



When quantum memory is useful for dense coding

Ryuji Takagi^{1,2} · Masahito Hayashi^{3,4,5}

Received: 19 June 2023 / Revised: 6 April 2024 / Accepted: 27 May 2024 /
Published online: 22 June 2024
© The Author(s), under exclusive licence to Springer Nature B.V. 2024

Abstract

We discuss dense coding with n copies of a specific preshared state between the sender and the receiver when the encoding operation is limited to the application of group representation. Typically, to act on multiple local copies of these preshared states, the receiver needs quantum memory, because in general the multiple copies will be generated sequentially. Depending on available encoding unitary operations, we investigate what preshared state offers an advantage of using quantum memory on the receiver's side.

Keywords Dense coding · Preshared state · Group representation · Quantum memory

Mathematics Subject Classification 81P48 · 81P40 · 81P17 · 81R05

1 Introduction

Quantum dense coding is a key subroutine in many quantum information processing tasks. Dense coding utilizes preshared entanglement among the sender and receiver to communicate more classical bits than the number of quantum bits sent from the

✉ Ryuji Takagi
ryujitakagi.pat@gmail.com

✉ Masahito Hayashi
hmasahito@cuhk.edu.cn

¹ Department of Basic Science, Graduate School of Arts and Sciences, The University of Tokyo, 3-8-1 Komaba, Meguro-ku, Meguro-ku 153-8902, Tokyo, Japan

² Nanyang Quantum Hub, School of Physical and Mathematical Sciences, Nanyang Technological University, 637371 Singapore, Singapore

³ School of Data Science, The Chinese University of Hong Kong, Shenzhen 518172, China

⁴ International Quantum Academy (SIQA), Shenzhen 518048, China

⁵ Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan

sender to receiver [1–13]. It is well known that one preshared maximally entangled qubit together with one bit of quantum communication admits communicating two bits of classical information. Although it is evident that preshared entanglement is a necessary resource to enable dense coding, *how* entanglement helps the enhancement is still unclear—the presence of entanglement in a preshared state does not necessarily guarantee to enhance classical communication for a given encoding strategy. It is therefore important to characterize when entanglement indeed becomes helpful for dense coding.

This question can be approached by observing that holding entanglement during communication requires the receiver to store the preshared state in a quantum memory. If the receiver is not in possession of quantum memory but instead makes a measurement right after the preshared state is provided, entanglement is broken before the communication is completed. Therefore, characterizing when quantum memory enhances the classical communication rate gives insights into the role genuinely played by quantum entanglement. This question also has practical relevance, as preparing a long-term quantum memory may come with much technical difficulty [14, 15].

As the simplest setting, we restrict our encoding operations to a certain subgroup under the presence of preshared states [13]—we assume that the encoding operation is given as a (projective) unitary representation U of a group G on \mathcal{H}_A . When the preshared entangled state is written as ρ_{AB} and our coding operation is restricted to these unitaries, our channel can be written as the classical-quantum (cq) channel $g \mapsto U_g \rho_{AB} U_g^\dagger$. Since this cq channel has a symmetric property for the group G , we say that it is a *cq-symmetric* channel¹. Recently, Ref. [16] studied such a model in the context of the resource theory of asymmetry without considering shared entanglement. Reference [13] applied cq-symmetric channel to the above setting under the presence of shared entanglement.

In Ref. [13], two scenarios are considered; the first where Bob has to wait for the quantum communication from Alice before he can perform a global measurement on all systems, and a second where Bob is allowed to apply a global measurement on his local part of the shared states before he receives Alice’s communication. While the second system reduces memory requirements at Bob, Bob still requires quantum memory when the preshared states are generated one by one.

In this work, in order to model the lack of quantum memory, we consider a third case where Bob measures his local part of the entangled states one by one and investigate when the capacities of these three cases coincide. The practical meaning of the first and third cases are compared in Sect. 2.3.1, Remark 1. In particular, we study the conditions for a preshared entangled state when the capacities for the second and third case differ under which quantum memory becomes helpful in dense coding, whose encoding is realized by the action of a given group representation. We also relate our

¹ The class of cq-symmetric channels has been studied well in the literature [16]. It is a quantum generalization of a regular channel [17], which was introduced as a useful class of channels in classical information theory. This class of classical channels has various names, such as generalized additive [18, Section V] and conditional additive [18, Section 4] channels. The class of additive channels is contained in the regular channels as a subclass. The reference [19, Section VII-A-2] studied its quantum extension with an additive group and discussed the capacity and the wire-tap capacity with semantic security. Since this class has a good symmetric property, it is known that algebraic codes achieve the capacity [17, 19–22].

setting to private dense coding with the existence of an eavesdropper, extending the private capacity characterized for the first model, i.e., the case when the receiver is allowed to make a collective measurement on the joint system [23].

We begin by studying the setting involving an arbitrary preshared state and an arbitrary group representation, where we provide necessary (and sufficient) conditions for a quantum memory to be useful. Using a necessary condition, we show an example of an entangled state, in which the capacities are equal and quantum memory is useless in this sense. We then focus on pure preshared states and give an explicit structure of the preshared state such that the receiver does not need to hold a quantum memory to realize the optimal decoding. Imposing the multiplicity-free condition on the group representation, we establish a novel connection between dense coding and the resource theory of speakable coherence [24]—equivalent to the resource theory of asymmetry with $U(1)$ group with a multiplicity-free representation—which brings us a further characterization of such pure preshared states.

In fact, the resource theory of asymmetry is a topic to study physical resources for information processing and has been under active investigation [12, 25–34]. In the context of quantum hypothesis testing, the references [35] and [36, Theorem 2.9] considered the difference with respect to the relative entropy between a state and the averaged state under a certain group action, where the averaged state is the output of the noisy channel composed of a random unitary application. This relative entropy shows the difficulty of distinguishing the noiseless state and the noisy averaged state under a certain group action. Here, we discuss this type of discrimination as a modification of quantum illumination, which was originally introduced for enhancing the capability of detecting a target object with low reflectivity using entanglement [37, 38]. In particular, we apply our conditions to characterize when the entanglement in a given input state enhances the performance in guessing whether the noiseless or the group twirling channel acted on the entanglement half. We find that in the case of asymmetric discrimination with an abelian group, the performance with a maximally entangled input cannot be enhanced by local quantum memory, which can be contrasted to the conventional quantum illumination, in which quantum memory is essential when the input is a two-mode squeezing vacuum state [39].

The remainder of this paper is organized as follows. Section 2 formulates the two cases of interest for quantum dense coding. Section 2.1 formulates the case with quantum memory allowing for the global measurement, and Sect. 2.3 formulates the case without quantum memory after Sect. 2.2 prepares the notations for group representation. Section 3 discusses when quantum memory is useless for a general preshared state and presents several examples of such entangled states. Section 4 investigates simpler conditions for pure states and presents relevant examples. This analysis reveals the relation between the usefulness of quantum memory and the genuinely incoherent operations (GIO), a class of operations introduced in the resource theory of speakable coherence [40]. Section 5 applies obtained results to the case of the maximally entangled states. Section 6 applies our results to a modified version of quantum illumination. Section 7 provides discussion for our results and suggests future studies.

2 Dense coding with a preshared state

2.1 Dense coding with quantum memory

2.1.1 Standard capacity

We formulate dense coding with a preshared state as in Ref. [13], which is based on a cq-symmetric channel [16]. Assume that Alice and Bob share n copies of the quantum state ρ_{AB} on the system $\mathcal{H} := \mathcal{H}_A \otimes \mathcal{H}_B$, where \mathcal{H}_B is a d_B -dimensional system. We consider a (projective) unitary group representation of a group G on \mathcal{H}_A . That is, for each $g \in G$, we have a unitary operator U_g on \mathcal{H}_A such that for $g, g' \in G$, there exists a unit complex number $c(g, g')$ satisfying

$$U_g U_{g'} = c(g, g') U_{gg'}. \tag{1}$$

When $c(g, g')$ is 1, $\{U_g\}_{g \in G}$ is called a unitary group representation. Otherwise, it is called a projective unitary group representation. We also define the group twirling channel $\mathcal{G}(\rho) := \sum_{g \in G} \frac{1}{|G|} U_g \rho U_g^\dagger$.

Consider the case when encoding operation is given as an application of unitary. In practical scenario, due to the device condition, available unitaries are limited to a subset of unitaries. Since any combination of available unitaries is also available, it is natural to assume that the set of available unitaries is given as a (projective) unitary group representation of a group G on \mathcal{H}_A . In this scenario, we cannot exclude the case that $c(g, g')$ takes a non-identical element in general. For example, when the X and Z operations are available on a qubit system, $c(g, g')$ may take a non-identical element. Thus, our problem is formulated as channel coding for the cq-channel $g (\in G) \mapsto U_g \rho_{AB} U_g^\dagger$. Since this cq-channel has a group covariant form, the channel capacity $C_c(\rho_{AB})$ of this channel is calculated as [41, 42]

$$\begin{aligned} C_c(\rho_{AB}) &= \sup_p H \left(\sum_{g \in G} p(g) U_g \rho_{AB} U_g^\dagger \right) - \sum_{g \in G} p(g) H(U_g \rho_{AB} U_g^\dagger) \\ &= \sup_p H \left(\sum_{g \in G} p(g) U_g \rho_{AB} U_g^\dagger \right) - H(\rho_{AB}) \\ &= H(\mathcal{G}(\rho_{AB})) - H(\rho_{AB}) \\ &= D(\rho_{AB} \| \mathcal{G}(\rho_{AB})), \end{aligned} \tag{2}$$

where $H(\rho) := -\text{Tr} \rho \log \rho$, $D(\rho \| \sigma) = \text{Tr} \rho (\log \rho - \log \sigma)$. In the following, we use the word ‘‘capacity’’ to denote the channel capacity. Here, we used the following relation.

$$H \left(\sum_{g \in G} p(g) U_g \rho_{AB} U_g^\dagger \right) = \sum_{g' \in G} \frac{1}{|G|} H \left(\sum_{g \in G} p(U_{g'} g U_{g'}^\dagger) U_g \rho_{AB} U_g^\dagger \right)$$

$$\leq H \left(\sum_{g' \in G} \frac{1}{|G|} \sum_{g \in G} p(U_{g'} g U_{g'}^\dagger) U_g \rho_{AB} U_g^\dagger \right) = H \left(\sum_{g \in G} \frac{1}{|G|} U_g \rho_{AB} U_g^\dagger \right).$$

We describe here the first case with quantum memory mentioned above. In this case, Alice transmits a message to Bob with n uses of this cq-channel. The set of available encoding operations is characterized by the product group $G^n = \overbrace{G \times \dots \times G}^n$. The n -tensor product representation of U is given as $U_{(g_1, \dots, g_n)} := U_{g_1} \otimes \dots \otimes U_{g_n}$ for $(g_1, \dots, g_n) \in G^n$. By using the n -tensor product representation, a classical message $k \in \mathcal{K}_n$ is encoded by using an encoder

$$\phi_{e,n} : K_n \rightarrow G^n \tag{3}$$

and applying $U_{\phi_{e,n}(k)}$ to her local copies and sending them to Bob, thus producing the state

$$U_{\phi_{e,n}(k)} \rho_{AB} U_{\phi_{e,n}(k)}^\dagger \tag{4}$$

at Bob, effectively producing the cq channel from Alice to Bob. Using quantum memories to store the whole state, Bob then decodes the message using a decoder POVM

$$\phi_{d,n} = \{\Pi_k\}_{k \in \mathcal{K}_n} \tag{5}$$

on $\mathcal{H}_A \otimes \mathcal{H}_B$.

