rho_A \log_2(\rho_A)]$	Quantum entropy
$I(A;B)_\sigma = H(\sigma_A) + H(\sigma_B) - H(\sigma_{AB})$	Quantum mutual information
$H(A|B)_\sigma = H(\sigma_{AB}) - H(\sigma_B)$	Conditional quantum entropy

2.1.3 Quantum broadcast channels
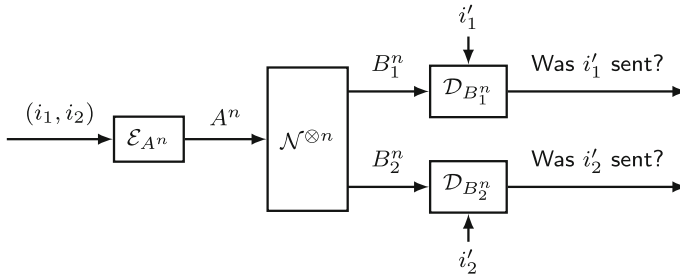
A quantum broadcast channel $\mathcal{N}_{A \to B_1 B_2} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2})$ corresponds to a quantum physical evolution from the input A to the combined output B_1, B_2, associated with the transmitter and two receivers, respectively. We assume that the channel is memoryless. That is, if the systems $A^n = (A_1, \dots, A_n)$ are sent through n channel uses, then the input ρ_{A^n} undergoes the tensor product mapping $\mathcal{N}_{A^n \to B_1^n B_2^n} \equiv \mathcal{N}_{A \to B_1 B_2}^{\otimes n}$. The marginal channel is defined by $\mathcal{N}_{A \to B_1}^{(1)}(\rho_A) = \text{Tr}_{B_2}\left(\mathcal{N}_{A \to B_1 B_2}(\rho_A)\right)$ for Receiver 1, and similarly $\mathcal{N}_{A \to B_2}^{(2)}$ for Receiver 2. The transmitter, Receiver 1, and Receiver 2 are often called Alice, Bob 1, and Bob 2. A classical-quantum (c-q) broadcast channel $\mathcal{N}_{X \to B_1 B_2}^{\text{c-q}}$ is defined, in a similar manner, as a mapping $\mathcal{X} \to \mathcal{D}(\mathcal{H}_B)$.

2.2 Identification codes

In the following, we define the communication task of identification over a quantum broadcast channel, where the decoder is not required to recover the sender's message i, but simply determines whether a particular message i' was sent or not.

Definition 1 An (N_1, N_2, n) identification (ID) code for the quantum broadcast channel $\mathcal{N}_{A \to B_1 B_2}$ consists of an encoding channel $\mathcal{E}_{A^n} : [N_1] \times [N_2] \to \mathcal{D}(\mathcal{H}_A^{\otimes n})$ and a collection of binary decoding POVMs $\mathcal{D}_{B_1^n}^{i_1} = \{\mathbb{1} - D_{i_1}^{(1)}, D_{i_1}^{(1)}\}$ and $\mathcal{D}_{B_2^n}^{i_2} = \{\mathbb{1} - D_{i_2}^{(2)}, D_{i_2}^{(2)}\}$, for $i_1 \in [N_1]$ and $i_2 \in [N_2]$. We denote the identification code by $\mathcal{C} = (\mathcal{E}_{A^n}, \mathcal{D}_{B_1^n}, \mathcal{D}_{B_2^n})$.

The identification scheme is depicted in Fig. 2. Alice chooses a pair of messages (i_1, i_2), where $i_k \in [N_k]$, for $k \in \{1, 2\}$. She encodes the messages by preparing an input state $\rho_{A^n}^{i_1, i_2} \equiv \mathcal{E}_{A^n}(i_1, i_2)$ and sends the input system A^n through n uses of the quantum broadcast channel $\mathcal{N}_{A \to B_1 B_2}$. Bob 1 and Bob 2 receive the output systems B_1^n and B_2^n, respectively. Suppose that Bob k is interested in a particular message $i_k' \in [N_k]$, where $k \in \{1, 2\}$. Then, he performs the binary measurement $\{\mathbb{1} - D_{i_k}^{(k)}, D_{i_k}^{(k)}\}$ to determine whether i_k' was sent or not and obtains a measurement outcome $s_k \in \{0, 1\}$. He declares 'no' if the measurement outcome is $s_k = 0$, and 'yes' if $s_k = 1$.

Fig. 2 Identification over the quantum broadcast channel $\mathcal{N}^{\otimes n}_{A \to B_1 B_2}$. Alice chooses a message pair (i_1, i_2). She encodes the messages by preparing an input state $\mathcal{E}_{A^n}(i_1, i_2)$, and sends the input system A^n through n uses of the quantum broadcast channel $\mathcal{N}^{\otimes n}_{A \to B_1 B_2}$. Bob 1 and Bob 2 receive the output systems B_1^n and B_2^n, respectively. As Bob k is interested in the message $i'_k \in [N_k]$, he performs the binary measurement $\mathcal{D}^{i'_k}_{B_k^n} = \{\mathbb{1} - D^{(k)}_{i'_k}, D^{(k)}_{i'_k}\}$ to determine whether i'_k was sent or not

The ID rates of the code $\mathcal{C}$ are defined as $R_k = \frac{1}{n} \log \log(N_k)$, for $k \in \{1, 2\}$. In this work, we assume that the ID messages i_k are uniformly distributed over the set $[N_k]$, for $k \in \{1, 2\}$. Therefore, the error probabilities are defined on average over the messages for the other receiver. Bob 1 makes an error in two cases: (1) He decides that i_1 was *not* sent (missed ID); (2) Bob 1 decides that i'_1 was sent, while in fact i_1 was sent, and $i_1 \neq i'_1$ (false ID). The probabilities of these two kinds of error, averaged over $i_2 \in [N_2]$, are defined as

$$\bar{e}_{1,1}(\mathcal{N}, n, \mathcal{C}, i_1) = \frac{1}{N_2} \sum_{i_2 \in [N_2]} \text{Tr}\left[(\mathbb{1} - D^{(1)}_{i_1}) \mathcal{N}^{\otimes n}(\mathcal{E}(i_1, i_2)) \right], \qquad (1a)$$

$$\bar{e}_{1,2}(\mathcal{N}, n, \mathcal{C}, i'_1, i_1) = \frac{1}{N_2} \sum_{i_2 \in [N_2]} \text{Tr}\left[D^{(1)}_{i'_1} \mathcal{N}^{\otimes n}(\mathcal{E}(i_1, i_2)) \right], \qquad (1b)$$

for $i_1, i'_1 \in [N_1]$ such that $i_1 \neq i'_1$. Similarly, Bob 2's error probabilities are

$$\bar{e}_{2,1}(\mathcal{N}, n, \mathcal{C}, i_2) = \frac{1}{N_1} \sum_{i_1 \in [N_1]} \text{Tr}\left[(\mathbb{1} - D^{(2)}_{i_2}) \mathcal{N}^{\otimes n}(\mathcal{E}(i_1, i_2)) \right], \qquad (1c)$$

$$\bar{e}_{2,2}(\mathcal{N}, n, \mathcal{C}, i'_2, i_2) = \frac{1}{N_1} \sum_{i_1 \in [N_1]} \text{Tr}\left[D^{(2)}_{i'_2} \mathcal{N}^{\otimes n}(\mathcal{E}(i_1, i_2)) \right]. \qquad (1d)$$

for $i_2, i'_2 \in [N_2]$ such that $i_2 \neq i'_2$.

An $(N_1, N_2, n, \lambda_1, \lambda_2)$ ID-code $\mathcal{C}$ for the quantum broadcast channel $\mathcal{N}_{A \to B_1 B_2}$ satisfies

$$\max_{i_k \in [N_k]} \bar{e}_{k,1}(\mathcal{N}, n, \mathcal{C}, i_k) < \lambda_1, \qquad (2a)$$

$$\max_{\substack{i_k, i'_k \in [N_k], \\ i'_k \neq i_k}} \bar{e}_{k,2}(\mathcal{N}, n, \mathcal{C}, i'_k, i_k) < \lambda_2, \qquad (2b)$$

for $k \in \{1, 2\}$. An ID rate pair (R_1, R_2) is *achievable* if for every $\lambda_1, \lambda_2 > 0$ and sufficiently large n, there exists an $\left(\exp e^{nR_1}, \exp e^{nR_2}, n, \lambda_1, \lambda_2\right)$ ID-code. The ID capacity region $\mathsf{C}_{\mathrm{ID}}(\mathcal{N})$ of the quantum broadcast channel $\mathcal{N}_{A \to B_1 B_2}$ is defined as the set of achievable rate pairs.

2.3 Previous results

In the traditional transmission setting [5], the decoder Bob is required to find an estimate $\hat{i}$ of Alice's message. This is a more stringent requirement than identification, and it results in exponentially slower communication. Specifically, the number of messages scales as $\exp(nR)$ for transmission, whereas $\exp(e^{nR})$ for identification. While the transmission rate is measured in units of information bits per channel use, the identification rate has different units. Nonetheless, for the classical-quantum single-user channel, it turns out that the identification and transmission capacities have the same *value*.

In the single-user setting, the ID capacity of the classical-quantum channel was determined by Löber [12] and Ahlswede and Winter [13]. Let $\mathcal{W}_{X \to B}$ be a single-user c-q channel. The ID capacity $C_{\mathrm{ID}}(\mathcal{W})$ is then defined, in a similar manner, as the supremum of achievable ID rates over the c-q channel $\mathcal{W}_{X \to B}$.

Theorem 1 (see [12, 13][64, Theorem 4]) *The ID capacity of a single-user classical-quantum channel $\mathcal{W}_{X \to B}$ is given by*

$$C_{\mathrm{ID}}(\mathcal{W}) = \max_{P_X \in \mathcal{P}(\mathcal{X})} I(X; B)_\rho, \tag{3}$$

where $\rho_{XB} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \mathcal{W}(x)$.

While the single-user achievability proof in [6, 12] employs a random binning scheme based on transmission codes [65], we will see that the broadcast coding methods are significantly more involved and do not follow from the transmission characterization.

3 Results

Our results are presented below. Consider the quantum broadcast channel $\mathcal{N}_{A \to B_1 B_2}$, as defined in Sect. 2.1.3. Define the rate region $\mathscr{R}(\mathcal{N})$ as

$$\mathscr{R}(\mathcal{N}) = \bigcup_{P_X \in \mathcal{P}(\mathcal{X}), \ |\phi_A^x\rangle} \left\{ \begin{array}{c} (R_1, R_2) : R_1 \leq I(X; B_1)_\rho, \\ R_2 \leq I(X; B_2)_\rho \end{array} \right\} \tag{4}$$

with $\rho_{XB_1B_2} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \mathcal{N}(|\phi_A^x\rangle\langle\phi_A^x|)$.

Theorem 2 *1. The region $\mathscr{R}(\mathcal{N})$ is achievable for identification over the quantum broadcast channel $\mathcal{N}_{A \to B_1 B_2}$. That is,*

$$\mathsf{C}_{\text{ID}}(\mathcal{N}) \supseteq \mathscr{R}(\mathcal{N}). \tag{5}$$

2. The identification capacity region of a classical-quantum broadcast channel $\mathcal{N}^{c\text{-}q}_{X \to B_1 B_2}$ is given by

$$\mathsf{C}_{\text{ID}}(\mathcal{N}^{c\text{-}q}) = \bigcup_{P_X \in \mathcal{P}(\mathcal{X})} \left\{ \begin{array}{r} (R_1, R_2) : R_1 \le I(X; B_1)_\rho, \\ R_2 \le I(X; B_2)_\rho \end{array} \right\}, \tag{6}$$

with $\rho_{X B_1 B_2} = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x| \otimes \mathcal{N}^{c\text{-}q}(x)$.

The proof of part 1 is given in Sect. 5, where we show that all rate pairs in the interior of the region $\mathscr{R}(\mathcal{N})$ are achievable. In Sect. 6, we prove part 2 and show the classical-quantum converse part, *i.e.* that no rate pair outside the region above can be achieved for identification over the classical-quantum broadcast channel. In the proof of part 1, we use the pool-selection method by Bracher and Lapidoth [24, 25]. This will enable the same extension to the broadcast setting as in [24, 25]. On the other hand, in the converse proof, we used a different approach exploiting recent observations by Boche et al. [17] along with the methods of Ahlswede and Winter [13].

Remark 1 As mentioned in Sect. 2.3, in the classical-quantum single-user setting, the ID and transmission capacity characterizations are identical. On the other hand, in the broadcast ID setting, we see a departure from this equivalence [24, 25, 28]. The examples in the following section demonstrate this departure in a more explicit manner, showing that the ID capacity region can be strictly larger than the transmission capacity region.

Remark 2 Consider the classical-quantum broadcast channel. In general, the rate R_k of User k must be limited by the ID capacity of the single-user channel from A to B_k, for $k \in \{1, 2\}$. This observation leads to the following rectangular upper bound,

$$\mathsf{C}_{\text{ID}}(\mathcal{N}^{c\text{-}q}) \subseteq \left\{ \begin{array}{r} (R_1, R_2) : R_1 \le \mathsf{C}^{(1)}_{\text{ID}}, \\ R_2 \le \mathsf{C}^{(2)}_{\text{ID}} \end{array} \right\}, \tag{7}$$

where $\mathsf{C}^{(k)}_{\text{ID}} = \max_{P_X} I(X; B_k)_\rho$. However, in identification over the broadcast channel, the users cannot necessarily achieve the full capacity of each marginal channel simultaneously, since both marginal channels must share the same input distribution in the capacity formula on the right hand side of (6). Equality holds in (7) if the same input distribution $P_X^\star$ maximizes both mutual informations simultaneously, *i.e.* when

$$P_X^\star = \arg \max_{P_X} I(X; B_1)_\rho = \arg \max_{P_X} I(X; B_2)_\rho. \tag{8}$$
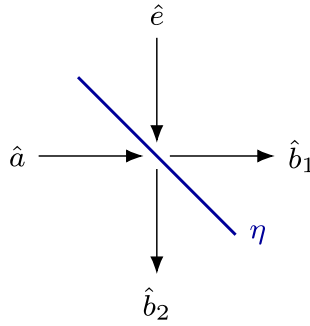
Fig. 3 The beam splitter relation of the single-mode bosonic broadcast channel. The channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is a pair of modes with annihilation operators $\hat{b}_1$ and $\hat{b}_2$, corresponding to each receiver. The mode $\hat{e}$ is associated with the environment noise in the pure-loss setting, the environment is in the vacuum state, i.e., $\hat{e} = |0\rangle$. The parameter η is the transmissivity, which captures the length of the optical fiber and its absorption length

4 Examples

As examples, we consider the pure-loss bosonic broadcast channel and the erasure broadcast channel.

4.1 Bosonic broadcast channel

To demonstrate our results, consider the single-mode bosonic broadcast channel. We extend the finite-dimension result in Theorem 2 to the bosonic channel with infinite-dimension Hilbert spaces based on the discretization limiting argument by Guha limiting argument by Guha [57]. A detailed description of (continuous-variable) bosonic systems can be found in [54]. Here, we only define the notation for the quantities that we use. We use hat-notation, *e.g.* $\hat{a}$, $\hat{b}_1$, $\hat{b}_2$, $\hat{e}$, to denote annihilation operators that act on a quantum state. A thermal state $\tau(N)$ is a Gaussian mixture of coherent states, where $\tau(N) \equiv \int_{\mathbb{C}} d^2\alpha \frac{e^{-|\alpha|^2/N}}{\pi N} |\alpha\rangle\langle\alpha|$, with an average photon number $N > 0$.

Consider a bosonic broadcast channel, whereby the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the output is a pair of modes with annihilation operators $\hat{b}_1$ and $\hat{b}_2$. The annihilation operators correspond to Alice, Bob 1, and Bob 2, respectively. The input–output relation of the pure-loss bosonic broadcast channel in the Heisenberg picture [66] is given by

$$\hat{b}_1 = \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{e}, \tag{9}$$

$$\hat{b}_2 = \sqrt{1-\eta}\,\hat{a} - \sqrt{\eta}\,\hat{e}, \tag{10}$$

where $\hat{e}$ is associated with the environment noise and η is the transmissivity, $0 \leq \eta \leq 1$, which captures, for instance, the length of the optical fiber and its absorption length [67]. The relations above correspond to the outputs of a beam splitter, as illustrated in Fig. 3. In the pure-loss setting, the environment is in the vacuum state, i.e.,

$\hat{e} = |0\rangle$. It is assumed that the encoder uses a coherent state protocol with an input constraint. That is, the input state is a coherent state $|x\rangle$, $x \in \mathbb{C}$, such that each codeword satisfies $\frac{1}{n} \sum_{i=1}^{n} |x_i|^2 \le N_A$.

Based on part 1 of Theorem 2, the ID capacity region of the pure-loss bosonic broadcast channel with coherent encoding and average photon number at most N_A is given by

$$\mathsf{C_{ID}}(\mathcal{N}) = \left\{ (R_1, R_2) \; : \; \begin{matrix} R_1 \le g(\eta N_A) \\ R_2 \le g((1-\eta)N_A) \end{matrix} \right\} \tag{11}$$

where $g(N) = (N+1)\log(N+1) - N\log(N)$ is the entropy of a thermal state with mean photon number N, with $0\log 0 := 0$. See Fig. 1. The converse part immediately follows from the single-user capacity characterization. To show achievability, set the input to be an ensemble of coherent states, $|X\rangle$, with a circularly-symmetric Gaussian distribution with zero mean and variance $\mathbb{E}[|X|^2] = N_A$. As mentioned in Remark 2, the users cannot necessarily achieve the marginal capacity. Nevertheless, for the bosonic broadcast channel, each user achieves the full capacity of the respective marginal channel.

On the other hand, the transmission capacity region of the single-mode pure-loss bosonic broadcast channel is [56, 57],

$$\mathsf{C_T}(\mathcal{N}) = \bigcup_{0 \le \beta \le 1} \left\{ (R_1, R_2) : \begin{matrix} R_1 \le g(\eta \beta N_A) \\ R_2 \le g((1-\eta)N_A) - g((1-\eta)\beta N_A) \end{matrix} \right\}. \tag{12}$$

where the subscript 'T' stands for 'Transmission', under the assumption that the minimum output-entropy conjecture holds (see Strong Conjecture 2 in [57]). The transmission capacity region and the ID capacity region are depicted in Fig. 1 as the light gray area (T) and additionally the dark gray area (ID), respectively.

The converse part for the transmission result on the pure-loss bosonic broadcast channel relies on the strong minimum output-entropy conjecture [56], as stated below. Let the noise modes $\{\hat{e}_i\}_{i=1}^n$ be in a product state $\rho_{E^n} = |0\rangle\langle 0|^{\otimes n}$ of n vacuum states, and assume that $H(A^n)_\rho = ng(N_A)$. Then, the strong minimum output-entropy conjecture states that [56]

$$H(B^n)_\rho \ge ng(\eta N_A). \tag{13}$$

We note that in the single-user case, the conjecture is not required for neither identification nor transmission [68–70] [71, Section VI.B]. There are several special cases that are known to hold [72, Section III]. E.g., it is well known that the conjecture holds for $n = 1$. However, as pointed out in [70, Section V], this is insufficient for the converse proof of the bosonic broadcast channel, which requires the strong minimum output-entropy conjecture stated above.

4.2 Erasure broadcast channel

We consider the qubit erasure broadcast channel, specified by $\mathcal{N}(\rho) = U\rho U^{\dagger}$,

$$U = \sqrt{1-\lambda}\mathbb{1}_{A \to B_1} \otimes |e\rangle_{B_2} + \sqrt{\lambda}\,|e\rangle_{B_1} \otimes \mathbb{1}_{A \to B_2}, \qquad (14)$$

where the erasure state $|e\rangle$ is orthogonal to the qubit space, and $0 \le \lambda \le \frac{1}{2}$ is a given parameter. Hence, the marginal channels to Bob 1 and Bob 2 are standard quantum erasure channels, with erasure parameters λ and $1 - \lambda$, respectively. Specifically,

$$\mathcal{N}^{(1)}(\rho) = (1-\lambda)\rho + \lambda|e\rangle\langle e|, \qquad (15)$$

$$\mathcal{N}^{(2)}(\rho) = \lambda\rho + (1-\lambda)|e\rangle\langle e|. \qquad (16)$$

The ID capacity region of the erasure broadcast channel $\mathcal{N}_{A \to B_1 B_2}$ satisfies

$$\mathsf{C}_{\mathsf{ID}}(\mathcal{N}) \supseteq \mathscr{R}(\mathcal{N}) = \left\{ \begin{array}{c} (R_1, R_2) : R_1 \le 1 - \lambda, \\ R_2 \le \lambda \end{array} \right\}. \qquad (17)$$

This result is obtained in a straightforward manner. To show achievability, we apply part 1 of Theorem 2 and set $P_X = \left(\frac{1}{2}, \frac{1}{2}\right)$ over the ensemble $\{|0\rangle, |1\rangle\}$.

First, consider the symmetric case of $\lambda = \frac{1}{2}$. Our achievable region $\mathscr{R}(\mathcal{N})$ is then the best known bound on the ID capacity region. Whereas, for $\lambda < \frac{1}{2}$, we can improve upon our bound.

For a single-user quantum erasure channel $\mathcal{L}_{A \to B}$ with a parameter ε, Winter established achievability of the identification rate $R = 2(1 - \varepsilon)$ for $\varepsilon < \frac{1}{2}$, and $R = 1 - \varepsilon$ for $\varepsilon \ge \frac{1}{2}$ [14, Section 4], where ρ_X is a classical state. If $\lambda = \frac{1}{2}$, then this yields the rate pair $(R_1, R_2) = \left(\frac{1}{2}, \frac{1}{2}\right)$, which is the corner of our region in (17). On the other hand, for $\lambda < \frac{1}{2}$, the rate pairs $(R_1, R_2) = (2(1 - \lambda), 0)$ and $(R_1, R_2) = (0, \lambda)$ are achievable. Hence, by time division, i.e., coding for User 1 over a sub-block of length αn, and for User 2 over the remaining sub-block of $(1 - \alpha)n$ channel uses, we have that the ID capacity region is lower-bounded by

$$\mathsf{C}_{\mathsf{ID}}(\mathcal{N}) \supseteq \mathscr{T} := \bigcup_{0 \le \alpha \le 1} \left\{ \begin{array}{c} (R_1, R_2) : R_1 \le 2\alpha(1 - \lambda), \\ R_2 \le (1 - \alpha)\lambda \end{array} \right\}. \qquad (18)$$

The transmission capacity region $\mathsf{C}_{\mathsf{T}}(\mathcal{N})$ of the quantum erasure broadcast channel is also achieved by time-division. It is given by the rate pairs (R_1, R_2) satisfying $R_1 \le \alpha(1-\lambda)$ and $R_2 \le (1-\alpha)\lambda$, for some $0 \le \alpha \le 1$, as can be shown using the same methods used in [73, Example 3.2 and Section 5.4.1] and [19, Section 20.4.3]. Clearly, $\mathsf{C}_{\mathsf{T}}(\mathcal{N})$ is contained in either of the regions $\mathscr{R}(\mathcal{N})$, $\mathscr{T}$. We deduce that for an erasure channel that is not symmetric, our achievable region $\mathscr{R}(\mathcal{N})$ in Theorem 2 is suboptimal, but improves on the best previously known bound in the interval $0 < R_1 \le 1 - \lambda$.
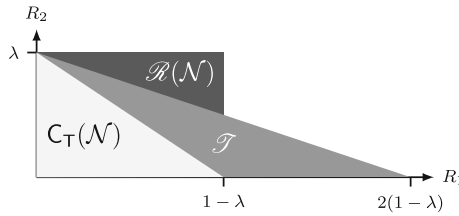
Fig. 4 Achievable regions for ID over the qubit erasure broadcast channel $\mathcal{N}$ with erasure probability $\lambda = \frac{1}{4}$. The transmission capacity region $\mathsf{C_T}(\mathcal{N})$ corresponds to the light gray area. The region $\mathscr{T}$ achievable by time-division between single-user identification codes comprises additionally the middle gray area. The rectangle indicated by the dark gray area corresponds to our lower bound $\mathscr{R}(\mathcal{N})$

Figure 4 shows the regions $\mathsf{C_T}(\mathcal{N})$, $\mathscr{T}$ and $\mathscr{R}(\mathcal{N})$ for a quantum erasure broadcast channel $\mathcal{N}$ with $\lambda = \frac{1}{4}$.