A pair of an encoder $\phi_{e,n}$ and a decoder $\phi_{d,n}$ is called a code Φ_n . The performance of a code Φ_n is evaluated by the size of \mathcal{K}_n denoted by $|\mathcal{K}_n|$ and the averaged decoding error probability $\epsilon(\Phi_n)$ given as

$$\epsilon(\Phi_n) := \frac{1}{|\mathcal{K}_n|} \sum_{k \in \mathcal{K}_n} \left(1 - \text{Tr} U_{\phi_{e,n}(k)} \rho_{AB}^{\otimes n} U_{\phi_{e,n}(k)}^\dagger \Pi_k \right). \tag{6}$$

Then, the channel coding theorem for cq-channels [43, 44] states that the quantity in (2) gives the operational capacity, i.e.,

$$C_c(\rho_{AB}) = \sup_{\{\Phi_n\}} \left\{ \lim_{n \rightarrow \infty} \frac{1}{n} \log |\mathcal{K}_n| \mid \lim_{n \rightarrow \infty} \epsilon(\Phi_n) = 0 \right\}. \tag{7}$$

2.1.2 Private capacity

In addition, the recent paper [23] considers private dense coding that covers a risk that the eavesdropper, Eve, might intercept the transmitted state and thus obtain (a part of) the information for the transmitted message. In this case, if Eve wants to hide her attack, she applies another quantum channel to the intercepted system, sends the output to Bob, and keeps its environment system. However, if she does not need to hide her attack, she does not need to send the output to Bob. We also assume that Eve has the environment system of the state ρ_{AB} , i.e., the joint state among Alice, Bob, and Eve is a pure state ρ_{ABE} . In this case, the following two conditions are required.

- (1) When Eve does not intercept the transmitted state, Bob recovers the message with a probability of almost 1.
- (2) Even when Eve intercepts the transmitted state, Eve obtains no information about the message.

This problem was studied in the case with a preshared maximally entangled state [45] and a general noisy preshared state [23]. When Alice and Bob share the maximally entangled state, Eve obtains no information about the message even when Eve intercepts the transmitted state [45]. In this case, the conventional dense coding satisfies the above two conditions. In the general noisy case with a general state ρ_{AB} , the reference [23] derived the following lower bound \underline{C}_c^p of the private capacity C_c^p as

$$C_c^p(\rho_{AB}) \geq \underline{C}_c^p(\rho_{AB}) = D(\rho_{AB} \parallel \mathcal{G}(\rho_{AB})) - D(\rho_{AE} \parallel \mathcal{G}(\rho_{AE})). \tag{8}$$

In particular, it is known that the above value gives the private capacity when ρ_{AB} is a maximally correlated state [23, Appendix A].

2.2 Notations for group representation

For further study on the capacity $C_c(\rho_{AB})$ under the given symmetry, we prepare several notations for group representation. We let \hat{G} denote a set of irreducible projective unitary representations of G . For all irreducible representations $\lambda \in \hat{G}$, let \mathcal{H}_λ be the projective representation space and d_λ be its dimension. In general, the representation space \mathcal{H}_A can be written as

$$\mathcal{H}_A = \bigoplus_{\lambda \in \hat{G}'} \mathcal{H}_\lambda \otimes \mathcal{M}_\lambda, \tag{9}$$

where $\mathcal{M}_\lambda = \mathbb{C}^{n_\lambda}$ expresses the multiplicity space of the irreducible projective unitary presentation λ , the integer n_λ is the multiplicity, and $\hat{G}' \subset \hat{G}$ is the set of irreducible representations with $n_\lambda > 0$ for \mathcal{H}_A . Since our representation is unitary, vectors in different irreducible components are orthogonal to each other. Hence, we can write our space in the above way. Therefore, recalling $\mathcal{H}_B = \mathbb{C}^{d_B}$, the joint system $\mathcal{H}_A \otimes \mathcal{H}_B$ is written as

$$\mathcal{H}_A \otimes \mathcal{H}_B = \bigoplus_{\lambda \in \hat{G}'} \mathcal{H}_\lambda \otimes \mathbb{C}^{n_\lambda d_B}. \tag{10}$$

Let Π_λ be the projection to $\mathcal{H}_\lambda \otimes \mathcal{M}_\lambda = \mathcal{H}_\lambda \otimes \mathbb{C}^{n_\lambda}$. Defining the probability distribution $P_\Lambda(\lambda) := \text{Tr}(\Pi_\lambda \otimes I_B)\rho_{AB}$ where we denote by Λ the corresponding random variable and the state $\rho_\lambda := \frac{1}{P_\Lambda(\lambda)}(\Pi_\lambda \otimes I_B)\rho_{AB}(\Pi_\lambda \otimes I_B)$, we have

$$\mathcal{G}(\rho_{AB}) = \bigoplus_{\lambda \in \hat{G}'} P_\Lambda(\lambda) \frac{1}{d_\lambda} I_\lambda \otimes \text{Tr}_{\mathcal{H}_\lambda}(\rho_\lambda), \tag{11}$$

where I_B and I_λ are the identity operators acting on \mathcal{H}_B and \mathcal{H}_λ , respectively. This gives

$$H(\mathcal{G}(\rho_{AB})) = H(P_\Lambda) + \sum_{\lambda \in \hat{G}'} P_\Lambda(\lambda) \left(\log d_\lambda + H(\text{Tr}_{\mathcal{H}_\lambda} \rho_\lambda) \right). \tag{12}$$

Therefore, the capacity $C_c(\rho_{AB})$ admits the following form.

$$C_c(\rho_{AB}) = H(P_\Lambda) + \sum_{\lambda \in \hat{G}'} P_\Lambda(\lambda) \left(\log d_\lambda + H(\text{Tr}_{\mathcal{H}_\lambda} \rho_\lambda) \right) - H(\rho_{AB}). \tag{13}$$

When ρ_{AB} is a pure state, this reduces to [13]

$$\begin{aligned} C_c(\rho_{AB}) &= H(P_\Lambda) + \sum_{\lambda \in \hat{G}'} P_\Lambda(\lambda) \left(\log d_\lambda + H(\text{Tr}_{\mathcal{H}_\lambda} \rho_\lambda) \right) \\ &= H(P_\Lambda) + \sum_{\lambda \in \hat{G}'} P_\Lambda(\lambda) \left(\log d_\lambda + H(\text{Tr}_{M_\lambda} \rho_\lambda) \right) \end{aligned} \tag{14}$$

where the second equality (changing the system of the trace) follows because ρ_λ is also a pure state.

To simplify our analysis, let us introduce the following condition on a unitary representation.

Definition 1 (*Multiplicity-free condition*) We say that a unitary representation U of G on \mathcal{H} is *multiplicity-free* when there exists a subset $\hat{G}' \subset \hat{G}$ such that the unitary representation U is equivalent to

$$\bigoplus_{\lambda \in \hat{G}'} \mathcal{H}_\lambda, \tag{15}$$

namely, when all multiplicities are either 0 or 1, and \hat{G}' is the set of all irreducible representations such that $n_\lambda = 1$.

2.3 Dense coding without quantum memory

2.3.1 Standard capacity

To achieve the capacity $C_c(\rho_{AB})$, Bob needs to keep his state in his quantum memory while first $\mathcal{H}_B^{\otimes n}$ and then $\mathcal{H}_A^{\otimes n}$ are collected. Since the cost to keep quantum memory is expensive, it is practical to replace it with classical memory by performing a projective measurement on each system \mathcal{H}_B as they are received. To this end, let $\mathcal{B} := \{|k\rangle\}_{k=1}^{d_B}$ be Bob's measurement basis on \mathcal{H}_B . We also let \mathcal{B} denote the measurement channel with respect to the basis \mathcal{B} . When Bob applies the measurement \mathcal{B} , the initial preshared

state is given by

$$\mathcal{B}(\rho_{AB}) := \sum_k \langle k | \rho_{AB} | k \rangle \otimes |k\rangle \langle k| = \sum_k P_K(k) \rho_{A|k}, \tag{16}$$

where

$$\begin{aligned} P_K(k) &:= \text{Tr}_A \langle k | \rho_{AB} | k \rangle \\ \rho_{A|k} &:= \frac{1}{P_K(k)} \langle k | \rho_{AB} | k \rangle \otimes |k\rangle \langle k| \end{aligned} \tag{17}$$

When Bob makes a measurement with the basis \mathcal{B} on every quantum system \mathcal{H}_B in advance, the capacity of (2) satisfies (notice that \mathcal{G} acts on A and thus commutes with B)

$$C_c(\mathcal{B}(\rho_{AB})) = D(\mathcal{B}(\rho_{AB}) \| \mathcal{G} \circ \mathcal{B}(\rho_{AB})) = D(\mathcal{B}(\rho_{AB}) \| \mathcal{B} \circ \mathcal{G}(\rho_{AB})). \tag{18}$$

Here, since the support of $\mathcal{B} \circ \mathcal{G}(\rho_{AB})$ contains the support of $\mathcal{B}(\rho_{AB})$, the above quantity does not diverge.

Indeed, even when Bob sends his measurement outcome to Alice before Alice sends her message, the capacity has the same value because it does not distinguish whether k is at Alice or Bob, as can be seen in the following. We have the capacity of this setting as

$$\begin{aligned} \sum_{k=1}^{d_B} P_K(k) C_c(\rho_{A|k}) &= \sum_{k=1}^{d_B} P_K(k) (H(\mathcal{G}(\rho_{A|k})) - H(\rho_{A|k})) \\ &= H(\mathcal{G}(\mathcal{B}(\rho_{AB}))) - H(\mathcal{B}(\rho_{AB})) \\ &= D(\mathcal{B}(\rho_{AB}) \| \mathcal{G} \circ \mathcal{B}(\rho_{AB})) \\ &= C_c(\mathcal{B}(\rho_{AB})). \end{aligned} \tag{19}$$

The data-processing inequality for the relative entropy implies that for all measurements \mathcal{B}

$$C_c(\rho_{AB}) = D(\rho_{AB} \| \mathcal{G}(\rho_{AB})) \geq D(\mathcal{B}(\rho_{AB}) \| \mathcal{B} \circ \mathcal{G}(\rho_{AB})) = C_c(\mathcal{B}(\rho_{AB})). \tag{20}$$

When the equality in (20) holds with a measurement \mathcal{B} , Bob’s quantum memory is useless with respect to the measurement \mathcal{B} . We call such a state ρ_{AB} *\mathcal{B} - q -memory useless*. In particular, when there exists such a measurement \mathcal{B} , we call such a state ρ_{AB} *q -memory useless*. Otherwise, we call the state ρ_{AB} *q -memory useful*. Our aim is to characterize the condition when the equality holds.