5 Achievability proof

In this section, we prove the lower bound on the capacity region in Theorem 2, *i.e.* we show that

$$\mathsf{C_{ID}}(\mathcal{N}) \supseteq \mathscr{R}(\mathcal{N}). \tag{19}$$

In the classical achievability proof, Bracher and Lapidoth [24, 25] first generate a single-user random code, based on a pool-selection technique, as shown below. Then, a similar pool-selection code is constructed for the BC using a pair of single-user codes, one for each receiver. It is shown in [24, 25] that the corresponding ID error probabilities for the BC can be approximated in terms of the error probabilities of the single-user codes. We use a similar approach, and begin with the *single-user* quantum channel.

We use standard tools of typical space projectors as detailed in Appendix A. In particular, $\mathcal{T}_\delta^n(P_X)$ denotes the classical δ-typical set with respect to a given PMF $P_X \in \mathcal{P}(\mathcal{X})$ over $\mathcal{X}$. Furthermore, $\Pi_\delta^n(\rho)$ is the projector onto the δ-typical subspace of an average state $\rho = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x|$, and $\Pi_\delta^n(\sigma_{XB}|x^n)$ is the conditionally δ-typical projector for a classical-quantum state σ_{XB}.

5.1 Single-user quantum channel

First, we construct and analyze an identification code for a single-user quantum channel. In Sect. 5.2, we will use the single-user code in order to construct a code for the broadcast channel. Let $\mathcal{L}_{A \to B}$ be a single-user quantum channel.

5.1.1 Code construction

Let $N = \exp e^{nR}$ be the code size. Fix a PMF P_X over $\mathcal{X}$, a pool rate R_{pool}, and a binning rate $\tilde{R}$, such that

$$R < \tilde{R} < I(X; B)_\rho \tag{20}$$

$$R_{\text{pool}} > \tilde{R}. \tag{21}$$

We generate the codebook such that all codewords are δ-typical. Therefore, consider the distribution

$$P_{X'^n}(x^n) = \frac{P_X^n(x^n)}{P_X^n\left(\mathcal{T}_\delta^n(P_X)\right)} \cdot \mathbb{1}\left(x^n \in \mathcal{T}_\delta^n(P_X)\right), \tag{22}$$

where the indicator function $\mathbb{1}(\pi)$ takes the value 1 if π is true, and 0 otherwise. For every index $v \in \mathcal{V} = [e^{nR_{\text{pool}}}]$, choose a codeword $F(v) \sim P_{X'^n}$ at random. Then, for every $i \in [N]$, decide whether to add v to the set $\mathcal{V}_i$ by a binary experiment, with probability $e^{-n\tilde{R}}/|\mathcal{V}| = e^{-n(R_{\text{pool}} - \tilde{R})}$. That is, decide to include v in $\mathcal{V}_i$ with probability $e^{-n(R_{\text{pool}} - \tilde{R})}$, and not to include it with probability $1 - e^{-n(R_{\text{pool}} - \tilde{R})}$. Reveal this construction to all parties. Denote the collection of codewords and index bins by

$$\mathcal{B} = \left(\{F(v)\}_{v \in \mathcal{V}}, \{\mathcal{V}_i\}_{i=1}^N\right). \tag{23}$$

5.1.2 Encoding

To send an ID Message $i \in [N]$, Alice chooses an index v uniformly at random from $\mathcal{V}_i$. If $\mathcal{V}_i$ is non-empty, she prepares the state

$$\left|\phi_{A^n}^{F(v)}\right\rangle \equiv \bigotimes_{t=1}^n \left|\phi_A^{F_t(v)}\right\rangle, \tag{24}$$

where $F_t(v)$ is the t-th symbol of the sequence $F(v)$. Otherwise, if $\mathcal{V}_i = \emptyset$, she prepares $|\phi_{A^n}^{F(1)}\rangle$. Then, Alice transmits the systems A^n through the channel. Therefore, if $\mathcal{V}_i \neq \emptyset$, then the average input state $\mathcal{E}_{A^n}(i)$ is given by

$$\mathcal{E}_{A^n}(i) = \frac{1}{|\mathcal{V}_i|} \sum_{v \in \mathcal{V}_i} \left|\phi_{A^n}^{F(v)}\middle\rangle\middle\langle\phi_{A^n}^{F(v)}\right|. \tag{25}$$

5.1.3 Decoding

Bob receives the output systems B^n, and he would like to determine whether the message i' was sent. To this end, he selects any constant δ such that

$$0 < \delta < \frac{I(X; B)_\rho - \tilde{R}}{c + c'}, \tag{26}$$

where $c, c' > 0$ are constants as in Section A. Then, he performs a series of binary decoding measurements (POVMs)

$$\mathcal{D}^{F(v)} = \left\{ \mathbb{1} - \Pi \Pi^{F(v)} \Pi, \Pi \Pi^{F(v)} \Pi \right\}, \tag{27}$$

where we denote $\Pi \equiv \Pi_\delta^n(\rho_B)$ and $\Pi^{F(v)} \equiv \Pi_\delta^n(\rho_{XB}|F(v))$. Bob obtains a binary sequence of measurement outcomes $(a(v))_{v \in \mathcal{V}_{i'}}$. If $a(v) = 1$ for some $v \in \mathcal{V}_{i'}$, then Bob declares that i' was sent. Otherwise, he declares that i' was not sent. Note that we can also construct one POVM $\mathcal{D}_{B^n}^{i'}$ that is equivalent to the series of measurements.

Thus, the ID code associated with the construction above is denoted by

$$\mathcal{C}_\mathcal{B} = (\mathcal{E}_{A^n}, \mathcal{D}_{B^n}).$$

The error analysis for the single-user identification code is delegated to Appendix B.

5.2 Broadcast channel

In this section, we show the direct part for the ID capacity region of the quantum broadcast channel. That is, we show that $C_{ID}(\mathcal{N}) \supseteq \mathscr{R}(\mathcal{N})$. The analysis makes use of the our single-user derivation above.

5.2.1 Code construction

We extend Bracher and Lapidoth's [24, 25] idea to combine two BL codebooks $\mathcal{B}^{(1)}, \mathcal{B}^{(1)}$ that share the same pool. Fix a PMF P_X over $\mathcal{X}$ and rates $R_k, \tilde{R}_k$, for $k \in \{1, 2\}$, that satisfy

$$R_1 < \qquad \tilde{R}_1 \qquad < \min_{s \in \mathcal{S}} I(X; B_1)_\rho \tag{28a}$$

$$R_2 < \qquad \tilde{R}_2 \qquad < \min_{s \in \mathcal{S}} I(X; B_2)_\rho \tag{28b}$$

$$\max \left\{ \tilde{R}_1, \tilde{R}_2 \right\} < R_{\text{pool}} \tag{28c}$$

$$R_{\text{pool}} < \quad \tilde{R}_1 + \tilde{R}_2. \tag{28d}$$

Let $N_k = e^{nR_k}$. For every index $v \in \mathcal{V} = [e^{nR_{\text{pool}}}]$, perform the following. Choose a codeword $F(v) \sim P_X^n$ at random, as in the single-user case. Then, for every i_k, decide whether to add v to the set $\mathcal{V}_{i_k}^{(k)}$ by a binary experiment, with probability $e^{-n\tilde{R}_k} / |\mathcal{V}| = e^{-n(R_{\text{pool}} - \tilde{R}_k)}$. That is, decide that v is included in $\mathcal{V}_{i_k}^{(k)}$ with probability $e^{-n(R_{\text{pool}} - \tilde{R}_k)}$, and not to include with probability $1 - e^{-n(R_{\text{pool}} - \tilde{R}_k)}$. Finally, for every pair $(i_1, i_2) \in [N_1] \times [N_2]$, select a common index V_{i_1,i_2} uniformly at random from $\mathcal{V}_{i_1}^{(1)} \cap \mathcal{V}_{i_2}^{(2)}$, if this intersection is non-empty. Otherwise, if $\mathcal{V}_{i_1}^{(1)} \cap \mathcal{V}_{i_2}^{(2)} = \emptyset$, then draw V_{i_1,i_2} uniformly from $\mathcal{V}$. Reveal this construction to all parties.

Denote the collection of codewords and index bins by

$$\mathcal{B}_{\mathcal{N}} = \left(F, \{\mathcal{V}_{i_1}^{(1)}\}_{i_1 \in [N_1]}, \{\mathcal{V}_{i_2}^{(2)}\}_{i_2 \in [N_2]}, \{V_{i_1,i_2}\}_{(i_1,i_2) \in [N_1] \times [N_2]} \right). \qquad (29)$$

Note that, for $k \in \{1, 2\}$, $\mathcal{B}_{\mathcal{N}}$ includes all elements of $\mathcal{B}^{(k)} = \left(F, \left\{ \mathcal{V}_{i_k}^{(k)} \right\}_{i_k \in [N_k]} \right)$, defined for the marginal channels $\mathcal{N}_{A \to B_k}^{(k)}$ as in Sect. 5.1. We denote the corresponding single-user code by

$$\mathcal{C}_{\mathcal{B}^{(k)}} = (\tilde{\mathcal{E}}_{A^n}^{(k)}, \mathcal{D}_{B_k^n}). \qquad (30)$$

5.2.2 Encoding

To send an ID message pair $(i_1, i_2) \in [N_1] \times [N_2]$, Alice prepares the input state $\left| \phi_{A^n}^{F(V_{i_1,i_2})} \right\rangle$ and transmits the input system A^n.

5.2.3 Decoding

Receiver k, for $k = 1, 2$, employs the decoder of the single-user code $\mathcal{C}_{\mathcal{B}^{(k)}}$. Specifically, suppose that Bob k is interested in an ID message $i_k' \in [N_k]$. Then, he uses the decoding POVM $\mathcal{D}_{B_k^n}^{i_k'}$ to decide whether i_k' was sent or not.

We denote the broadcast ID code associated with the construction above by

$$\mathcal{C}_{\mathcal{B}_{\mathcal{N}}} = (\mathcal{E}_{A^n}, \mathcal{D}_{B_1^n}, \mathcal{D}_{B_2^n}) \qquad (31)$$

5.2.4 Error analysis

We show that the semi-average error probabilities of the ID code defined above can be approximately upper-bounded by the respective error probabilities of the single-user ID-codes $\mathcal{C}_{\mathcal{B}^{(1)}}$ and $\mathcal{C}_{\mathcal{B}^{(2)}}$ for the respective receivers.

Consider a given pair of codebooks $\mathcal{B}^{(1)}$ and $\mathcal{B}^{(2)}$. Conditioned on those codebooks, the input state can be written in terms of an encoding distribution

$$\mathcal{E}_{A^n}(i_1, i_2) = \sum_{v \in \mathcal{V}} \mathbf{Q}_{i_1,i_2}(v) \left| \phi_{A^n}^{F(v)} \right\rangle\!\!\left\langle \phi_{A^n}^{F(v)} \right|, \qquad (32)$$

where $\mathbf{Q}_{i_1,i_2}(v) = \mathbb{1}\left(v = V_{i_1,i_2} \right)$. Similarly,

$$\tilde{\mathcal{E}}_{A^n}^{(k)}(i_k) = \sum_{v \in \mathcal{V}} \tilde{\mathbf{Q}}_{i_k}^{(k)}(v) \left| \phi_{A^n}^{F(v)} \right\rangle\!\!\left\langle \phi_{A^n}^{F(v)} \right| \qquad (33)$$

where $\tilde{Q}_{i_k}^{(k)}(v)$ is the respective distribution for the single-user code from Sect. 5.1, namely

$$\tilde{Q}_{i_k}^{(k)}(v) = \begin{cases} \frac{1}{\left|\mathcal{V}_{i_k}^{(k)}\right|} \mathbb{1}\left(v \in \mathcal{V}_{i_k}^{(k)}\right) & \text{if } \mathcal{V}_{i_k}^{(k)} \neq \emptyset, \\ \mathbb{1}\,(v = 1) & \text{if } \mathcal{V}_{i_k}^{(k)} = \emptyset. \end{cases} \tag{34}$$

We consider now only Receiver 1 and his marginal channel $\mathcal{N}_{A_1 \to B}^{(1)}$. Since the code construction is completely symmetric between the two receivers, the same arguments hold for Receiver 2 and $\mathcal{N}_{A_2 \to B}^{(2)}$. The missed-ID error probability for $\mathcal{C}_{\mathcal{B}_\mathcal{N}}$ and Bob 1 is given by

$$\bar{e}_{1,1}(\mathcal{N}, n, \mathcal{C}_{\mathcal{B}_\mathcal{N}}, i_1) = \frac{1}{N_2} \sum_{i_2 \in [N_2]} \text{Tr}\left[(\mathbb{1} - D_{i_1}^{(1)})\mathcal{N}_{A \to B_1}^{(1) \otimes n}\left(\mathcal{E}_{A^n}(i_1, i_2)\right)\right] \tag{35}$$

and for $\mathcal{C}_{\mathcal{B}^{(k)}}$, it is given by

$$e_1(\mathcal{N}_{A \to B_1}^{(1)}, n, \mathcal{C}_{\mathcal{B}^{(1)}}, i_1) = \text{Tr}\left[(\mathbb{1} - D_{i_1}^{(1)})\mathcal{N}_{A \to B_1}^{(1) \otimes n}\left(\tilde{\mathcal{E}}_{A^n}^{(k)}(i_1)\right)\right]. \tag{36}$$

By the linearity of the channel and the measurement, we have

$$\bar{e}_{1,1}(\mathcal{N}, n, \mathcal{C}_{\mathcal{B}^{(1)}}, i_1) - e_1(\mathcal{N}_{A \to B_1}^{(1)}, n, \mathcal{C}_{\mathcal{B}^{(1)}}, i_1)$$

$$\leq \frac{1}{2}\left\|\frac{1}{N_2}\sum_{i_2 \in [N_2]}\mathcal{E}_{A^n}(i_1, i_2) - \tilde{\mathcal{E}}_{A^n}^{(k)}(i_1)\right\|_1$$

$$= \frac{1}{2}\left\|\frac{1}{N_2}\sum_{i_2 \in [N_2]}\sum_{v \in \mathcal{V}} Q_{i_1,i_2}(v)\left|\phi_{A^n}^{F(v)}\middle\rangle\!\middle\langle\phi_{A^n}^{F(v)}\right| - \sum_{v \in \mathcal{V}}\tilde{Q}_{i_1}^{(k)}(v)\left|\phi_{A^n}^{F(v)}\middle\rangle\!\middle\langle\phi_{A^n}^{F(v)}\right|\right\|_1$$

$$= \frac{1}{2}\left|\sum_{v \in \mathcal{V}}\left(\frac{1}{N_2}\sum_{i_2 \in [N_2]} Q_{i_1,i_2}(v) - \sum_{v \in \mathcal{V}}\tilde{Q}_{i_1}^{(k)}(v)\right)\right|$$

$$\leq \delta_{i_1}^{(1)}, \tag{37}$$

where $\delta_{i_1}^{(1)}$ is the total variation distance

$$\delta_{i_1}^{(1)} = \frac{1}{2}\sum_{v \in \mathcal{V}}\left|\frac{1}{N_2}\sum_{i_2 \in [N_2]} Q_{i_1,i_2}(v) - \sum_{v \in \mathcal{V}}\tilde{Q}_{i_1}^{(1)}(v)\right| = d\left(\frac{1}{N_2}\sum_{i_2 \in [N_2]} Q_{i_1,i_2}, \tilde{Q}_{i_1}^{(1)}\right), \tag{38}$$

and the inequalities follow from the triangle inequality. The same argument applies to the false-ID error. Hence,

$$\bar{e}_{1,1}(\mathcal{N}, n, \mathcal{C}_{\mathcal{B}_\mathcal{N}}, i_1) \leq e_1(\mathcal{N}^{(1)}_{A \to B_1}, n, \mathcal{C}_{\mathcal{B}^{(1)}}, i_1) + \delta^{(1)}_{i_1}, \tag{39a}$$

$$\bar{e}_{1,2}(\mathcal{N}, n, \mathcal{C}_{\mathcal{B}_\mathcal{N}}, i_1', i_1) \leq e_2(\mathcal{N}^{(1)}_{A \to B_1}, n, \mathcal{C}_{\mathcal{B}^{(1)}}, i_1', i_1) + \delta^{(1)}_{i_1}, \tag{39b}$$

Similarly, the error probabilities for the second marginal channel are bounded by

$$\bar{e}_{2,1}(\mathcal{N}, n, \mathcal{C}_{\mathcal{B}_\mathcal{N}}, i_2) \leq e_1(\mathcal{N}^{(2)}_{A \to B_2}, n, \mathcal{C}_{\mathcal{B}^{(2)}}, i_2) + \delta^{(2)}_{i_2}, \tag{39c}$$

$$\bar{e}_{2,2}(\mathcal{N}, n, \mathcal{C}_{\mathcal{B}_\mathcal{N}}, i_2', i_2) \leq e_2(\mathcal{N}^{(2)}_{A \to B_2}, n, \mathcal{C}_{\mathcal{B}^{(2)}}, i_2', i_2) + \delta^{(2)}_{i_2}, \tag{39d}$$

where $\delta^{(2)}_{i_2} = d\left(\frac{1}{N_1} \sum_{i_1 \in [N_1]} \boldsymbol{Q}_{i_1, i_2}, \, \tilde{\boldsymbol{Q}}^{(2)}_{i_2} \right)$.

From this point, we can continue as in the classical derivation due to Bracher and Lapidoth [24, 25]. The next lemma bounds $\delta^{(k)}_{i_k}$ in (39) to zero in probability as $n \to \infty$. By [24], [30, Lemma 3], for every $k \in \{1, 2\}$ and some $\tau > 0$,

$$\lim_{n \to \infty} \Pr\left(\max_{i_k \in [N_k]} \delta^{(k)}_{i_k} \geq e^{-n\tau} \right) = 0. \tag{40}$$

Hence by (39), the error probabilities for the quantum broadcast-channel code $\mathcal{C}_{\mathcal{B}_\mathcal{N}}$ are approximately upper-bounded by the corresponding error probabilities for the single-user marginal codes $\mathcal{C}_{\mathcal{B}^{(1)}}$ and $\mathcal{C}_{\mathcal{B}^{(2)}}$.

By (59) for the single-user quantum channel $\mathcal{N}^{(k)}_{A \to B_k}$ and $k \in \{1, 2\}$, the error probabilities $e_1(\mathcal{N}^{(k)}_{A \to B_k}, n, \mathcal{C}_{\mathcal{B}^{(k)}}, i_k)$ and $e_2(\mathcal{N}^{(k)}_{A \to B_k}, n, \mathcal{C}_{\mathcal{B}^{(k)}}, i_k', i_k)$ converge in probability to zero with convergence speed exponentially in n, for all messages $i_k, i_k' \in [N_k]$ such that $i_k \neq i_k'$. This completes the proof of the direct part. $\qquad\square$

6 Converse proof

The direct part follows from part 1. Hence, it remains to prove the converse part. To this end, consider an $(N_1, N_2, n, \lambda_1, \lambda_2)$ ID code, $\mathcal{C} = (\mathcal{E}_{X^n}, \mathcal{D}_{B_1^n}, \mathcal{D}_{B_2^n})$, for the c-q broadcast channel $\mathcal{N}_{X \to B_1 B_2}$. In the case of a classical input, the encoder effectively assigns a probability distribution Q_{i_1, i_2} to each message pair, *i.e.*

$$\mathcal{E}_{X^n}(i_1, i_2) = \sum_{x^n \in \mathcal{X}^n} Q_{i_1, i_2}(x^n) \left| x^n \middle\rangle\!\middle\langle x^n \right|. \tag{41}$$

Thus, the ID code is specified by $\left\{ \left(Q_{i_1, i_2}, D^{(1)}_{i_1}, D^{(2)}_{i_2} \right) : (i_1, i_2) \in [N_1] \times [N_2] \right\}$. We denote the Holevo information for each c-q channel $\mathcal{N}^{(k)}_{X \to B_k}$ with respect to an input distribution $P_X \in \mathcal{P}(\mathcal{X})$ by $\mathsf{I}(P_X, \mathcal{N}^{(k)}_{X \to B_k}) \equiv I(X; B_k)_\rho$.

Following the approach of Boche et al. [17], we prove the converse part in three stages, beginning with a modification of the code.

6.1 Code modification

6.1.1 δ-net on $\mathcal{P}(\mathcal{X})$

First, we fix a δ-net $\mathcal{T}$ of probability distributions on $\mathcal{X}$. That is, for $|\mathcal{T}| \leq \left(\frac{c}{\delta}\right)^{|\mathcal{X}|}$, there exists $\mathcal{T} \subseteq \mathcal{P}(\mathcal{X})$ such that $\mathcal{X}^n = \bigcup_{P \in \mathcal{T}} \mathcal{A}_P$ and such that the type of an input sequence $x^n \in \mathcal{A}_P$ is δ-close to P. Hence,

$$Q_{i_1,i_2} = \bigoplus_{P \in \mathcal{T}} \mu_{i_1,i_2}(P) Q_{i_1,i_2}^P \tag{42}$$

where μ_{i_1,i_2} is a PMF over $\mathcal{T}$, and Q_{i_1,i_2}^P are PMFs over $\mathcal{A}_P$.

6.1.2 ϵ-net on $\mathcal{P}(\mathcal{T})$

For $|\mathcal{M}| \leq \left(\frac{c}{\epsilon}\right)^{|\mathcal{T}|}$, there exists an ϵ-net $\mathcal{M} \subseteq \mathcal{P}(\mathcal{T})$. Hence, for every i_2, there exists a PMF $\mu'_{i_2} \in \mathcal{M}$ such that at least a fraction $\frac{1}{|\mathcal{M}|}$ of the messages $i_1 \in [N_1]$ has μ_{i_1,i_2} that is ϵ-close to μ'_{i_2}. Without loss of generality, for $N'_1 = \left\lfloor \frac{N_1}{|\mathcal{M}|} \right\rfloor$,

$$\forall i_1 \in [N'_1] : \frac{1}{2} \left\| \mu_{i_1,i_2} - \mu'_{i_2} \right\|_1 \leq \epsilon. \tag{43}$$

Similarly, there exists a probability distribution $\mu'' \in \mathcal{M}$ such that at least a $\frac{1}{|\mathcal{M}|}$ of the messages $i_2 \in [N_2]$ has μ'_{i_2} that is ϵ-close to μ''. Without loss of generality, for $N'_2 = \left\lfloor \frac{N_2}{|\mathcal{M}|} \right\rfloor$, $\forall i_2 \in [N'_2] : \frac{1}{2} \left\| \mu'_{i_2} - \mu'' \right\|_1 \leq \epsilon$. Thereby,

$$\forall (i_1,i_2) \in [N'_1] \times [N'_2] : \frac{1}{2} \left\| \mu'_{i_1,i_2} - \mu'' \right\|_1 \leq 2\epsilon. \tag{44}$$

Then, we modify the encoding distribution and define

$$Q''_{i_1,i_2} = \bigoplus_{P \in \mathcal{T}} \mu''(P) Q_{i_1,i_2}^P, \tag{45}$$

leaving the decoder as it is. This results in an $(n, N'_1, N'_2, \lambda_1 + 2\epsilon, \lambda_2 + 2\epsilon)$ code, where we choose ϵ to be sufficiently small such that $\lambda_1 + \lambda_2 + 2\epsilon < 1$.

6.2 Encoder truncation

There exists $P^* \in \mathcal{T}$ such that $\mu''(P^*) \geq \frac{1}{|\mathcal{T}|}$. Thereby, we modify the code once more and truncate all the other distributions in $\mathcal{T}$. That is, we consider the code $\left\{ (Q_{i_1,i_2}^{P^*}, D_{i_1}^{(1)}, D_{i_2}^{(2)}) : (i_1,i_2) \in [N'_1] \times [N'_2] \right\}$. For the new code, the error probabilities of the first and the second kind are bounded by $\lambda_k^* = |\mathcal{T}| (\lambda_k + 2\epsilon)$ for $k \in \{1, 2\}$.

Letting $\epsilon \equiv \epsilon(\lambda_1, \lambda_2) \to 0$ as $\lambda_1, \lambda_2 \to 0$, the error probabilities of the truncated code tend to zero for every given $\delta > 0$.