Here, it is instructive to clarify the difference between the setting in Ref. [13] and ours. Reference [13] discussed the channel capacity when Bob is allowed to make a measurement across n -tensor product space $\mathcal{H}_B^{\otimes n}$ before Bob receives the transmitted systems. In contrast, we allow Bob to apply a measurement only on a single system

\mathcal{H}_B n times. That is, in our setting, Bob is not allowed to apply quantum measurements over multiple copies of preshared states on Bob’s side before the communication. The measurement in Ref. [13] is called a collective measurement and our measurement here is called an individual measurement. Reference [13] studied the setting with a collective measurement at the asymptotic limit $n \rightarrow \infty$. They showed that the optimal transmission rate under their setting becomes $C_c(\rho_{AB})$ when the group G is abelian, the representation U is multiplicity-free, and the state ρ_{AB} is pure. Although their setting does not ask Bob to keep the quantum system before receiving the other parts from Alice, it still requires quantum memory in Bob’s system. This is because when Bob receives these n quantum systems one by one, he needs to store these n quantum systems before making a measurement across his n quantum systems $\mathcal{H}_B^{\otimes n}$. On the other hand, our setting described above prohibits the use of quantum memory.

Remark 1 In our setting, we allow a collective measurement across many quantum systems received by Alice at the decoding stage, although a collective measurement is not allowed on shared quantum systems distributed to Bob. This assumption is justified by considering the situation where the communication from Alice to Bob is done within a short period of time while it takes much longer for quantum systems to be distributed to Bob before the communication. Indeed, if the use of the quantum communication channel is expensive, this scenario is reasonable for the following reasons. The distribution step (before the communication) can take a longer time because it is a preparation for the communication between Alice and Bob. Since fast communication channels are expensive, it is reasonable to use slower channels for distributing shared quantum systems. In such a case, to make a collective measurement on shared quantum systems distributed to Bob, Bob needs to have a quantum memory to keep his quantum systems for a long time. On the other hand, the communication from Alice to Bob typically needs to be accomplished quickly, where they are expected to use faster communication channels. There, Bob does not need to hold a good quantum memory lasting for a long time to make a collective measurement over the quantum systems received in a short period of time from Alice.

2.3.2 Private capacity

Next, we discuss the private dense coding when Bob makes a measurement with the basis \mathcal{B} . We have the following lower bound for the private capacity [23]

$$\underline{C}_c^P(\rho_{AB}, \mathcal{B}) = D(\mathcal{B}(\rho_{AB}) \parallel \mathcal{G} \circ \mathcal{B}(\rho_{AB})) - D(\rho_{AE} \parallel \mathcal{G}(\rho_{AE})). \tag{21}$$

The difference between $\underline{C}_c^P(\rho_{AB})$ and $\underline{C}_c^P(\rho_{AB}, \mathcal{B})$ is given by

$$\begin{aligned} \underline{C}_c^P(\rho_{AB}) - \underline{C}_c^P(\rho_{AB}, \mathcal{B}) &= D(\rho_{AB} \parallel \mathcal{G}(\rho_{AB})) - D(\mathcal{B}(\rho_{AB}) \parallel \mathcal{B} \circ \mathcal{G}(\rho_{AB})) \\ &= C_c(\rho_{AB}) - C_c(\mathcal{B}(\rho_{AB})) \geq 0. \end{aligned} \tag{22}$$

Therefore, the equality condition in (20) is useful for comparing the lower bounds for these two private capacities.

3 General preshared states

3.1 Conditions for q-memory uselessness

We begin our investigation of conditions for q-memory uselessness with a general mixed preshared resource state. We denote with ρ^{-1} the pseudoinverse of an operator ρ on \mathcal{H} and its support \mathcal{H}_ρ . For the general case, we consider $[\mathcal{G} \circ \mathcal{B}(\rho_{AB})]^{-1}$ of $\mathcal{G} \circ \mathcal{B}(\rho_{AB})$ and denote the support of the operator $\mathcal{G} \circ \mathcal{B}(\rho_{AB})$ as $\mathcal{H}_{\mathcal{B},\mathcal{G},\rho_{AB}}$. Then, the supports of $\mathcal{B}(\rho_{AB})$, $\mathcal{G}(\rho_{AB})$, and ρ_{AB} are included in $\mathcal{H}_{\mathcal{B},\mathcal{G},\rho_{AB}}$. Applying the equality condition for the information processing inequality for relative entropy [46] to (20), we have the following characterizations.

Theorem 1 *Given a preshared state ρ_{AB} and the basis \mathcal{B} , the following conditions are equivalent.*

- (A1) *The equality in (20) holds, i.e., ρ_{AB} is \mathcal{B} -q-memory useless.*
- (A2) *The following relation holds as an operator on $\mathcal{H}_{\mathcal{B},\mathcal{G},\rho_{AB}}$.*

$$\rho_{AB} = \sqrt{\mathcal{G}(\rho_{AB})}\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}\mathcal{B}(\rho_{AB})\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}\sqrt{\mathcal{G}(\rho_{AB})}. \tag{23}$$

- (A3) *There exists a CPTP map Γ such that*

$$\Gamma(\mathcal{B}(U_g\rho_{AB}U_g^\dagger)) = U_g\rho_{AB}U_g^\dagger \tag{24}$$

for $g \in G$.

Proof The equivalence between (A1) and (A2) follows from [47, Theorem 3]. The relation (A3) \Rightarrow (A1) is trivial. Assume (A2). We have $U_g\mathcal{G}(\rho_{AB}) = \mathcal{G}(\rho_{AB})U_g$ and $U_g\mathcal{G} \circ \mathcal{B}(\rho_{AB}) = \mathcal{G} \circ \mathcal{B}(\rho_{AB})U_g$. We denote the space orthogonal to $\mathcal{H}_{\mathcal{B},\mathcal{G},\rho_{AB}}$ by $\mathcal{H}_{\mathcal{B},\rho_{AB}}^\perp$. We denote the projection to $\mathcal{H}_{\mathcal{B},\rho_{AB}}^\perp$ by I^\perp . We consider $\sqrt{\mathcal{G}(\rho_{AB})}\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}$ as a map on $\mathcal{H}_{\mathcal{B},\mathcal{G},\rho_{AB}}$. Then, we can define the map $T := \sqrt{\mathcal{G}(\rho_{AB})}\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1} \oplus I^\perp$ on \mathcal{H} .

Since $U_g\sqrt{\mathcal{G}(\rho_{AB})}U_g^{-1} = \sqrt{\mathcal{G}(\rho_{AB})}$ and $U_g\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}U_g^{-1} = \sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}$, we have $\sqrt{\mathcal{G}(\rho_{AB})}\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}U_g = U_g\sqrt{\mathcal{G}(\rho_{AB})}\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}$. Thus, we have

$$\begin{aligned} & TU_g\mathcal{B}(\rho_{AB})U_g^\dagger T^\dagger \\ &= \sqrt{\mathcal{G}(\rho_{AB})}\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}U_g\mathcal{B}(\rho_{AB})U_g^\dagger\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}\sqrt{\mathcal{G}(\rho_{AB})} \\ &= U_g\sqrt{\mathcal{G}(\rho_{AB})}\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}\mathcal{B}(\rho_{AB})\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1}\sqrt{\mathcal{G}(\rho_{AB})}U_g^\dagger \\ &= U_g\rho_{AB}U_g^\dagger, \end{aligned} \tag{25}$$

where the final equation follows from the condition (A2). Defining $\Gamma(\rho) := T\rho T^\dagger$, we have (A3). □

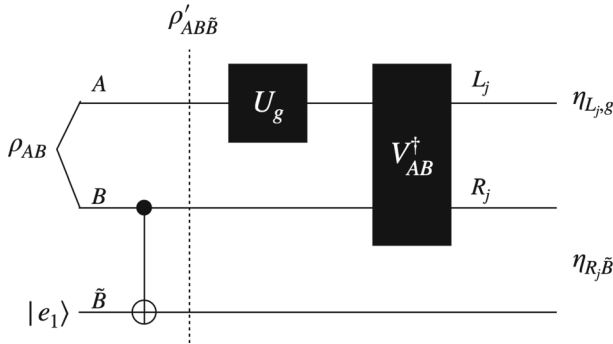


Fig. 1 Circuit representation of the conditions in Theorem 2

We remark that the above results can be extended to a general quantum channel \mathcal{B} following the same proof. Apart from (23), we obtain an alternative necessary and sufficient condition for a general resource state ρ_{AB} using the result in Ref. [47].

Theorem 2 Let \tilde{B} be a system isomorphic to B and $CX_{B \rightarrow \tilde{B}} := \sum_{k, k'=1}^{d_B} |k\rangle\langle k|_B \otimes |k' + k\rangle\langle k'|_{\tilde{B}}$, where $k' + k$ is implicitly $k' + k \bmod d_B$, be the CNOT gate with respect to the basis \mathcal{B} controlled on B . Let $\rho'_{AB\tilde{B}}$ be the state on $AB\tilde{B}$ defined as

$$\rho'_{AB\tilde{B}} := CX_{B \rightarrow \tilde{B}} (\rho_{AB} \otimes |0\rangle\langle 0|_{\tilde{B}}) CX_{B \rightarrow \tilde{B}}^\dagger \tag{26}$$

Then, the condition $C_c(\rho_{AB}) = C_c(\mathcal{B}(\rho_{AB}))$ holds if and only if there exist the following six items satisfying the condition (27).

- (1) an index set \mathcal{J} , which is possibly an infinite set,
- (2) a decomposition $\mathcal{H}_A \otimes \mathcal{H}_B = \bigoplus_{j \in \mathcal{J}} \mathcal{H}_{L_j} \otimes \mathcal{H}_{R_j}$ for some subspaces \mathcal{H}_{L_j} and \mathcal{H}_{R_j} ,
- (3) states $\eta_{L_j, g}$ on \mathcal{H}_{L_j} that can depend on g ,
- (4) states $\eta_{R_j, \tilde{B}}$ on $\mathcal{H}_{R_j} \otimes \mathcal{H}_{\tilde{B}}$ independent of g ,
- (5) a probability distribution $\{p_{j|g}\}_j$ for each $g \in G$,
- (6) a unitary V_{AB} on AB .

$$U_g \rho'_{AB\tilde{B}} U_g^\dagger = V_{AB} \left(\bigoplus_j p_{j|g} \eta_{L_j, g} \otimes \eta_{R_j, \tilde{B}} \right) V_{AB}^\dagger, \quad \forall g \in G. \tag{27}$$

Proof Step 1. First, we introduce another useful necessary and sufficient condition for the equation $C_c(\rho_{AB}) = C_c(\mathcal{B}(\rho_{AB}))$. Define the classical-quantum state

$$\tau_{GAB} := \sum_{g \in G} \frac{1}{|G|} |g\rangle\langle g| \otimes U_g \rho_{AB} U_g^\dagger. \tag{28}$$

To take into account the action of Bob’s measurement, we also consider a classical-quantum state

$$\tau'_{GAB\tilde{B}} := CX_{B \rightarrow \tilde{B}} \tau_{GAB} \otimes |0\rangle\langle 0|_{\tilde{B}} CX_{B \rightarrow \tilde{B}}^\dagger = \sum_{g \in G} \frac{1}{|G|} |g\rangle\langle g| \otimes U_g \rho'_{AB\tilde{B}} U_g^\dagger, \tag{29}$$

where $\rho'_{AB\tilde{B}}$ is the state defined in (26). This gives

$$\tau'_{GAB} := \text{Tr}_{\tilde{B}}(\tau'_{GAB\tilde{B}}) = \sum_{g \in G} \frac{1}{|G|} |g\rangle\langle g| \otimes U_g \mathcal{B}(\rho_{AB}) U_g^\dagger. \tag{30}$$

Note that due to the invariance of the relative entropy under isometries like in (29), we have

$$C_c(\rho_{AB}) = D(\tau_{GAB} \| \tau_G \otimes \tau_{AB}) = D(\tau'_{GAB\tilde{B}} \| \tau'_G \otimes \tau'_{AB\tilde{B}}). \tag{31}$$

On the other hand, Eq. (30) implies that

$$C_c(\mathcal{B}(\rho_{AB})) = D(\tau'_{GAB} \| \tau'_G \otimes \tau'_{AB}). \tag{32}$$

Therefore, $C_c(\rho_{AB}) = C_c(\mathcal{B}(\rho_{AB}))$ if and only if

$$D(\tau'_{GAB\tilde{B}} \| \tau'_G \otimes \tau'_{AB\tilde{B}}) = D(\tau'_{GAB} \| \tau'_G \otimes \tau'_{AB}). \tag{33}$$

Step 2. Next, employing condition (33), we show that the existence of the six items is equivalent to the equation $C_c(\rho_{AB}) = C_c(\mathcal{B}(\rho_{AB}))$. Applying the result from Ref. [47, Theorem 6], we get that (33) holds if and only if there exists a decomposition of Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ as

$$\mathcal{H}_A \otimes \mathcal{H}_B = \bigoplus_j \mathcal{H}_{L_j} \otimes \mathcal{H}_{R_j} \tag{34}$$

such that

$$\tau'_{GAB\tilde{B}} = V_{AB} \left(\bigoplus_j q_j \eta_{GL_j} \otimes \eta_{R_j\tilde{B}} \right) V_{AB}^\dagger \tag{35}$$

for some unitary V_{AB} on AB and for some states η_{GL_j} on $\mathcal{H}_G \otimes \mathcal{H}_{L_j}$ and $\eta_{R_j\tilde{B}}$ on $\mathcal{H}_{R_j} \otimes \mathcal{H}_{\tilde{B}}$. Since Eq. (34) corresponds to the items (1) and (2), it is sufficient to show the equivalence between (35) and the condition (27) with the items (3), (4), (5), and 6), which does not come with the subsystem G holding a classical state.

Suppose $\tau'_{GAB\tilde{B}}$ has the form (35). Because of (29), we have

$$\sum_{g \in G} |g\rangle\langle g| \tau'_{GAB\tilde{B}} |g\rangle\langle g| = \tau'_{GAB\tilde{B}}. \tag{36}$$

This implies that

$$\sum_{g \in G} |g\rangle\langle g| \eta_{GL_j} |g\rangle\langle g| = \eta_{GL_j} \forall j. \tag{37}$$

This condition requires η_{GL_j} to have classical states on the subsystem G , which has the classical-quantum form

$$\eta_{GL_j} = \sum_{g \in G} |g\rangle\langle g| \otimes c_{j,g} \eta_{L_j,g}, \quad \forall j \tag{38}$$

for some coefficient $c_{j,g}$ and some state $\eta_{L_j,g}$ on \mathcal{H}_{L_j} . Since $\text{Tr}\langle g|\tau'_{GAB\tilde{B}}|g\rangle = 1/|G|$ by (29), we have $\sum_j q_j c_{j,g} = 1/|G|, \forall g \in G$. Together with the form in (29), we get

$$U_g \rho'_{AB\tilde{B}} U_g^\dagger = V_{AB} \left(\bigoplus_j p_{j|g} \eta_{L_j,g} \otimes \eta_{R_j\tilde{B}} \right) V_{AB}^\dagger, \quad \forall g \in G \tag{39}$$

where $p_{j|g} := |G| q_j c_{j,g}$ constructs a probability distribution labeled by g with $\sum_j p_{j|g} = 1$. Since this is the form advertised in (27), we just showed that (35) implies (27).

On the other hand, one can recover the form of (35) by applying $\frac{1}{|G|} \sum_g |g\rangle\langle g| \otimes$ from left in both sides of (27), which means that (27) implies (35). Therefore, (27) and (35) are equivalent, which concludes the proof. \square

Let us consider a mixed-state example that satisfies the conditions in Theorem 2. Clearly, when the state ρ_{AB} has the following separable form

$$\rho_{AB} = \sum_{k=1}^{d_B} P_K(k) |\psi_k\rangle\langle\psi_k| \otimes |k\rangle\langle k|, \tag{40}$$

we have $\mathcal{B}(\rho_{AB}) = \rho_{AB}$, which implies the equality of the capacities in (20). That is, the state ρ_{AB} is \mathcal{B} -q-memory useless. However, a general separable state cannot be written in the form (40) even when the basis $\{|k\rangle\}_{k=1}^{d_B}$ can be freely chosen because a general separable state is written with the sum of non-orthogonal product states. Hence, it is, in general, unclear whether a general separable state ρ_{AB} is q-memory useless.

Let us now investigate whether there exists an entangled q-memory useless state.

Proposition 3 *Let ρ_{AB} be a state having the following form*

$$\rho_{AB} = \sum_j P_J(j) |\Psi_j\rangle\langle\Psi_j|, \tag{41}$$

where the state $|\Psi_j\rangle$ has the form

$$|\Psi_j\rangle = \sum_{k=1}^{d_B} e^{i\theta_{k,j}} \sqrt{P_{K|J}(k|j)} \sum_{\lambda \in \hat{G}'} e^{i\theta_{\lambda,k}} \sqrt{P_\Lambda(\lambda)} |\psi_{\lambda,k}\rangle \otimes |k\rangle, \tag{42}$$

and the vector $|\psi_{\lambda,k}\rangle \in \mathcal{H}_\lambda \otimes \mathcal{M}_\lambda$ satisfies

$$\text{Tr}_{\mathcal{M}_\lambda} |\psi_{\lambda,k}\rangle \langle \psi_{\lambda,k}| = \text{Tr}_{\mathcal{M}_\lambda} |\psi_{\lambda,k'}\rangle \langle \psi_{\lambda,k'}| \tag{43}$$

for every k, k' . Then, there is a basis \mathcal{B} such that the conditions for Theorem 2 hold. That is, the state ρ_{AB} is q -memory useless.

Proof Step 1 First, we observe that for each $|\psi_{\lambda,k}\rangle$ in (42) there exists a Schmidt decomposition

$$|\psi_{\lambda,k}\rangle = \sum_j \sqrt{c_{\lambda,j}} |r_{\lambda,j}\rangle_{\mathcal{H}_\lambda} |m_{\lambda,k,j}\rangle_{\mathcal{M}_\lambda} \tag{44}$$

where neither $c_{\lambda,j}$ nor $|r_{\lambda,j}\rangle$ depends on k . This is because the marginal states for $|\psi_{\lambda,k}\rangle$ on \mathcal{H}_λ do not depend on k because of (43), and thus we can use the same eigenbasis for \mathcal{H}_λ in the Schmidt decomposition, recalling that any eigenbasis of the marginal state gives a Schmidt basis.

Step 2 Next, employing the form in (44), we show that ρ_{AB} in (41) satisfies the conditions in Theorem 2. Let us define $|\Psi'_j\rangle$ as

$$|\Psi'_j\rangle := \text{CX}_{B \rightarrow \tilde{B}} |\Psi_j\rangle |0\rangle_{\tilde{B}}, \tag{45}$$

where $|0\rangle_{\tilde{B}}$ is a computational basis state on \tilde{B} . Then, using (42) and (44), we can write

$$|\Psi'_j\rangle = \sum_\lambda \sqrt{P_\Lambda(\lambda)} \sum_{k=1}^{d_B} \sqrt{P_{K|J}(k|j)} e^{i(\theta_{\lambda,k} + \theta_{k,j})} \sum_l \sqrt{c_{\lambda,l}} |r_{\lambda,l}\rangle_{\mathcal{H}_\lambda} |m_{\lambda,k,l}\rangle_{\mathcal{M}_\lambda} |k\rangle_B |k\rangle_{\tilde{B}}. \tag{46}$$

Applying $U_g = \bigoplus_\lambda U_{\lambda,g} \otimes I_{\mathcal{M}_\lambda}$ to $|\Psi'\rangle$, we get

$$\begin{aligned} & U_g |\Psi'_j\rangle \\ &= \sum_\lambda \sqrt{P_\Lambda(\lambda)} \sum_{k=1}^{d_B} \sqrt{P_{K|J}(k|j)} e^{i(\theta_{\lambda,k} + \theta_{k,j})} \sum_l \sqrt{c_{\lambda,l}} |r_{\lambda,g,l}\rangle_{\mathcal{H}_\lambda} |m_{\lambda,k,l}\rangle_{\mathcal{M}_\lambda} |k\rangle_B |k\rangle_{\tilde{B}} \end{aligned} \tag{47}$$

where $|r_{\lambda,g,l}\rangle := U_{\lambda,g} |r_{\lambda,l}\rangle$. Let $V_k := \bigoplus_\lambda e^{-i\theta_{\lambda,k}} I_{\mathcal{H}_\lambda} \otimes \sum_l |m_{\lambda,l}\rangle \langle m_{\lambda,k,l}|_{\mathcal{M}_\lambda}$ be a unitary on A where $\{|m_{\lambda,l}\rangle\}_l$ is an arbitrary basis independent of k . We then define a controlled unitary $V_{AB} := \sum_{k=1}^{d_B} V_k \otimes |k\rangle \langle k|_B$. We get

$$\begin{aligned} & V_{AB} U_g |\Psi'_j\rangle \\ &= \sum_\lambda \sqrt{P_\Lambda(\lambda)} \sum_{k=1}^{d_B} e^{i\theta_{k,j}} \sqrt{P_{K|J}(k|j)} \sum_l \sqrt{c_{\lambda,l}} |r_{\lambda,g,l}\rangle_{\mathcal{H}_\lambda} |m_{\lambda,l}\rangle_{\mathcal{M}_\lambda} |k\rangle_B |k\rangle_{\tilde{B}} \end{aligned}$$

$$= \left(\sum_{\lambda} \sqrt{P_{\Lambda}(\lambda)} \sum_l \sqrt{c_{\lambda,l}} |r_{\lambda,g,l}\rangle_{\mathcal{H}_{\lambda}} |m_{\lambda,l}\rangle_{\mathcal{M}_{\lambda}} \right) \otimes \left(\sum_{k=1}^{d_B} e^{i\theta_{k,j}} \sqrt{P_{K|J}(k|j)} |k\rangle_B |k\rangle_{\bar{B}} \right) \tag{48}$$

$$=: |\Psi_{A,g}\rangle \otimes |\Psi_{B\bar{B},j}\rangle \tag{49}$$

Therefore, we have for the state $\rho_{AB} = \sum_j P_J(j) |\Psi_j\rangle \langle \Psi_j|$ that

$$V_{AB} U_g \rho_{AB} U_g^{\dagger} V_{AB}^{\dagger} = |\Psi_{A,g}\rangle \langle \Psi_{A,g}| \otimes \sum_j P_J(j) |\Psi_{B\bar{B},j}\rangle \langle \Psi_{B\bar{B},j}|. \tag{50}$$