6.3 Rate bounds

Consider the marginal $\mathcal{N}_{A \to B_1}^{(1)}$ and $Q_{i_1}^{P^*} \equiv \frac{1}{N_2} \sum_{i_2=1}^{N_2'} Q_{i_1, i_2}^{P^*}$. Let i_2 be uniformly distributed. Then, observe that the randomized-encoder code $\left\{ (Q_{i_1}^{P^*}, D_{i_1}^{(1)}) : i_1 \in [N_1'] \right\}$ is an $(n, N_1', \lambda_1^*, \lambda_2^*)$ ID code for the single-user channel $\mathcal{N}_{A \to B_1}^{(1)}$. Therefore, following the single-user converse proof by Ahlswede and Winter [13] (see also [17, Section III]),

$$R_1 = \frac{1}{n} \log \log(N_1') < \mathsf{I}(P^*, \mathcal{N}_{X \to B_1}^{(1)}) + \epsilon_1 = I(X; B_1)_\rho + \epsilon_1 \qquad (46)$$

where $X \sim P^*$ and ϵ_1 tends to zero as $\delta \to 0$. For completeness, we prove the inequality in the appendix. Similarly, we also have $R_2 < I(X; B_2)_\rho + \epsilon_2$. This completes the proof of the ID capacity theorem. $\square$

7 Summary and outlook

We derive an achievable ID region for the quantum broadcast channel and established full characterization for the classical-quantum broadcast channel. To prove achievability, we extend the classical proof due to Bracher and Lapidoth [24, 25] to the quantum setting. On the other hand, in the converse proof, we use the truncation approach by Boche et al. [17] along with the arguments of Ahlswede and Winter [13].

As examples, we derive explicit expressions for the ID capacity regions for the quantum erasure broadcast channel and for the pure-loss bosonic broadcast channel in Sect. 4. In those examples, each user can achieve the capacity of the respective marginal channel. In particular, the ID capacity region of the pure-loss bosonic broadcast channel is rectangular and strictly larger than the transmission capacity region. In general, the ID capacity region is not necessarily rectangular, as demonstrated for the classical Z-channel [30, Section IV.C] and the classical Gaussian Product channel [30, Section IV.E], [29, Section IV.B].

The ID capacity has a different behavior compared to the single-user setting, in which the ID capacity equals the transmission capacity [74] (see Sect. 2.3). Here, in the broadcast setting, the ID capacity region can strictly larger than in transmission, since interference between receivers can be seen as part of the randomization of the coding scheme.

Extending the results to more than two receivers remains an open challenge. Upper and lower bounds for such a model may be derived in a similar manner as in the classical setting [24, Section IV.A]. To derive the identification capacity of classical-quantum channels, new methods are required. The capacity of quantum-quantum channels is even unknown for general point-to-point discrete memoryless channels [14, 18]. These are interesting and challenging directions of further research.

Data availability A part of this paper was presented at the 2022 IEEE International Symposium on Information Theory [79]. A preprint of this work was posted on arXiv [80]. Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

A Quantum method of types

We review the basic method-of-types properties that will be useful in the analysis. The n-type $\hat{P}_{x^n}$ of a sequence $x^n \in \mathcal{X}^n$ is defined by $\hat{P}_{x^n}(a) = \frac{n(a|x^n)}{n}$ for $a \in \mathcal{X}$, where $n(a|x^n)$ is the number of occurrences of the letter a in the sequence x^n. The set of all n-types over a set $\mathcal{X}$ is denoted by $\mathcal{P}(n, \mathcal{X})$. Joint and conditional types are defined similarly, as in [73]. Furthermore, a δ-typical set is defined as follows. Given a PMF $P_X \in \mathcal{P}(\mathcal{X})$ over $\mathcal{X}$, define the robustly[1] δ-typical set,

$$\mathcal{T}_\delta^n(P_X) = \left\{ x^n \in \mathcal{X}^n : \left| \hat{P}_{x^n}(a) - P_X(a) \right| \leq \delta \cdot P_X(a), \ a \in \mathcal{X} \right\}. \qquad (47)$$

Given $P_{Y|X} : \mathcal{X} \to \mathcal{P}(\mathcal{Y})$, the *conditionally* δ-typical set $\mathcal{T}_\delta^n(x^n)$ is defined as the set of all sequences y^n such that $(x^n, y^n) \in \mathcal{T}_\delta^n(\hat{P}_{x^n} \times P_{Y|X})$. We will use the property (see [75, Lemma 2.12])

$$\Pr\left(X^n \in \mathcal{T}_\delta^n(P_X) \right) \geq 1 - 2 \left| \mathcal{X} \right| 2^{-2n\delta^2}. \qquad (48)$$

---

[1] This is the similar to strong ϵ-typicality [19], but we have $\epsilon = \delta P_X(a)$, which depends on a.

Consider the state A^n of a quantum system generated from an ensemble $\{P_X(x), |x\rangle\}_{x \in \chi}$. Then, the average density operator is $\rho = \sum_{x \in \mathcal{X}} P_X(x) |x\rangle\langle x|$. The projector onto the δ-typical subspace is defined as

$$\Pi_\delta^n(\rho) = \Pi_\delta^{A^n}(\rho) = \sum_{x^n \in \mathcal{T}_\delta^n(P_X)} |x^n\rangle\langle x^n|_{A^n}. \tag{49}$$

For every $\delta > 0$ and sufficiently large n, the δ-typical projector satisfies

$$\mathrm{Tr}(\Pi_\delta^n(\rho)\rho^{\otimes n}) \geq 1 - 2^{-b\delta n}, \tag{50}$$

$$2^{-n(H(\rho)+c\delta)} \Pi_\delta^n(\rho) \preceq \Pi_\delta^n(\rho)\,\rho^{\otimes n}\,\Pi_\delta^n(\rho)$$
$$\preceq 2^{-n(H(\rho)-c\delta)} \Pi_\delta^n(\rho), \tag{51}$$

$$\mathrm{Tr}(\Pi_\delta^n(\rho)) \leq 2^{n(H(\rho)+c\delta)} \tag{52}$$

where $b, c > 0$ are constants [76, Subsection 15.1.3], while the exponential convergence in (50) follows from Hoeffding's inequality [77, Theorem 1] (see proof of (48) in [75, Lemma 2.12]).

We will also need conditionally δ-typical subspaces. Consider a joint classical-quantum system (X^n, B^n) with density matrix $\sigma_{XB}^{\otimes n}$. Then, let $B_a(x^n) = \bigotimes_{i:x_i=a} B_i$ be the subsystem of B^n with indices i such that $x_i = a$, and note that there exists a cq-channel $\mathcal{N}_{X \to B} : a \mapsto (\langle a| \otimes \mathbb{1})\,\sigma_{XB}\,(|a\rangle \otimes \mathbb{1})\,/P_X(a)$. As in [76, Definition 15.2.3], the conditionally δ-typical projector $\Pi_\delta^n(\sigma_{XB}|x^n)$ is defined by

$$\Pi_\delta^n(\sigma_{XB}|x^n) = \bigotimes_{a \in \mathcal{X}} \Pi_\delta^{t(a|x^n)}\,(\mathcal{N}_{X \to B}(a)), \tag{53}$$

where $t(a|x^n) \equiv \{t : x_t = a\}$, and $\Pi_\delta^{t(a|x^n)}(\sigma_B)$ is the projector onto the subspace of $\mathcal{H}_B^{\otimes n}$ where the positions in $t(a|x^n)$ are δ-typical for σ_B. Given $x^n \in \mathcal{T}_\delta^n(P_X)$, it satisfies

$$\mathrm{Tr}\left(\Pi_\delta^n(\sigma_{XB}|x^n)\mathcal{N}(x^n)\right) \geq 1 - 2^{-b'\delta n}, \tag{54}$$

$$2^{-n(H(B|X)_\sigma+c'\delta)} \Pi_\delta^n(\sigma_{XB}|x^n) \preceq \Pi_\delta^n(\sigma_{XB}|x^n)\,\mathcal{N}(x^n)\,\Pi_\delta^n(\sigma_{XB}|x^n)$$
$$\preceq 2^{-n(H(B|X)_\sigma-c'\delta)} \Pi_\delta^n(\sigma_{XB}|x^n), \tag{55}$$

$$\mathrm{Tr}(\Pi_\delta^n(\sigma_{XB}|x^n)) \leq 2^{n(H(B|X)_\sigma+c'\delta)} \tag{56}$$

where $b', c' > 0$ is a constant, $\mathcal{N}(x^n) = \bigotimes_{i=1}^n \mathcal{N}_{X_i \to B_i}(x_i)$. Furthermore,

$$\mathrm{Tr}(\Pi_\delta^n(\sigma_B)\mathcal{N}(x^n)) \geq 1 - 2^{-c'\delta n} \tag{57}$$

(see [76, Property 15.2.7]), and hence, by the Gentle Operator Lemma [76, Lemma 9.4.2],

$$\left\|\mathcal{N}(x^n) - \Pi_\delta^n(\sigma_B)\,\mathcal{N}(x^n)\,\Pi_\delta^n(\sigma_B)\right\|_1 \leq 2^{-c'\delta n/2+1}. \tag{58}$$

B Error analysis for single-user achievability

We show that for some $\tau > 0$, the error probabilities of the random code $\mathcal{C}_\mathcal{B}$ satisfy

$$\lim_{n \to \infty} \Pr \left\{ \max_{i \in [N]} e_1(\mathcal{L}_{A \to B}, n, \mathcal{C}_\mathcal{B}, i) \geq e^{-n\tau} \right\} = 0, \tag{59a}$$

$$\lim_{n \to \infty} \Pr \left\{ \max_{i, i' \in [N]} \max_{i \neq i'} e_2(\mathcal{L}_{A \to B}, n, \mathcal{C}_\mathcal{B}, i', i) \geq e^{-n\tau} \right\} = 0. \tag{59b}$$

The codebook that is used here is the same as in the classical derivation [24, 25]. Hence, we can use the cardinality bounds for the index bins $\{\mathcal{V}_i\}_{i \in [N]}$ that were established in [24, 25]. Denote the collection of index bins by $\mathcal{V}^N = \{\mathcal{V}_i\}_{i \in [N]}$.

Lemma 1 *(see [24, Lemma 5]) Given $\mu > 0$, let $\mathcal{G}_\mu$ be the set of all realizations $\mathcal{V}^N$ of $\mathcal{V}^N$ such that*

$$|\mathcal{V}_i| > (1 - \delta_n)e^{n\tilde{R}}, \tag{60}$$

$$|\mathcal{V}_i| < (1 + \delta_n)e^{n\tilde{R}}, \tag{61}$$

$$|\mathcal{V}_i \cap \mathcal{V}_{i'}| < 2\delta_n e^{n\tilde{R}} \tag{62}$$

for all $\mathcal{V}_i, \mathcal{V}_{i'} \in \mathcal{V}^N$, $i \neq i'$, where $\delta_n = e^{-n\mu/2}$. Then, the probability that $\mathcal{V}^N \in \mathcal{G}_\mu$ converges to 1 as $n \to \infty$, i.e.

$$\lim_{n \to \infty} \Pr \left\{ \mathcal{V}^N \in \mathcal{G}_\mu \right\} = 1, \tag{63}$$

for $\mu < R_{pool} - \tilde{R}$.

Hence, it suffices to consider the bin collection realizations $\mathcal{V}^N$ of $\mathcal{V}^N$ that satisfy (61)–(62), for $\mu \in (0, R_{\text{pool}} - \tilde{R})$. Thus, the input state is as in (25), since $\mathcal{V}_i \neq \emptyset$ by (60).