This is the form in (27), where we choose $L_j = A, R_j = B$ for item 2) in Theorem 2. This concludes the proof that the state ρ_{AB} in (41) satisfies the conditions in Theorem 2. □

3.2 Examples of entangled q-memory useless state based on Proposition 3

We derive examples of entangled q-memory useless states using Proposition 3. This construction contains mixed states as well as pure states. To simplify the condition in Proposition 3, we assume that our unitary representation U_g of G on \mathcal{H} is multiplicity-free. Then, the condition (42) is rewritten as

$$|\Psi_j\rangle = \sum_{k=1}^{d_B} e^{i\theta_{k,j}} \sqrt{P_{K|J}(k|j)} \left(\sum_{\lambda \in \hat{G}'} e^{i\theta_{\lambda,k}} \sqrt{P_{\Lambda}(\lambda)} |\psi_{\lambda}\rangle \right) \otimes |k\rangle. \tag{51}$$

where \hat{G}' with $|\hat{G}'| = l$ is a subset of irreducible representations. We write the set \hat{G}' as $\{\lambda_s\}_{s=1}^l$ and remember that the basis \mathcal{B} is written as $\{|k\rangle\}_{k=1}^{d_B}$. As a special case, let $d_B = l, P_{K|J}(k|j) = P_{\Lambda}(\lambda_s) = \frac{1}{l}, \theta_{\lambda_s,k} = \frac{2\pi sk}{l},$ and $\theta_{k,j} = \frac{2\pi jk}{l}$. The states

$$|\phi_k\rangle := \sum_{\lambda_s \in \hat{G}'} e^{i \frac{2\pi sk}{l}} \sqrt{P_{\Lambda}(\lambda_s)} |\psi_{\lambda_s}\rangle, \quad k = 1, \dots, d_B \tag{52}$$

form normalized orthogonal vectors. The states $|\Psi_j\rangle$ with $j = 1, \dots, l$ are simplified as

$$|\Psi_j\rangle = \sum_{k=1}^l e^{i \frac{2\pi jk}{l}} \frac{1}{\sqrt{l}} |\phi_k\rangle \otimes |k\rangle. \tag{53}$$

We find that the states $|\Psi_j\rangle$ with $j = 1, \dots, l$ also form normalized orthogonal vectors and are all examples of entangled q-memory useless states. Then, the state $\rho_{AB} = \sum_{j=1}^l P_J(j) |\Psi_j\rangle \langle \Psi_j|$ is separable if and only if P_J is the uniform distribution on $\{1, \dots, l\}$ [48]. In this case, the state ρ_{AB} is written as

$$\rho_{AB} = \frac{1}{l} \sum_{k=1}^l |\Psi_j\rangle\langle\Psi_j| = \frac{1}{l} \sum_{k=1}^l |\phi_k\rangle\langle\phi_k| \otimes |k\rangle\langle k|. \tag{54}$$

In addition, the state ρ_{AB} in the example is a maximally correlated state with respect to the basis $\{|\phi_k\rangle \otimes |k'\rangle\}_{k,k'=1}^l$. Hence, the lower bound $\underline{C}_c^p(\rho_{AB})$ of the private capacity equals the private capacity in this case [23, Appendix A]. The above example also guarantees that $\underline{C}_c^p(\rho_{AB}) = \underline{C}_c^p(\rho_{AB}, \mathcal{B})$. Thus, $\underline{C}_c^p(\rho_{AB}, \mathcal{B})$ also attains the private capacity. In this case, even when Bob makes a measurement in the basis \mathcal{B} , Alice and Bob can attain the private capacity. That is, Bob’s quantum memory is not needed even for private dense coding.

3.3 Examples of entangled q-memory useless state based on Condition (A2)

Let G be commutative and \mathcal{H}_A be multiplicity free, and consider the maximally entangled state

$$|\Phi\rangle = \sum_{s=1}^l \frac{1}{\sqrt{l}} |\psi_{\lambda_s}\rangle |v_{\lambda_s}\rangle \tag{55}$$

where the set \hat{G}' of irreducible representations appearing in \mathcal{H}_A is given as $\{\lambda_s\}_{s=1}^l$ and $\{|v_{\lambda_s}\rangle\}_{s=1}^l$ are orthogonal states on \mathcal{H}_B defined by

$$|v_{\lambda_s}\rangle = \frac{1}{\sqrt{l}} \sum_{k=1}^l e^{-2\pi k\lambda_s i/l} |k\rangle. \tag{56}$$

Although the previous section shows the fact that the maximally entangled state $|\Phi\rangle$ is q-memory useless by using Proposition 3, this section shows the same fact by using the condition (A2).

Note that

$$|\Phi\rangle = \frac{1}{l} \sum_{k=1}^l \sum_{s=1}^l e^{-2\pi k\lambda_s i/l} |\psi_{\lambda_s}\rangle |k\rangle \tag{57}$$

Therefore, defining $|\phi_k\rangle := \frac{1}{\sqrt{l}} \sum_{s=1}^l |\psi_{\lambda_s}\rangle$, we obtain the following lemma.

Lemma 4 *The maximally entangled state $|\Phi\rangle$ has the following form.*

$$|\Phi\rangle = \frac{1}{\sqrt{l}} \sum_{k=1}^l |\phi_k\rangle |k\rangle. \tag{58}$$

While the capacity is $\log l$, it can be achieved even when Bob measures the system B with the basis $\{|e_k\rangle\}_k$ because the resultant state on A is $|\phi_k\rangle$ and $H(\mathcal{G}(|\phi_k\rangle\langle\phi_k|)) = \log l$. Hence, $|\Phi\rangle$ is q-memory useless.

This q-memory useless property can be seen from the fact that the state $|\Phi\rangle$ satisfies the condition (A2) as follows. We have

$$\mathcal{B}(|\Phi\rangle\langle\Phi|) = \frac{1}{l} \sum_{k=1}^l |\phi_k\rangle\langle\phi_k| \otimes |k\rangle\langle k| \tag{59}$$

$$\mathcal{G}(|\Phi\rangle\langle\Phi|) = \frac{1}{l} \sum_{s=1}^l |\psi_{\lambda_s}\rangle\langle\psi_{\lambda_s}| \otimes |v_{\lambda_s}\rangle\langle v_{\lambda_s}| \tag{60}$$

$$\mathcal{G} \circ \mathcal{B}(|\Phi\rangle\langle\Phi|) = \frac{1}{l^2} I. \tag{61}$$

The matrices $l\mathcal{B}(|\Phi\rangle\langle\Phi|)$ and $l\mathcal{G}(|\Phi\rangle\langle\Phi|)$ are projections. The intersection of the range of these projections is the one-dimensional space generated by $|\Phi\rangle$. Hence,

$$\sqrt{\mathcal{G}(|\Phi\rangle\langle\Phi|)}\mathcal{B}(|\Phi\rangle\langle\Phi|)\sqrt{\mathcal{G}(|\Phi\rangle\langle\Phi|)} = \frac{1}{l^2}|\Phi\rangle\langle\Phi|. \tag{62}$$

The combination of (61) and (62) guarantees the condition (A2). Therefore, the state $|\Phi\rangle\langle\Phi|$ is q-memory useless.

This fact can be extended to the dephased state $\rho_{AB,p} = (1 - p)|\Phi\rangle\langle\Phi| + p\mathcal{G}(|\Phi\rangle\langle\Phi|)$ [49] as follows. Instead of (59), we have

$$\mathcal{B}(\rho_{AB,p}) = (1 - p)\frac{1}{l} \sum_{k=1}^l |\phi_k\rangle\langle\phi_k| \otimes |k\rangle\langle k| + \frac{p}{l^2} I. \tag{63}$$

Even when $\rho_{AB,0}$ is replaced by $\rho_{AB,p}$, the relations (60) and (61) still hold as follows.

$$\mathcal{G}(\rho_{AB,p}) = (1 - p)\mathcal{G}(|\Phi\rangle\langle\Phi|) + p\mathcal{G}(|\Phi\rangle\langle\Phi|) = \frac{1}{l} \sum_{\lambda=1}^l |\psi_{\lambda}\rangle\langle\psi_{\lambda}| \otimes |v_{\lambda}\rangle\langle v_{\lambda}| \tag{64}$$

$$\begin{aligned} \mathcal{G} \circ \mathcal{B}(\rho_{AB,p}) &= (1 - p)\frac{1}{l} \sum_{k=1}^l \mathcal{G}(|\phi_k\rangle\langle\phi_k|) \otimes |e_k\rangle\langle e_k| + \frac{p}{l^2} I \\ &= (1 - p)\frac{1}{l} \sum_{k=1}^l I \otimes |e_k\rangle\langle e_k| + \frac{p}{l^2} I = \frac{1}{l^2} I. \end{aligned} \tag{65}$$

Combining (62) and (63) with the above relations, we have

$$\begin{aligned} &\sqrt{\mathcal{G}(\rho_{AB,p})}\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB,p})}^{-1} \mathcal{B}(\rho_{AB,p})\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB,p})}^{-1} \sqrt{\mathcal{G}(\rho_{AB,p})} \\ &= (1 - p)|\Phi\rangle\langle\Phi| + p\mathcal{G}(|\Phi\rangle\langle\Phi|). \end{aligned} \tag{66}$$

Since the condition (A2) holds, the dephased state $\rho_{AB} = (1 - p)|\Phi\rangle\langle\Phi| + p\mathcal{G}(|\Phi\rangle\langle\Phi|)$ serves as another example of an entangled q-memory useless state.

4 Pure preshared states

4.1 General conditions for q-memory uselessness

Next, we consider the case with a pure state $\rho_{AB} = |\Psi\rangle\langle\Psi|$. For $\mathcal{B} = \{|k\rangle\}_{k=1}^{d_B}$ on \mathcal{H}_B , without loss of generality, we can assume that $\langle k|\rho_B|k\rangle > 0$. (Otherwise, we restrict k to the index to satisfy $\langle k|\rho_B|k\rangle > 0$.) Then, we have

$$|\Psi\rangle_{AB} = \sum_{k=1}^{d_B} \sqrt{P_K(k)} |\psi_k\rangle_A |k\rangle_B. \tag{67}$$

Theorem 5 *Assume that the preshared state ρ_{AB} is a pure state $|\Psi\rangle\langle\Psi|$. Given the basis \mathcal{B} , the following condition is equivalent to Conditions (A1), (A2), and (A3).*

(C1) *The state $|\Psi\rangle$ has the form as*

$$|\Psi\rangle = \sum_{k=1}^{d_B} \sqrt{P_K(k)} \sum_{\lambda \in \hat{G}'} \sqrt{P_\Lambda(\lambda)} e^{i\theta_{\lambda,k}} |\psi_{\lambda,k}\rangle \otimes |k\rangle, \tag{68}$$

where for all k, k' the vector $|\psi_{\lambda,k}\rangle \in \mathcal{H}_\lambda \otimes \mathcal{M}_\lambda$ satisfies the condition;

$$\text{Tr}_{\mathcal{M}_\lambda} |\psi_{\lambda,k}\rangle\langle\psi_{\lambda,k}| = \text{Tr}_{\mathcal{M}_\lambda} |\psi_{\lambda,k'}\rangle\langle\psi_{\lambda,k'}|, \tag{69}$$

and P_K and P_Λ are independent probability distributions.