Missed ID error
Consider an index bin $\mathcal{V}_i \in \mathcal{V}^N$. We bound the probability of the missed-ID error (first kind), given by

$$e_1(\mathcal{L}_{A \to B}, n, \mathcal{C}_\mathcal{B}, i) = \frac{1}{|\mathcal{V}_i|} \sum_{v \in \mathcal{V}_i} \Pr \left(a(v') = 0, \text{ for all } v' \in \mathcal{V}_i \,\middle|\, F(v) \text{ was sent} \right) \tag{64}$$

Note that for $\rho_{B^n}^{F(v)} = \mathcal{L}_{A \to B}(F(v))$,

$$\Pr \left(a(v') = 0, \text{ for all } v' \in \mathcal{V}_i \,\middle|\, F(v) \text{ was sent} \right)$$

$$= \text{Tr} \left(\prod_{v' \in \mathcal{V}_i} \left(\mathbb{1} - \Pi \Pi^{F(v')} \Pi \right) \rho_{B^n}^{F(v)} \right)$$

$$\leq \mathrm{Tr}\left(\left(\mathbb{1} - \Pi\Pi^{F(v)}\Pi\right)\rho_{B^n}^{F(v)}\right)$$

$$= 1 - \mathrm{Tr}\left(\Pi^{F(v)}\Pi\rho_{B^n}^{F(v)}\Pi\right)$$

$$\leq 1 - \mathrm{Tr}\left(\Pi^{F(v)}\rho_{B^n}^{F(v)}\right) + \left\|\rho_{B^n}^{F(v)} - \Pi\rho_{B^n}^{F(v)}\Pi\right\|_1. \tag{65}$$

By the Gentle Operator Lemma [76, Lemma 9.4.2], we have $\left\|\rho_{B^n}^{F(v)} - \Pi\rho_{B^n}^{F(v)}\Pi\right\|_1 \leq e^{-nc'\delta/2+1}$ (see (58)), because $F(v) \in \mathcal{T}_\delta^n(P_X)$, for all $v \in \mathcal{V}$. Since also $\mathrm{Tr}\left(\Pi^{F(v)}\rho_{B^n}^{F(v)}\right) \geq 1 - e^{-nb'\delta}$ (54), there exists $\tau_1 > 0$ such that

$$e_1(\mathcal{L}_{A\to B}, n, \mathcal{C}_\mathcal{B}, i) \leq e^{-nb'\delta} + e^{-nc'\delta/2+1} < e^{-n\tau_1}. \tag{66}$$

False ID error

Next, we bound the probability of an error of the second kind. Suppose that the sender sends an ID message i and the receiver is interested in $i' \neq i$. Recall that we can restrict our attention to realizations $\mathcal{V}^N = \{\mathcal{V}_i\} \in \mathcal{G}_\mu$, following Lemma 1. Let $v \in \mathcal{V}_i$ be the index that Alice has chosen. Observe that

$$e_2(\mathcal{L}_{A\to B}, n, \mathcal{C}_\mathcal{B}, i', i)$$

$$= \frac{1}{|\mathcal{V}_i|}\sum_{v\in\mathcal{V}_i}\mathrm{Pr}\left(\exists\, v' \in \mathcal{V}_{i'} : a(v') = 1 \,\big|\, F(v) \text{ was sent}\right)$$

$$\leq \frac{1}{|\mathcal{V}_i|}\sum_{v\in\mathcal{V}_i\cap\mathcal{V}_{i'}}1 + \frac{1}{|\mathcal{V}_i|}\sum_{v\in\mathcal{V}_i\cap\mathcal{V}_{i'}^c}\mathrm{Pr}\left(\exists\, v' \in \mathcal{V}_{i'} : a(v') = 1 \,\big|\, F(v) \text{ was sent}\right)$$

$$\leq \frac{|\mathcal{V}_i\cap\mathcal{V}_{i'}|}{|\mathcal{V}_i|}$$

$$+ \frac{1}{|\mathcal{V}_i\cap\mathcal{V}_{i'}^c|}\sum_{v\in\mathcal{V}_i\cap\mathcal{V}_{i'}^c}\mathrm{Pr}\left(\exists\, v' \in \mathcal{V}_{i'} : a(v') = 1 \,\big|\, F(v) \text{ was sent}\right), \tag{67}$$

since any probability is at most 1 and $\left|\mathcal{V}_i\cap\mathcal{V}_{i'}^c\right| \leq |\mathcal{V}_i|$. The first term is bounded by

$$\frac{|\mathcal{V}_i\cap\mathcal{V}_{i'}|}{|\mathcal{V}_i|} < \frac{2\delta_n}{1-\delta_n} < \delta_n \tag{68}$$

(see (60) and (62)), where the second inequality holds as $\delta_n < 1/2$, for sufficiently large n.

It remains to bound the second term in the right-hand side of (67), for which $v \in \mathcal{V}_i$ and $v \notin \mathcal{V}_{i'}$. For every pair of indices $v \notin \mathcal{V}_{i'}$ and $v' \in \mathcal{V}_{i'}$, we have that the codewords $F(v)$ and $F(v')$ are statistically independent.

Assume without loss of generality that $\mathcal{V}_{i'} = \{1, 2, \ldots, |\mathcal{V}_{i'}|\}$. Let $\mathcal{A}_{i'}(v')$ denote the event that $v' \in \mathcal{V}_{i'}$ is the first index to hit 'yes' as the measurement outcome, *i.e.*

$a(1) = a(2) = \cdots = a(v' - 1) = 0$ and $a(v') = 1$. Then,

$$
\begin{aligned}
\Pr\left(\mathcal{A}_{i'}(v') \,\middle|\, F(v) \text{ was sent}\right) &= \mathrm{Tr}\left(D_{v'} D^c_{v'-1} \cdots D^c_1 \, \rho^{F(v)}_{B^n} D^c_1 \cdots D^c_{v'-1}\right) \\
&\leq \mathrm{Tr}\left(D_{v'} \, \rho^{F(v)}_{B^n}\right) \\
&= \mathrm{Tr}\left(\Pi^{F(v')}\Pi \, \rho^{F(v)}_{B^n} \, \Pi\right)
\end{aligned}
\tag{69}
$$

where $D_v = \Pi\Pi^{F(v)}\Pi$, $D^c_v = \mathbb{1} - D_v$ and again $\rho^{F(v)}_{B^n} = \mathcal{L}_{A \to B}(F(v))$. Thus, we have

$$
\mathbb{E}_{\mathcal{B}}\left[\Pr\left(\mathcal{A}_{i'}(v') \,\middle|\, F(v) \text{ was sent}\right)\right] \leq \mathrm{Tr}\left(\mathbb{E}\left[\Pi^{F(v')}\right] \Pi \, \mathbb{E}\left[\rho^{F(v)}_{B^n}\right] \Pi\right),
\tag{70}
$$

and note that by (48), there exists ϵ_n with $\lim_{n\to\infty} = 0$ such that

$$
\mathbb{E}\left[\rho^{F(v)}_{B^n}\right] = \frac{1}{P_X(\mathcal{T}^n_\delta(P_X))} \sum_{x^n \in \mathcal{T}^n_\delta(P_X)} P^n_X(x^n)\rho^{x^n}_{B^n} = \frac{1}{1-\epsilon_n}\rho^{\otimes n}_B.
\tag{71}
$$

It follows that

$$
\begin{aligned}
(1 - \epsilon_n)\mathbb{E}_{\mathcal{B}}\left[\Pr\left(\mathcal{A}_{i'}(v') \,\middle|\, F(v) \text{ was sent}\right)\right] &= \mathrm{Tr}\left(\mathbb{E}\left[\Pi^{F(v')}\right] \Pi \, \rho^{\otimes n}_B \, \Pi\right) \\
&\overset{(a)}{\leq} e^{-n(H(B)_\rho - c\delta)} \, \mathrm{Tr}\left(\mathbb{E}\left[\Pi^{F(v')}\right] \Pi\right) \\
&\overset{(b)}{<} e^{-n(H(B)_\rho - H(B|X)_\rho - (c+c')\delta)} \\
&= e^{-n(I(X;B)_\rho - (c+c')\delta)},
\end{aligned}
\tag{72}
$$

where (a) holds by (51), and (b) by (56) since $F(v') \in \mathcal{T}^n_\delta(P_X)$ for all $v' \in \mathcal{V}$. Therefore, there exists $\theta > 0$ such that

$$
\begin{aligned}
\mathbb{E}_{\mathcal{B}}&\left[\Pr\left(\exists\, v' \in \mathcal{V}_{i'} : a(v') \,\middle|\, F(v) \text{ was sent}\right)\right] \\
&= \mathbb{E}_{\mathcal{B}}\left[\Pr\left(\exists\, v' \in \mathcal{V}_{i'} : \mathcal{A}_{i'}(v') \,\middle|\, F(v) \text{ was sent}\right)\right] \\
&\overset{(a)}{\leq} \frac{1}{1 - \epsilon_n} \sum_{v' \in \mathcal{V}_{i'}} \mathbb{E}_{\mathcal{B}}\left[\Pr\left(\mathcal{A}_{i'}(v') \,\middle|\, F(v) \text{ was sent}\right)\right] \\
&\leq \frac{1}{1 - \epsilon_n} |\mathcal{V}_{i'}| \, e^{-n(I(X;B) - (c+c')\delta)} \\
&\overset{(b)}{<} \frac{1 + \delta_n}{1 - \epsilon_n} e^{-n(I(X;B)_\rho - \tilde{R} - (c+c')\delta)} \\
&\overset{(c)}{<} e^{-n\theta},
\end{aligned}
\tag{73}
$$

where (a) follows from the union-of-events bound, (b) is due to (61), and (c) holds since $(c + c')\delta < I(X; B)_\rho - \tilde{R}$ by (26).

We show now that the false-ID error is small with high probability. Let α satisfy

$$0 < \alpha < (\tilde{R} - R)/2. \tag{74}$$

By the union-of-events bound,

$$\Pr\left(\max_{i' \in [N]} \max_{i \neq i'} e_2(\mathcal{L}_{A \to B}, n, \mathcal{C}_\mathcal{B}, i', i) \geq \delta_n + e^{-n\theta} + e^{-n\alpha}\right)$$
$$\leq \sum_{i' \in [N]} \sum_{i \neq i'} \Pr\left(e_2(\mathcal{L}_{A \to B}, n, \mathcal{C}_\mathcal{B}, i', i) \geq \delta_n + e^{-n\theta} + e^{-n\alpha}\right). \tag{75}$$

Note that by (67) and (68),

$$e_2(\mathcal{L}_{A \to B}, n, \mathcal{C}_\mathcal{B}, i', i)$$
$$\leq \delta_n + \frac{1}{\left|\mathcal{V}_i \cap \mathcal{V}_{i'}^c\right|} \sum_{v \in \mathcal{V}_i \cap \mathcal{V}_{i'}^c} \Pr\left(\exists\, v' \in \mathcal{V}_{i'} : a(v') = 1 \mid F(v) \text{ was sent}\right). \tag{76}$$

Therefore, there exists $\tau_2 > 0$ such that

$$\Pr\left\{\max_{i' \in [N]} \max_{i \neq i'} e_2(\mathcal{L}_{A \to B}, n, \mathcal{C}_\mathcal{B}, i', i) \geq e^{-n\tau_2}\right\}$$
$$\leq \sum_{i' \in [N]} \sum_{i \neq i'} \Pr\left\{\frac{1}{\left|\mathcal{V}_i \cap \mathcal{V}_{i'}^c\right|} \sum_{v \in \mathcal{V}_i \cap \mathcal{V}_{i'}^c} \Pr\left(\exists\, v' \in \mathcal{V}_{i'} : a(v') = 1 \mid F(v) \text{ was sent}\right)\right.$$
$$\left.\geq e^{-n\theta} + e^{-n\alpha}\right\}$$
$$\overset{(a)}{\leq} \exp\left(-2e^{-2n\alpha} \left|\mathcal{V}_i \cap \mathcal{V}_{i'}^c\right|\right)$$
$$\overset{(b)}{<} \exp\left(2e^{nR} - e^{-2n\alpha}e^{-n\tilde{R}}\right), \tag{77}$$

for sufficiently large n, where (a) follows from Hoeffding's inequality [77, Theorem 1], since the codewords $F(v)$, $v \in \mathcal{V}$ are i.i.d., (b) follows from $N = \exp\left(e^{nR}\right)$, and

$$\left|\mathcal{V}_i \cap \mathcal{V}_{i'}^c\right| = |\mathcal{V}_i| - |\mathcal{V}_i \cap \mathcal{V}_{i'}| > (1 - \delta_n)e^{n\tilde{R}} - 2\delta_n e^{n\tilde{R}} \geq e^{n\tilde{R}}/2, \tag{78}$$

as $|\mathcal{V}_i| \geq (1 - \delta_n)e^{n\tilde{R}}$ and $|\mathcal{V}_i \cap \mathcal{V}_{i'}| < 2\delta_n e^{n\tilde{R}}$, by Lemma 1 (see (60) and (62), respectively), where the last inequality follows from $\delta_n < 1/2$, for sufficiently large n.

Based on (66) and (77), we have established that (59) holds for $\tau = \min\{\tau_1, \tau_2\}$.

C Proof of inequality (46)

The rate bound is based on the combinatorial argument in the single-user converse proof, due to Ahlswede and Winter [13]. First, we define a quantum hypergraph and give the Ahlswede–Winter covering lemma [13].