When a state ρ_{AB} is a pure state, Condition (C1) is equivalent to the condition in Proposition 3. That is, the above theorem shows the inverse direction of Proposition 3 in the case with pure states.

Proof It is sufficient to show the equivalence between (C1) and (A1). Defining

$$\rho_{\lambda,k} := \frac{1}{P_K(k)P_{\Lambda|k}(\lambda)} (P_\lambda \otimes |k\rangle\langle k|) \rho_{AB} (P_\lambda \otimes |k\rangle\langle k|) \tag{70}$$

and recalling (13), we have

$$\begin{aligned} C_c(\mathcal{B}(\rho_{AB})) &= \sum_{\lambda \in \hat{G}'} P_\Lambda(\lambda) \log d_\lambda + \sum_{k=1}^{d_B} P_K(k) \left(H(P_{\Lambda|k}) + \sum_{\lambda \in \hat{G}'} P_{\Lambda|k}(\lambda) H(\text{Tr}_{\mathcal{H}_\lambda} \rho_{\lambda,k}) \right) \\ &= \sum_{\lambda \in \hat{G}'} P_\Lambda(\lambda) \log d_\lambda + \sum_{k=1}^{d_B} P_K(k) H(P_{\Lambda|k}) \end{aligned}$$

$$\begin{aligned}
 &+ \sum_{\lambda \in \hat{G}'} P_{\Lambda}(\lambda) \sum_{k=1}^{d_B} P_{K|\lambda}(k) H(\text{Tr}_{\mathcal{H}_{\lambda}} \rho_{\lambda,k}) \\
 &= \sum_{\lambda \in \hat{G}'} P_{\Lambda}(\lambda) \log d_{\lambda} + \sum_{k=1}^{d_B} P_K(k) H(P_{\Lambda|k}) + \sum_{\lambda \in \hat{G}'} P_{\Lambda}(\lambda) \sum_{k=1}^{d_B} P_{K|\lambda}(k) H(\text{Tr}_{M_{\lambda}} \rho_{\lambda,k}).
 \end{aligned} \tag{71}$$

The final equation follows from the fact that $\rho_{\lambda,k}$ is a pure state because ρ_{AB} is pure.

In this case, by comparing (14) and (71), Condition (A1), i.e., $C_c(\rho) = C_c(\mathcal{B}(\rho))$, is equivalent to

$$\begin{aligned}
 &H(P_{\Lambda}) + \sum_{\lambda \in \hat{G}'} P_{\Lambda}(\lambda) H(\text{Tr}_{M_{\lambda}} \rho_{\lambda}) \\
 &= \sum_{k=1}^{d_B} P_K(k) H(P_{\Lambda|k}) + \sum_{\lambda \in \hat{G}'} P_{\Lambda}(\lambda) \sum_{k=1}^{d_B} P_{K|\lambda}(k) H(\text{Tr}_{M_{\lambda}} \rho_{\lambda,k}).
 \end{aligned} \tag{72}$$

Since $P_{\Lambda} = \sum_{k=1}^{d_B} P_K(k) P_{\Lambda|k}$ and $\text{Tr}_{M_{\lambda}} \rho_{\lambda} = \sum_{k=1}^{d_B} P_{K|\lambda}(k) \text{Tr}_{M_{\lambda}} \rho_{\lambda,k}$, the concavity of entropy implies that

$$H(P_{\Lambda}) \geq \sum_{k=1}^{d_B} P_K(k) H(P_{\Lambda|k}) \tag{73}$$

$$H(\text{Tr}_{M_{\lambda}} \rho_{\lambda}) \geq \sum_{k=1}^{d_B} P_{K|\lambda}(k) H(\text{Tr}_{M_{\lambda}} \rho_{\lambda,k}) \quad \forall \lambda \tag{74}$$

and therefore, (72) is equivalent to

$$P_{\Lambda} = P_{\Lambda|k}, \quad \text{Tr}_{M_{\lambda}} \rho_{\lambda} = \text{Tr}_{M_{\lambda}} \rho_{\lambda,k} \tag{75}$$

for all k and λ . Since the condition (75) is equivalent to Condition (C1), we obtain the equivalence between (C1) and (A1). \square

Although we have already proven the equivalence between (C1) and all the conditions in Theorem 1, it may not be immediately clear how the form of (C1) can induce the form in (A2). In Appendix, we explicitly derive how the form in (A2) can be reached starting from the form in (C1).

Theorem 1 and the proof of Proposition 3 give the following characterization for pure resource states. The following is a summary of the results for general pure states.

Theorem 6 *For an arbitrary pure resource state $\rho_{AB} = |\Psi\rangle\langle\Psi|$, the following are equivalent.*

- (D1) *The equality in (20) holds, i.e., ρ_{AB} is \mathcal{B} -q-memory useless.*
- (D2) *$|\Psi\rangle$ satisfies (68) and (69).*

(D3) The following relation holds.

$$\rho_{AB} = \sqrt{\mathcal{G}(\rho_{AB})} \sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1} \mathcal{B}(\rho_{AB}) \sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1} \sqrt{\mathcal{G}(\rho_{AB})}. \tag{76}$$

(D4) There exists a controlled unitary $V_{AB} = \sum_{k=1}^{d_B} V_k \otimes |k\rangle\langle k|_B$ and a set $\{|\eta_g\rangle_A\}_g$ of states on \mathcal{H}_A and some state $|\phi\rangle_B$ on \mathcal{H}_B such that

$$V_{AB} U_g |\Psi\rangle = |\eta_g\rangle_A \otimes |\phi\rangle_B, \forall g \in G. \tag{77}$$

To obtain a further characterization, we recall the multiplicity-free condition. When the multiplicity-free condition is satisfied, (68) and (69) can be represented by the following single form

$$|\Psi\rangle = \sum_{\lambda \in \hat{G}'} \sqrt{P_\Lambda(\lambda)} |\psi_\lambda\rangle \otimes \sum_{k=1}^{d_B} \sqrt{P_K(k)} e^{i\theta_{\lambda,k}} |k\rangle, \tag{78}$$

for some vector $|\psi_\lambda\rangle \in \mathcal{H}_\lambda$ independent of k . On the other hand, if G is abelian (but not necessarily multiplicity-free), then $\dim \mathcal{H}_\lambda = 1$ for all $\lambda \in \hat{G}'$, implying that (69) is always satisfied and thus the condition (68) solely serves as the necessary and sufficient condition for Bob’s quantum memory to be useless.

Therefore, we obtain the following corollary.

Corollary 7 *Let the preshared state ρ_{AB} be a pure state given by $|\Psi\rangle = \sum_{\lambda \in \hat{G}'} \sqrt{P_\Lambda(\lambda)} |\psi_\lambda\rangle |v_\lambda\rangle$, where \hat{G}' with $|\hat{G}'| = l$ is a subset of irreducible representations for which $P_\Lambda(\lambda) \neq 0 \forall \lambda \in \hat{G}'$, and $|v_1\rangle, \dots, |v_l\rangle$ are some quantum states on \mathcal{H}_B . Suppose also that the multiplicity-free condition holds. Then, the following conditions are equivalent.*

(E1) The state $|\Psi\rangle$ is q -memory useless.

(E2) There exist a basis $\{|k\rangle\}_{k=1}^{d_B}$ of \mathcal{H}_B , a probability distribution P_K on $\{1, \dots, d_B\}$ independent of λ , and real numbers $\{\theta_{\lambda,k}\}_{\lambda,k}$ such that

$$|v_\lambda\rangle = \sum_{k=1}^{d_B} \sqrt{P_K(k)} e^{i\theta_{\lambda,k}} |k\rangle. \tag{79}$$

Since Condition (E2) can be considered as a condition for the l vectors $V := (|v_1\rangle, \dots, |v_l\rangle)$ in \mathcal{H}_B , the problem of q -memory uselessness is reduced to the analysis for the l vectors V .

For example, when the vectors $|v_1\rangle, \dots, |v_l\rangle$ are orthogonal, Condition (E2) holds by choosing the basis $\{|k\rangle\}_{k=1}^{d_B}$ of \mathcal{H}_B as follows. The orthogonality guarantees that $l \leq d_B$. We set $|1\rangle, \dots, |l\rangle$ as

$$|k\rangle = \frac{1}{\sqrt{l}} \sum_{s=1}^l e^{i2\pi ks/l} |v_s\rangle, \quad k = 1, \dots, l \tag{80}$$

and $|l + 1\rangle, \dots, |r\rangle$ to be vectors orthogonal to $|v_1\rangle, \dots, |v_l\rangle$. Equation (79) is then satisfied by choosing $P_K(k) = 1/l$ for $k = 1, \dots, l$ and $\theta_{\lambda,k} = -2\pi\lambda k/l$.

The fact that Condition (E2) always holds when $l = 2$ can be seen as follows. We choose θ and θ' as $e^{i\theta'} \cos \theta = \langle v_1 | v_2 \rangle$. Then, we choose the basis $\{|1\rangle, |2\rangle\}$ to satisfy

$$|v_1\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle) \tag{81}$$

$$|v_2\rangle = \frac{1}{\sqrt{2}}(e^{i(\theta'+\theta)}|1\rangle + e^{i(\theta'-\theta)}|2\rangle). \tag{82}$$

4.2 Characterization by genuinely incoherent operations

Under the multiplicity-free condition, we characterize our conditions for q-memory uselessness for pure states by using genuinely incoherent operations (GIO) [40], one of the major classes of operations considered in the resource theory of coherence [24]. The GIO, which we denote as \mathcal{O}_{GIO} , is defined as the set of operations that preserve all incoherent states, $\Gamma_{\text{GIO}}(\sigma) = \sigma$ for every incoherent state σ , where a state is called incoherent when it is diagonal with a given preferred orthogonal basis. Then, it was shown in [40, Thm.2] that Γ is in \mathcal{O}_{GIO} if and only if Γ can be written as $\Gamma(\rho) = A \odot \rho$ with some positive semidefinite matrix A with $A_{\lambda\lambda} = 1 \forall \lambda$, where $(X \odot Y)_{\lambda\eta} := X_{\lambda\eta}Y_{\lambda\eta}$ is the Hadamard product.

We find that GIO is a useful tool for analyzing the condition (E2) for general l through the Gram matrix of $V = (|v_1\rangle, \dots, |v_l\rangle)$ defined as $J(V)_{\lambda\eta} := \langle v_\lambda | v_\eta \rangle$, $\lambda, \eta = 1, \dots, l$, or equivalently, $J(V) := V^\dagger V$. Since the diagonal element of the Gram matrix $J(V)$ is 1, the CPTP map $\Gamma_{J(V)}$ defined as $\Gamma_{J(V)}(\rho) := J(V) \odot \rho$ is also in \mathcal{O}_{GIO} . Then, we have the following characterizations.