Definition 2 A quantum hypergraph $(\mathcal{H}, \mathcal{G})$ is defined by a finite-dimensional Hilbert space $\mathcal{H}$ and a finite collection $\mathcal{G} = \{G_x\}_{x \in \mathcal{X}}$ of operators on $\mathcal{H}$, where $0 \preceq G_x \preceq \mathbb{1}$ for $x \in \mathcal{X}$.

Lemma 2 *(see [13, Lemma 9]) Let $(\mathcal{H}, \mathcal{G})$ be a quantum hypergraph such that $G \preceq \eta \mathbb{1}$ for all $G \in \mathcal{G}$, and fix $\epsilon, \tau > 0$. Given a probability distribution P on $\mathcal{G}$, define*

$$\rho = \sum_{G \in \mathcal{G}} P(G)G. \tag{79}$$

Then, there exists a subspace $\mathcal{H}_0 \subseteq \mathcal{H}$ and operators $G_1, \ldots, G_L \in \mathcal{G}$ such that

$$\mathrm{Tr}(\Pi_0 \rho) \leq \tau \tag{80}$$

$$(1 - \epsilon)\Pi_1 \rho \Pi_1 \preceq \Pi_1 \bar{\rho} \Pi_1 \preceq (1 + \epsilon)\Pi_1 \rho \Pi_1 \tag{81}$$

$$L \leq 1 + \eta|\mathcal{H}| \frac{2 \ln 2 \log(2|\mathcal{H}|)}{\epsilon^2 \tau} \tag{82}$$

with

$$\bar{\rho} = \frac{1}{L} \sum_{\ell=1}^{L} G_\ell, \tag{83}$$

while Π_0 and Π_1 are the orthogonal projections onto $\mathcal{H}_0$ and $\mathcal{H}_1 \equiv \mathcal{H}/\mathcal{H}_0$, respectively.

Intuitively, the covering lemma has the following interpretation. We can think of ρ as the average of an ensemble $\mathcal{G}$ of operators. Then, we consider a compressed ensemble, $\{G_1, \ldots, G_L\} \subseteq \mathcal{G}$, from which an operator is drawn uniformly. The resulting average of this compression is $\bar{\rho}$. Then, within the subspace $\mathcal{H}_1$, the projection $\Pi_1 \rho \Pi_1$ onto $\mathcal{H}_1$ is almost unaffected by the compression. The idea in the single-user converse proof for the classical-quantum channel $\mathcal{N}^{(1)}_{X \to B_1}$ is now to replace the arbitrary distributions Q_{i_1} of an ID code by uniform distributions $\overline{Q}_{i_1}$ on subsets of $\mathcal{A}_{P^*}$, with cardinality bounded by $L \approx e^{nI(P^*:\mathcal{N}^{(1)})}$. The condition is that the corresponding output states are close, so the resulting ID code will have similar error probabilities. As reliable identification requires the encoder to assign a different distribution $\overline{Q}_{i_1}$ to each message i_1, the number messages is thus bounded by the number of options for choosing L input sequences, which is $|\mathcal{X}^n|^L$. Now, we formalize this argument. Let $\lambda > 0$ be arbitrarily small, such that $\lambda < 1 - \lambda_1^* - \lambda_2^*$. Let $\Pi^\delta(B_1^n)$ and $\Pi_\delta^n(B_1^n|x^n)$ denote the δ-typical projector and the conditional δ-typical projector, respectively, for $\rho_{B_1} = \sum_{x \in \mathcal{X}} P^*(x)\mathcal{N}^{(1)}_{A \to B_1}(x)$. Then, denote the projection of each output state onto the

δ-typical subspace by

$$\Upsilon_{X^n \to B_1^n}(x^n) = \Pi^{2\delta}(B_1^n) \, \Pi_\delta^n(B_1^n|x^n) \, \mathcal{N}_{X^n \to B_1^n}^{(1)}(x^n) \, \Pi_\delta^n(B_1^n|x^n) \, \Pi^{2\delta}(B_1^n). \quad (84)$$

Then, for sufficiently large n,

$$\left\| \Upsilon(x^n) - \mathcal{N}^{(1)}(x^n) \right\|_1 \le \frac{\lambda}{6}, \quad (85)$$

for all $x^n \in \mathcal{A}_{P^*}$, by [78, Lemma V.9].

We apply Lemma 2 with $\epsilon = \tau = \frac{\lambda^2}{1200}$ to the quantum hypergraph for which the vertex space $\mathcal{H}$ is the range of $\Pi^{2\delta}(B_1^n)$, and the edges are $\Upsilon_{X^n \to B_1^n}(x^n)$, $x^n \in \mathcal{A}_{P^*}$. Thereby, for every $i_1 \in [N_1']$, there exist L_1 sequences $x^n(\ell_{i_1}) \in \mathcal{A}_{P^*}$,

$$L_1 = e^{n(\mathrm{I}(P^*;\mathcal{N}_{A \to B_1}^{(1)}) + \delta_n)}, \quad (86)$$

such that $G_{\ell_{i_1}} = \Upsilon_{X^n \to B_1^n}(x^n(\ell_{i_1}))$ satisfy the properties in the lemma, with $\overline{\rho}_{B_1^n}^{i_1} = \frac{1}{L_1} \sum_{j_{i_1}=1}^{L_1} \Upsilon_{X^n \to B_1^n}(x^n(j_{i_1}))$. Then, the uniform L_1-distribution $\overline{Q}_{i_1}^{P^*}$ satisfies

$$\left\| Q_{i_1}^{P^*} \Upsilon^{(k)} - \overline{Q}_{i_1}^{P^*} \Upsilon^{(k)} \right\|_1 \le \frac{\lambda}{6}. \quad (87)$$

Thus, by (85),

$$\left\| Q_{i_1}^{P^*} \mathcal{N}^{(1)} - \overline{Q}_{i_1}^{P^*} \mathcal{N}^{(1)} \right\|_1 \le \frac{\lambda}{3} \quad (88)$$

for $i_1 \in [N_1']$. Therefore, $\{\overline{Q}_{i_1}^{P^*}, D_{i_1}^{(1)}\}$ is an $(n, N_1', \lambda_1^* + \frac{\lambda}{3}, \lambda_2^* + \frac{\lambda}{3})$ code for the single-user channel $\mathcal{N}_{A \to B_1}^{(1)}$.

Since $\lambda_1^* + \lambda_2^* + \frac{2\lambda}{3} < 1$, each message must have a different input distribution. That is, $\overline{Q}_{i_1}^{P^*} \ne \overline{Q}_{i_1'}^{P^*}$ for $i_1 \ne i_1'$. As each $\overline{Q}_{i_1}^{P^*}$ is uniform over L_1 sequences in $\mathcal{X}^n$, it follows that

$$\begin{aligned} N_1' &\le |\mathcal{X}^n|^{L_1} \\ &= \exp(e^{n(\mathrm{I}(P^*;\mathcal{N}_{A \to B_1}^{(1)}) + \delta_n + \frac{1}{n}\log\log|\mathcal{X}|)}) \\ &\le \exp(e^{n(\mathrm{I}(P^*;\mathcal{N}_{A \to B_1}^{(1)}) + \epsilon_1)}) \end{aligned} \quad (89)$$

for sufficiently large n. Inequality (46) readily follows. $\qquad \square$

References

1. de Carvalho Silva, J., Rodrigues, J.J.P.C., Alberti, A.M., Solic, P., Aquino, A.L.L.: LoRaWAN—a low power WAN protocol for Internet of Things: a review and opportunities. In: 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), pp. 1–6 (2017)
2. Tariq, F., Khandaker, M.R.A., Wong, K.-K., Imran, M.A., Bennis, M., Debbah, M.: A speculative study on 6G. IEEE Wirel. Commun. **27**(4), 118–125 (2020). https://doi.org/10.1109/MWC.001.1900488
3. Fettweis, G.P., Boche, H.: 6g: the personal tactile internet—and open questions for information theory. IEEE BITS Inf. Theory Mag. (2021). https://doi.org/10.1109/MBITS.2021.3118662
4. Dang, S., Amin, O., Shihada, M.S.B., Alouini: What should 6G be? Nat. Electron. **3**(1), 20–29 (2020). https://doi.org/10.1038/s41928-019-0355-6
5. Shannon, C.E.: A mathematical theory of communication. Bell Syst. Tech. J. **27**(4), 623–656 (1948). https://doi.org/10.1002/j.1538-7305.1948.tb00917.x
6. Ahlswede, R., Dueck, G.: Identification via channels. IEEE Trans. Inf. Theory **35**(1), 15–29 (1989). https://doi.org/10.1109/18.42172
7. Steinberg, Y., Merhav, N.: Identification in the presence of side information with application to watermarking. IEEE Trans. Inf. Theory **47**(4), 1410–1422 (2001). https://doi.org/10.1109/18.923724
8. Moulin, P., Koetter, R.: A framework for the design of good watermark identification codes. In: III, E.J.D., Wong, P.W. (eds.) Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, pp. 565–574. SPIE (2006). https://doi.org/10.1117/12.644642
9. Ahlswede, R., Cai, N.: Watermarking identification codes with related topics on common randomness. In: General Theory of Information Transfer and Combinatorics. Lecture Notes in Computer Science, vol. 4123, pp. 107–153. Springer, Berlin Heidelberg (2006). https://doi.org/10.1007/11889342_7
10. Günlü, O., Kliewer, J., Schaefer, R.F., Sidorenko, V.: Doubly-exponential identification via channels: code constructions and bounds. In: IEEE International Symposium on Information Theory (ISIT'2021), pp. 1147–1152 (2021). https://doi.org/10.1109/ISIT45174.2021.9518193
11. Boche, H., Deppe, C.: Secure identification for wiretap channels; robustness, super-additivity and continuity. IEEE Trans. Inf. Forensics Secur. **13**(7), 1641–1655 (2018). https://doi.org/10.1109/TIFS.2018.2797004
12. Löber, P.: Quantum Channels and Simultaneous ID Coding. PhD thesis, Universität Bielefeld, Bielefeld, Germany. Preprint at arXiv: quant-ph/9907019 (1999)
13. Ahlswede, R., Winter, A.: Strong converse for identification via quantum channels. IEEE Trans. Inf. Theory **48**(3), 569–579 (2002). https://doi.org/10.1109/18.985947
14. Winter, A.: Identification via quantum channels. In: Information Theory, Combinatorics, and Search Theory, pp. 217–233. Springer, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36899-8_9
15. Ahlswede, R.: Identication and other probabilistic models, 1st edn. In: Foundations in Signal Processing, Communications and Networking. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-65072-8
16. Di Adamo, S., Boche, H.: The simultaneous identification capacity of the classical–quantum multiple access channel with stochastic encoders for transmission. Preprint at arXiv:1903.03395 (2019)
17. Boche, H., Deppe, C., Winter, A.: Secure and robust identification via classical-quantum channels. IEEE Trans. Inf. Theory **65**(10), 6734–6749 (2019). https://doi.org/10.1109/TIT.2019.2920952
18. Atif, T.A., Pradhan, S.S., Winter, A.: Quantum soft-covering lemma with applications to rate-distortion coding, resolvability and identification via quantum channels. Preprint at arXiv:2306.12416 (2023)
19. Wilde, M.M.: Quantum Information Theory, 2nd edn. Cambridge University Press, Cambridge (2017). https://doi.org/10.1017/9781316809976
20. Cover, T.M., Thomas, J.A.: Elements of Information Theory. John Wiley & Sons, Hoboken (2005). https://doi.org/10.1002/047174882x
21. Marton, K.: A coding theorem for the discrete memoryless broadcast channel. IEEE Trans. Inf. Theory **25**(3), 306–311 (1979). https://doi.org/10.1109/tit.1979.1056046
22. Nair, C., El Gamal, A.: An outer bound to the capacity region of the broadcast channel. IEEE Trans. Inf. Theory **53**(1), 350–355 (2007). https://doi.org/10.1109/TIT.2006.887492
23. El Gamal, A.: The capacity of a class of broadcast channels. IEEE Trans. Inf. Theory **25**(2), 166–169 (1979). https://doi.org/10.1109/TIT.1979.1056029
24. Bracher, A., Lapidoth, A.: Identification via the broadcast channel. IEEE Trans. Inf. Theory **63**(6), 3480–3501 (2017). https://doi.org/10.1109/TIT.2017.2674669