Theorem 8 *Suppose \mathcal{H}_A satisfies the multiplicity-free condition. Let $|\Psi\rangle = \sum_{\lambda \in \hat{G}'} \sqrt{P_\Lambda(\lambda)} |\psi_\lambda\rangle |v_\lambda\rangle$ be a given resource state shared by Alice and Bob, where \hat{G}' with $|\hat{G}'| = l$ is a subset of irreducible representations for which $P_\Lambda(\lambda) \neq 0 \forall \lambda \in \hat{G}'$. The following conditions for l vectors $V := (|v_1\rangle, \dots, |v_l\rangle)$ in \mathcal{H}_B are equivalent.*

- (F1) *The state $|\Psi\rangle$ is q-memory useless.*
- (F2) *There exist a basis $\{|k\rangle\}_{k=1}^{d_B}$ of \mathcal{H}_B , a probability distribution P_K on $\{1, \dots, d_B\}$, and real numbers $\{\theta_{\lambda,k}\}_{\lambda,k}$ that satisfy (79).*
- (F3) *There exist a basis $\{|k\rangle\}_{k=1}^{d_B}$ of \mathcal{H}_B , a probability distribution P_K on $\{1, \dots, d_B\}$, and real numbers $\{\theta_{\lambda,k}\}_{\lambda,k}$ that satisfy*

$$J(V) = J(U) \tag{83}$$

where l vectors $U := (|u_1\rangle, \dots, |u_l\rangle)$ are defined as

$$|u_\lambda\rangle := \sum_{k=1}^{d_B} \sqrt{P_K(k)} e^{i\theta_{\lambda,k}} |k\rangle \tag{84}$$

for $\lambda = 1, \dots, l$.

(F4) *There exist a probability distribution P_K on $\{1, \dots, d_B\}$ and real numbers $\{\theta_{\lambda,k}\}_{\lambda,k}$ that satisfy*

$$\frac{1}{l} J(V) = \sum_k P_K(k) Z_k |+\rangle \langle +| Z_k^\dagger, \tag{85}$$

where $|+\rangle := \frac{1}{\sqrt{l}} \sum_{\lambda=1}^l |\lambda\rangle$ is the maximally coherent state and

$$Z_k := \sum_{\lambda} e^{i\theta_{\lambda,k}} |\lambda\rangle \langle \lambda| \tag{86}$$

is an (incoherent) diagonal unitary.

(F5) *There exist a probability distribution P_K on $\{1, \dots, d_B\}$ and real numbers $\{\theta_{\lambda,k}\}_{\lambda,k}$ such that $\Gamma_{J(V)} \in \mathcal{O}_{\text{GIO}}$ can be written as*

$$\Gamma_{J(V)}(\rho) = \sum_k P_K(k) Z_k \rho Z_k^\dagger. \tag{87}$$

For Condition (F4), Reference [40, Thm.3] found that, for $l = 2, 3$, any genuinely incoherent operation can be written as a probabilistic incoherent diagonal unitary, while for every $l \geq 4$, there exists a genuinely incoherent operation that cannot be written as a probabilistic incoherent diagonal unitary. In addition, for any $\Gamma \in \mathcal{O}_{\text{GIO}}$, there exist l vectors $V := (|v_1\rangle, \dots, |v_l\rangle)$ such that $\Gamma = \Gamma_{J(V)}$. Therefore, we obtain the following result.

Corollary 9 *For every choice of $|v_1\rangle, \dots, |v_l\rangle$, there exist a basis $\{|k\rangle\}_{k=1}^{d_B}$, a probability distribution $\{P_K(k)\}_{k=1}^{d_B}$, and real numbers $\{\theta_{\lambda,k}\}_{\lambda,k}$ that satisfy (79) for $l = 2, 3$. On the other hand, for every l with $l \geq 4$, there exist $|v_1\rangle, \dots, |v_l\rangle$ for which there is no choice of $\{|k\rangle\}_{k=1}^{d_B}$, $\{P_K(k)\}_{k=1}^{d_B}$, and $\{\theta_{\lambda,k}\}_{\lambda,k}$ that satisfies (79). In other words, Bob’s quantum memory is not useful to achieve the capacity $C_c(|\Phi\rangle)$ for $l = 2, 3$. However, when $l \geq 4$, there exists a state $|\Phi\rangle$ such that Bob’s quantum memory is useful to achieve the capacity $C_c(|\Phi\rangle)$.*

Therefore, when the preshared state ρ_{AB} is a pure state $|\Psi\rangle\langle\Psi|$ as in Theorem 8, the multiplicity-free condition holds, and $|\hat{G}'|$ is 2 or 3, the quantum memory \mathcal{H}_B can be replaced by a classical memory. However, when $|\hat{G}'| > 3$ there is a pure state $|\Psi\rangle\langle\Psi|$ even with the multiplicity-free condition such that the quantum memory \mathcal{H}_B enhances the communication speed.

Proof of Theorem 8 Corollary 7 shows the equivalence between Conditions (F1) and (F2). Since the application of a unitary operator to a basis does not change the Gram matrix, Conditions (F2) and (F3) are equivalent.

Next, we show the equivalence between (F3) and (F4). Since the Gram matrix $J(U)$ can be written by

$$J(U)_{\lambda\eta} = \sum_{k=1}^{d_B} P_K(k) e^{i\theta_{\lambda,k} - i\theta_{\eta,k}}, \tag{88}$$

it is written as

$$J(U) = l \sum_{k=1}^{d_B} P_K(k) |w_k\rangle\langle w_k|, \tag{89}$$

where we define $|w_k\rangle = \frac{1}{\sqrt{l}} \sum_{\lambda=1}^l e^{i\theta_{\lambda,k}} |\lambda\rangle$ for every k . We further note that $|w_k\rangle$ can be written by $|w_k\rangle = Z_k|+\rangle$, This fact implies

$$\frac{1}{l} J(U) = \sum_{k=1}^{d_B} P_K(k) Z_k|+\rangle\langle +|Z_k^\dagger, \tag{90}$$

which shows the equivalence between (F3) and (F4).

Next, we show the equivalence between (F4) and (F5). We assume Condition (F5). Then, we have

$$\begin{aligned} \frac{1}{l} J(V) &= J(V) \odot |+\rangle\langle +| \\ &= \Gamma_{J(V)}(|+\rangle\langle +|) = \sum_{k=1}^{d_B} P_K(k) Z_k|+\rangle\langle +|Z_k^\dagger, \end{aligned} \tag{91}$$

which implies Condition (F4).

We assume Condition (F4). Then, the GIO $\Gamma_{J(V)}$ satisfies

$$\begin{aligned} \Gamma_{J(V)}(\rho) &= J(V) \odot \rho = \sum_k P_K(k) Z_k|+\rangle\langle +|Z_k^\dagger \odot \rho \\ &= \sum_k P_K(k) \left(Z_k|+\rangle\langle +|Z_k^\dagger \odot \rho \right) = \sum_k P_K(k) Z_k \rho Z_k^\dagger, \end{aligned} \tag{92}$$

which implies Condition (F5). □

4.3 Construction of q-memory useful pure state

We provide a systematic method to construct a q-memory useful pure state by using the results of GIO. Since an arbitrary $\frac{1}{l} J(\mathbf{v})$ can be obtained by applying some genuinely incoherent operation to $|+\rangle_l$, our problem is reduced to finding whether such an operation in \mathcal{O}_{GIO} can be implemented by a probabilistic incoherent unitary. The

following result, which gives the extremality condition for \mathcal{O}_{GIO} , is useful to present examples for which quantum memory is useful for all Bob’s bases.

Lemma 10 ([40, Proof of Theorem 21]) *Let $\Gamma \in \mathcal{O}_{\text{GIO}}$ be represented by a set $\{K_t\}_{t=1}^{r'}$ of Kraus operators with $r' > 1$. Then, Γ cannot be realized by a probabilistic incoherent unitary if r'^2 operators $\{K_t^\dagger K_s\}_{t,s=1}^{r'}$ are linearly independent.*

Kraus operators of a channel $\Gamma_{J(V)} \in \mathcal{O}_{\text{GIO}}$ are given as follows.

Lemma 11 *Given l vectors $V := (|v_1\rangle, \dots, |v_l\rangle)$ in \mathcal{H}_B with the form $|v_j\rangle = \sum_{k=1}^{d_B} v_{j,k}|k\rangle$, the operators $K_k = \text{diag}(|\tilde{a}_k\rangle)$ for vectors $|\tilde{a}_k\rangle = \sum_{j=1}^l v_{j,k}|j\rangle$ with $k = 1, \dots, d_B$ form Kraus operators $\{K_t\}_{t=1}^{d_B}$ of a channel $\Gamma_{J(V)} \in \mathcal{O}_{\text{GIO}}$.*

Proof Since the relation

$$l \sum_{t=1}^{d_B} K_t |+\rangle\langle +| K_t^\dagger = \sum_{t=1}^{d_B} |\tilde{a}_t\rangle\langle \tilde{a}_t| = J(V) \tag{93}$$

holds, we have

$$\sum_{t=1}^{d_B} K_t \rho K_t^\dagger = \frac{1}{l} J(V) \odot \rho = \Gamma_{J(V)}(\rho). \tag{94}$$

□

The above lemma shows that Kraus operators of any genuinely incoherent operation $\Gamma_{J(V)} \in \mathcal{O}_{\text{GIO}}$ are given as diagonal operators. More generally, the following lemma is known.

Lemma 12 ([40, Theorem 2]) *A channel is GIO if and only if all Kraus operators are diagonal.*

Combining Lemmas 10 and 11 with the statement (F5) implies the following. When the d_B^2 vectors $\{(\overline{v_{j,t}} v_{j,s})_{j=1}^l\}_{t,s=1}^{d_B}$ are linearly independent, the genuinely incoherent operation $\Gamma_{J(V)} \in \mathcal{O}_{\text{GIO}}$ cannot be realized by a probabilistic incoherent unitary. Then, a state $|\Psi\rangle$ constructed by the set $\{|v_j\rangle\}_{j=1}^l$ serves as a resource state, for which quantum memory is useful for all Bob’s bases. To satisfy this condition, d_B^2 needs to be smaller than l .

A protocol to find such a resource state is as follows.

- (1) Given $l \leq |\hat{G}|$, we choose d_B such that $1 < d_B^2 \leq l$.
- (2) Pick l states $|v_j\rangle = \sum_{k=1}^{d_B} v_{j,k}|k\rangle \in \mathbb{C}^{d_B}$ for $j = 1, \dots, l$.
- (3) Check whether the d_B^2 vectors $\{(\overline{v_{j,t}} v_{j,s})_{j=1}^l\}_{t,s=1}^{d_B}$ are linearly independent. If not, go back to the previous step and try another set of $\{|v_j\rangle\}_j$.
- (4) Choose an arbitrary subset of irreps $\hat{G}' \subset \hat{G}$ such that $|\hat{G}'| = l$. Choose an arbitrary state $|\psi_\lambda\rangle \in \mathcal{H}_\lambda$ for each $\lambda \in \hat{G}'$ and an arbitrary probability distribution $P_\Lambda(\lambda)$ over $\lambda \in \hat{G}'$ with $P_\Lambda(\lambda) > 0 \forall \lambda \in \hat{G}'$.

(5) Define $|\Psi\rangle = \sum_{j=1}^l \sqrt{P_\Lambda(\lambda_j)} |\psi_{\lambda_j}\rangle \otimes |v_j\rangle = \sum_{j=1}^l \sum_{k=1}^{d_B} \sqrt{P_\Lambda(\lambda_j)} v_{j,k} |\psi_{\lambda_j}\rangle \otimes |k\rangle$, where λ_j refers to the j th irrep in \hat{G}' .