25. Bracher, A.: Identification and Zero-Error Codes. PhD thesis, ETH Zurich, Konstanz (2016). https://doi.org/10.3929/ethz-a-010739015

26. Verboven, B., van der Meulen, E.C.: Capacity bounds for identification via broadcast channels that are optimal for the determination broadcast channel. IEEE Trans. Inf. Theory **36**(6), 1197–1205 (1990). https://doi.org/10.1109/18.59922

27. Bilik, I, Steinberg, Y.: Inner and outer bounds on the identification capacity region of the degraded broadcast channel. In: Proceeding of IEEE International Symposium on Information Theory (ISIT'2001) (2001). https://doi.org/10.1109/isit.2001.936009

28. Ahlswede, R.: General theory of information transfer: Updated. Discret. Appl. Math. **156**(9), 1348–1388 (2008). https://doi.org/10.1016/j.dam.2007.07.007

29. Rosenberger, J., Pereg, U., Deppe, C.: Identification over compound MIMO broadcast channels. In: Proceedings of IEEE International Conference on Communications (ICC'2022), pp. 781–786 (2022). https://doi.org/10.1109/ICC45855.2022.9838478

30. Rosenberger, J., Pereg, U., Deppe, C.: Identification over compound multiple-input multiple-output broadcast channels. IEEE Trans. Inf. Theory **69**(7), 4178–4195 (2023). https://doi.org/10.1109/TIT.2023.3259580

31. Yard, J., Hayden, P., Devetak, I.: Quantum broadcast channels. IEEE Trans. Inf. Theory **57**(10), 7147–7162 (2011). https://doi.org/10.1109/TIT.2011.2165811

32. Savov, I., Wilde, M.M.: Classical codes for quantum broadcast channels. IEEE Trans. Inf. Theory **61**(12), 7017–7028 (2015). https://doi.org/10.1109/TIT.2015.2485998

33. Radhakrishnan, J., Sen, P., Warsi, N.: One-shot Marton inner bound for classical-quantum broadcast channel. IEEE Trans. Inf. Theory **62**(5), 2836–2848 (2016). https://doi.org/10.1109/TIT.2016.2531795

34. Wang, Q., Das, S., Wilde, M.M.: Hadamard quantum broadcast channels. Quantum Inform. Process. **16**(10), 248 (2017). https://doi.org/10.1007/s11128-017-1697-5

35. Dupuis, F., Hayden, P., Li, K.: A father protocol for quantum broadcast channels. IEEE Trans. Inf. Theory **56**(6), 2946–2956 (2010). https://doi.org/10.1109/TIT.2010.2046217

36. Dupuis, F.: The decoupling approach to quantum information theory. PhD thesis, Université de Montréal. Preprint at arXiv:1004.1641 (2009)

37. Hirche, C., Morgan, C.: An improved rate region for the classical-quantum broadcast channel. In: Proceedings of IEEE International Symposium on Information Theory (ISIT'2015), Hong Kong, pp. 2782–2786 (2015). https://doi.org/10.1109/ISIT.2015.7282963

38. Seshadreesan, K.P., Takeoka, M., Wilde, M.M.: Bounds on entanglement distillation and secret key agreement for quantum broadcast channels. IEEE Trans. Inf. Theory **62**(5), 2849–2866 (2016). https://doi.org/10.1109/TIT.2016.2544803

39. Bäuml, S., Azuma, K.: Fundamental limitation on quantum broadcast networks. Quantum Sci. Tech. **2**(2), 024004 (2017). https://doi.org/10.1088/2058-9565/aa6d3c

40. Heinosaari, T., Miyadera, T.: Incompatibility of quantum channels. J. Phys. A Math. Theor. **50**(13), 135302 (2017). https://doi.org/10.1088/1751-8121/aa5f6b

41. Boche, H., Cai, M., Deppe, C.: The broadcast classical-quantum capacity region of a two-phase bidirectional relaying channel. Quantum Inf. Process. **14**(10), 3879–3897 (2015). https://doi.org/10.1007/s11128-015-1065-2

42. Hirche, C.: Polar codes in quantum information theory. Master's thesis, Leibniz Universität Hannover (2015)

43. Xie, W., Wang, X., Duan, R.: Converse bounds for classical communication over quantum broadcast channels and quantum multi-access channels. In: Proceedings of IEEE International Symposium on Information Theory (ISIT'2018), pp. 2341–2345 (2018). https://doi.org/10.1109/ISIT.2018.8437766

44. De Palma, G.: New lower bounds to the output entropy of multi-mode quantum gaussian channels. IEEE Trans. Inf. Theory **65**(9), 5959–5968 (2019). https://doi.org/10.1109/TIT.2019.2914434

45. Anshu, A., Jain, R., Warsi, N.A.: Building blocks for communication over noisy quantum networks. IEEE Trans. Inf. Theory **65**(2), 1287–1306 (2019). https://doi.org/10.1109/TIT.2018.2851297

46. Cheng, H.C., Datta, N., Rouzé, C.: Strong converse for classical-quantum degraded broadcast channels. Preprint at arXiv:1905.00874 (2019)

47. Pereg, U., Deppe, C., Boche, H.: Quantum broadcast channels with cooperating decoders: an information-theoretic perspective on quantum repeaters. J. Math. Phys. **62**(6), 062204 (2021). https://doi.org/10.1063/5.0038083

48. Salek, F., Hsieh, M.H., Fonollosa, J.R.: Publicness, privacy and confidentiality in the single-serving quantum broadcast channel. Preprint at arXiv:1903.04463 (2019)

49. Salek, F., Hsieh, M., Fonollosa, J.R.: Publicness, privacy and confidentiality in the single-serving quantum broadcast channel. In: Proceedings of IEEE International Symposium on Information Theory (ISIT'2019), Paris, pp. 1712–1716 (2019). https://doi.org/10.1109/ISIT.2019.8849633

50. Bardhan, B.R., Shapiro, J.H.: Ultimate capacity of a linear time-invariant bosonic channel. Phys. Rev. A **93**(3), 032342 (2016). https://doi.org/10.1103/PhysRevA.93.032342

51. Pereg, U.: Bosonic dirty paper coding. In: Proceedings of IEEE International Symposium on Information Theory (ISIT'2021) (2021). https://doi.org/10.1109/ISIT45174.2021.9518053

52. Pereg, U.: Communication over quantum channels with parameter estimation. IEEE Trans. Inf. Theory **68**(1), 359–383 (2022). https://doi.org/10.1109/TIT.2021.3123221

53. Kumar, S., Deen, M.J.: Fiber Optic Communications: Fundamentals and Applications. John Wiley & Sons, Hoboken (2014). https://doi.org/10.1002/9781118684207

54. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S.: Gaussian quantum information. Rev. Mod. Phys. **84**, 621–669 (2012). https://doi.org/10.1103/RevModPhys.84.621

55. Wilde, M.M., Hayden, P., Guha, S.: Quantum trade-off coding for bosonic communication. Phys. Rev. A **86**(6), 062306 (2012). https://doi.org/10.1103/PhysRevA.86.062306

56. Guha, S., Shapiro, J.H.: Classical information capacity of the bosonic broadcast channel. In: Proceedings of IEEE International Symposium on Information Theory (ISIT'2007), Nice, pp. 1896–1900 (2007). https://doi.org/10.1109/ISIT.2007.4557498

57. Guha, S., Shapiro, J.H., Erkmen, B.I.: Classical capacity of bosonic broadcast communication and a minimum output entropy conjecture. Phys. Rev. A **76**(3), 032303 (2007). https://doi.org/10.1103/PhysRevA.76.032303

58. De Palma, G., Mari, A., Giovannetti, V.: A generalization of the entropy power inequality to bosonic quantum systems. Nat. Photonics **8**(12), 958 (2014). https://doi.org/10.1038/nphoton.2014.252

59. Takeoka, M., Seshadreesan, K.P., Wilde, M.M.: Unconstrained distillation capacities of a pure-loss bosonic broadcast channel. In: Proceedings of IEEE International Symposium on Information Theory (ISIT'2016), Barcelona, pp. 2484–2488 (2016). https://doi.org/10.1109/ISIT.2016.7541746

60. Takeoka, M., Seshadreesan, K.P., Wilde, M.M.: Unconstrained capacities of quantum key distribution and entanglement distillation for pure-loss bosonic broadcast channels. Phys. Rev. Lett. **119**(15), 150501 (2017). https://doi.org/10.1103/PhysRevLett.119.150501

61. Laurenza, R., Pirandola, S.: General bounds for sender-receiver capacities in multipoint quantum communications. Phys. Rev. A **96**(3), 032318 (2017). https://doi.org/10.1103/PhysRevA.96.032318

62. Anderson, E., Guha, S., Bash, B.: Fundamental limits of bosonic broadcast channels. In: Proceedings of IEEE International Symposium on Information Theory (ISIT'2021) (2021). https://doi.org/10.1109/ISIT45174.2021.9518198

63. Pereg, U., Ferrara, R., Bloch, M.R.: Key Assistance, key agreement, and layered secrecy for bosonic broadcast channels. In: Proceedings of the IEEE Information Theory Workshop (ITW'2021), pp. 1–6 (2021). https://doi.org/10.1109/ITW48936.2021.9611359

64. Winter, A.: Quantum and classical message identification via quantum channels. Preprint at arXiv:quant-ph/0401060 (2004)

65. Ahlswede, R., Dueck, G.: Identification in the presence of feedback—a discovery of new capacity formulas. IEEE Trans. Inf. Theory **35**(1), 30–36 (1989). https://doi.org/10.1109/18.42173

66. Holevo, A.S., Werner, R.F.: Evaluating capacities of bosonic gaussian channels. Phys. Rev. A **63**(3), 032312 (2001). https://doi.org/10.1103/PhysRevA.63.032312

67. Eisert, J., Wolf, M.M.: Gaussian quantum channels. Preprint at arXiv: quant-ph/0505151 (2005)

68. Giovannetti, V., Guha, S., Lloyd, S., Maccone, L., Shapiro, J.H., Yuen, H.P.: Classical capacity of the lossy bosonic channel: the exact solution. Phys. Rev. Lett. **92**(2), 027902 (2004)

69. Qi, H., Wilde, M.M., Guha, S.: On the minimum output entropy of single-mode phase-insensitive gaussian channels. Preprint at arXiv: 1607.05262 (2016)

70. De Palma, G., Trevisan, D., Giovannetti, V.: Gaussian states minimize the output entropy of the one-mode quantum attenuator. IEEE Trans. Inf. Theory **63**(1), 728–737 (2017)

71. Pereg, U., Ferrara, R., Bloch, M.R.: Key Assistance, key agreement, and layered secrecy for bosonic broadcast channels. Preprint at arXiv:2105.04033 (2021)

72. De Palma, G.: New lower bounds to the output entropy of multi-mode quantum gaussian channels. IEEE Trans. Inf. Theory **65**(9), 5959–5968 (2019)

73. El Gamal, A., Kim, Y.-H.: Network Information Theory. Cambridge University Press, Cambridge (2011). https://doi.org/10.1017/CBO9781139030687

74. Watanabe, S.: Minimax converse for identification via channels. IEEE Trans. Inf. Theory **68**(1), 25–34 (2022). https://doi.org/10.1109/TIT.2021.3120033
75. Csiszár, I., Körner, J.: Information Theory: Coding Theorems for Discrete Memoryless Systems, 2nd edn. Cambridge University Press, Cambridge (2011). https://doi.org/10.1017/CBO9780511921889
76. Wilde, M.M.: Quantum Information Theory, 2nd edn. Cambridge University Press, Cambridge (2017). https://doi.org/10.1017/9781316809976
77. Hoeffding, W.: Probability inequalities for sums of bounded random variables. J. Am. Stat. Assoc. **58**(301), 13–30 (1963). https://doi.org/10.1080/01621459.1963.10500830
78. Winter, A.: Coding theorem and strong converse for quantum channels. IEEE Trans. Inf. Theory **45**(7), 2481–2485 (1999). https://doi.org/10.1109/18.796385
79. Pereg, U., Rosenberger, J., Deppe, C.: Identification over quantum broadcast channels. In: Proceedings of the IEEE International Symposium on Information Theory (ISIT'2022), pp. 258–263 (2022). https://doi.org/10.1109/ISIT50566.2022.9834865
80. Pereg, U., Rosenberger, J., Deppe, C.: Identification over quantum broadcast channels. Preprint at arXiv:2201.11056 (2022)