The final state $|\Psi\rangle$ is a state for which quantum memory is useful for all Bob’s bases. For $1 < d_B^2 \leq l$, a randomly chosen $\{|v_j\rangle\}_{j=1}^l$ usually satisfies the linear independence condition in Step 3. As an analytical example, we find an instance for $\{|v_j\rangle\}_{j=1}^l$ for $l \geq 4$ and $d_B = 2$ discussed in Ref. [40], which is defined as

$$v_{j,1} := \begin{cases} \frac{1}{j} & \text{when } j \leq 4 \\ 1 & \text{when } j > 4 \end{cases} \tag{95}$$

$$v_{j,2} := \begin{cases} i^j \sqrt{1 - \frac{1}{j^2}} & \text{when } j \leq 4 \\ 0 & \text{when } j > 4. \end{cases} \tag{96}$$

One can then check that four vectors $\{(\overline{v_{j,t}} v_{j,s})_{j=1}^l\}_{t,s=1}^2$ are linearly independent. We then prepare $\{|v_j\rangle\}_{j=1}^l$ as $v_{j,1}|1\rangle + v_{j,2}|2\rangle$.

The states constructed by the above procedure Steps 1–5 provide situations where Bob wants to hold local quantum memory and make a collective measurement on his side before communication. Notice that, as shown in Ref. [13], the capacity $C_c(\rho_{AB})$ for the pure state case can be achieved by applying collective measurement across n Bob’s local systems of the preshared state.

5 Case with maximally entangled state

5.1 Commutative group

Similarly to Sect. 3.3, we assume that the group G is commutative. For simplicity, we assume the multiplicity-free condition to the space \mathcal{H}_A . We use the same notations as the ones used in Sect. 3.3. We assume that the preshared entangled state $|\Psi\rangle$ is a maximally entangled state $|\Phi\rangle$. Thus, due to the relations (55) and (56), the condition (79) in Corollary 7 holds. In this case, the condition (79) in Corollary 7 shows that the maximally entangled state $|\Phi\rangle$ is q-memory useless in a simpler way than Condition (A2) does. This is also a special case of the examples presented in Sect. 3.2.

Next, we proceed to the case when the multiplicity-free condition does not hold. Using an orthogonal basis $\{|e_{j,\lambda}\rangle\}_{j=1}^{l(\lambda)}$ where $l(\lambda) := \dim \mathcal{M}_\lambda$ and an orthogonal basis $\{|v_j\rangle\}_{j=1}^r$ with $r = \sum_{\lambda=1}^l l(\lambda)$, the maximally entangled state $|\Phi\rangle$ is written as $\frac{1}{\sqrt{r}} \sum_{\lambda=1}^l |\psi_\lambda\rangle \sum_{j=1}^{l(\lambda)} |e_{j,\lambda}\rangle |v_{j+\sum_{\lambda'=1}^{\lambda-1} l(\lambda')}\rangle$. We choose $|e_{B,k}\rangle$ as

$$|e_{B,k}\rangle := \frac{1}{\sqrt{r}} \sum_{\lambda=1}^r e^{2\pi k j i / r} |v_j\rangle. \tag{97}$$

Then, we have

$$\begin{aligned}
 |\Phi\rangle &= \frac{1}{\sqrt{r}} \sum_{\lambda=1}^l |\psi_\lambda\rangle \sum_{j=1}^{l(\lambda)} |e_{j,\lambda}\rangle \frac{1}{\sqrt{r}} \sum_{k=1}^r e^{-2\pi k(j+\sum_{\lambda'=1}^\lambda l(\lambda'))i/r} |e_{B,k}\rangle \\
 &= \sum_{k=1}^r \frac{1}{\sqrt{r}} \sum_{\lambda=1}^l \frac{\sqrt{l(\lambda)}}{\sqrt{r}} e^{-2\pi k \sum_{\lambda'=1}^\lambda l(\lambda')i/r} |\psi_\lambda\rangle \left(\frac{1}{\sqrt{l(\lambda)}} \sum_{j=1}^{l(\lambda)} e^{-2\pi kji/r} |e_{j,\lambda}\rangle \right) |e_{B,k}\rangle.
 \end{aligned}
 \tag{98}$$

Hence, by choosing $|\psi_\lambda\rangle \left(\frac{1}{\sqrt{l(\lambda)}} \sum_{j=1}^{l(\lambda)} e^{-2\pi kji/r} |e_{j,\lambda}\rangle \right)$ as $|\psi_{\lambda,k}\rangle$, Condition (C1) holds in Theorem 5. That is, the quantum memory is not needed even in this case.

In particular, when the set \hat{G}' is the whole set \hat{G} of irreducible representations of G , the entropy of $\sum_{g \in G} \frac{1}{|G|} U_g |\Phi\rangle \langle \Phi| U_g^\dagger$ is $\log |G|$. This means that the action of G can be distinguished perfectly even when Bob measures his memory in advance. In other words, the states $\{U_g |\Phi\rangle\}_{g \in G}$ can be distinguished perfectly by one-way local measurements. For example, given Weyl–Heisenberg representation of $\mathbb{Z}_d \times \mathbb{Z}_d$, the action of the commutative subgroup of $\mathbb{Z}_d \times \mathbb{Z}_d$ can be distinguished perfectly by one-way local measurements. As another example, given Weyl–Heisenberg representation of $\mathbb{F}_p^n \times \mathbb{F}_p^n$, the action of the commutative subgroup of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ can be distinguished perfectly by one-way local measurements. In fact, this kind of state discrimination has been discussed in the context of local discrimination of generalized Bell states in [50–57].

While the classification of a commutative subgroup in $\mathbb{Z}_d \times \mathbb{Z}_d$ is not easy [55–57], a commutative subgroup in $\mathbb{F}_p^n \times \mathbb{F}_p^n$ can be easily classified as follows. Commutativity can be characterized by the orthogonality under the symplectic inner product. The set of m -dimensional orthogonal subspace can be considered as an orthogonal version of Grassmannian over finite fields, whose classification is well known [58, Proposition 1.7.2]. For the identification of m -dimensional orthogonal subspace, it is sufficient to choose m independent commutative vectors in $\mathbb{F}_p^n \times \mathbb{F}_p^n$. The choice of the first nonzero vector has $p^{2n} - 1$ cases. The choice of the second nonzero vector has $p^{2(n-1)} - 1$ cases due to the commutativity with the first vector. The commutativity with the first vector is equivalent to the orthogonal property to the first vector for the symplectic inner product. Therefore, in the case of m -dimensional subgroups, we have $(p^{2n} - 1)(p^{2(n-1)} - 1) \dots (p^{2(n-m+1)} - 1)$ cases. Since $(p^m - 1)(p^{m-1} - 1) \dots (p - 1)$ choices of m independent commutative vectors correspond to the same m -dimensional subgroup, we have $\frac{(p^{2n}-1)(p^{2(n-1)}-1)\dots(p^{2(n-m+1)}-1)}{(p^m-1)(p^{m-1}-1)\dots(p-1)}$ commutative m -dimensional subgroup in total. When $m = n$, this number is simplified to $(p^n + 1)(p^{n-1} + 1) \dots (p + 1)$.

5.2 General group

Next, we observe how the above fact can be generalized to a general group G . When G is not a commutative group, the irreducible representation is not one-dimensional.

Hence, this case cannot be considered as a special case of the examples presented in Section 3.2.

We have the following lemma for a general group with respect to the relation between Condition (C1) and a maximally entangled state $|\Phi\rangle$ when the set \hat{G}' of irreducible representations appearing in \mathcal{H}_A is given as $\{1, \dots, l\}$.

Lemma 13 *A maximally entangled state $|\Phi\rangle$ satisfies Condition (C1) in Theorem 5 if and only if the relation $\dim \mathcal{M}_\lambda \geq \dim \mathcal{H}_\lambda$ holds for $\lambda \in \hat{G}'$.*

This lemma guarantees the following. When the preshared entangled state $|\Psi\rangle$ is a maximally entangled state $|\Phi\rangle$ and the relation $\dim \mathcal{M}_\lambda \geq \dim \mathcal{H}_\lambda$ holds for $\lambda \in \hat{G}'$, the states $\{U_g|\Phi\rangle\}_{g \in G}$ can be distinguished perfectly by one-way local measurements.

Proof The “only if” part. We assume that a maximally entangled state $|\Phi\rangle$ satisfies the condition (69). Then, the condition (69) implies $\text{Tr}_{\mathcal{M}_\lambda} |\psi_{\lambda,k}\rangle\langle\psi_{\lambda,k}|$ is $\text{Tr}_{\mathcal{M}_\lambda} \rho_A$. Hence, $\text{Tr}_{\mathcal{M}_\lambda} |\psi_{\lambda,k}\rangle\langle\psi_{\lambda,k}|$ is the completely mixed state. Thus, $\dim \mathcal{M}_\lambda \geq \dim \mathcal{H}_\lambda$.

The “if” part. We assume that $\dim \mathcal{M}_\lambda \geq \dim \mathcal{H}_\lambda$ for $\lambda \in \hat{G}'$. When two entangled states have the same reduced density matrix on \mathcal{H}_A , these two entangled states can be converted to each other via a local unitary on \mathcal{H}_B . It is sufficient to show the existence of the choice of $\{|k\rangle\}$ and $\{|\psi_{\lambda,k}\rangle\}$ to satisfy Condition (C1).

We denote the dimension of \mathcal{M}_λ by d'_λ . We choose an orthogonal basis $\{|e_{\lambda,A,j}\rangle\}_{j=0}^{d_\lambda-1}$ of \mathcal{H}_λ , and an orthogonal basis $\{|e'_{\lambda,A,j'}\rangle\}_{j'=0}^{d'_\lambda-1}$ of \mathcal{M}_λ . We define the operators $Z := \sum_{j=0}^{d_\lambda-1} e^{2\pi i j/d_\lambda} |e_{\lambda,A,j}\rangle\langle e_{\lambda,A,j}|$ on \mathcal{H}_λ , and $X := \sum_{j'=0}^{d'_\lambda-1} |e'_{\lambda,A,j'+1}\rangle\langle e'_{\lambda,A,j'}|$ on \mathcal{M}_λ , where modulo d'_λ is applied in the definition of X . For $(k_\lambda, k'_\lambda) \in \{0, 1, \dots, d_\lambda - 1\} \times \{0, 1, \dots, d'_\lambda - 1\}$, we define the vectors $|\psi_{\lambda,k,k'}\rangle := Z^k \otimes X^{k'} \frac{1}{\sqrt{d_\lambda}} \sum_{j=0}^{d_\lambda-1} |e_{\lambda,A,j}\rangle |e'_{\lambda,A,j}\rangle$ in $\mathcal{H}_\lambda \otimes \mathcal{M}_\lambda$, which forms an orthogonal basis of $\mathcal{H}_\lambda \otimes \mathcal{M}_\lambda$.

For $(k_\lambda, k'_\lambda) \in \{0, 1, \dots, d_\lambda - 1\} \times \{0, 1, \dots, d'_\lambda - 1\}$ with $\lambda \in \hat{G}' = \{1, 2, \dots, l\}$, we define the vector $|e_{B,k_1,k'_1,\dots,k_l,k'_l}, \lambda\rangle$ in \mathcal{H}_B . Then, we define the vector

$$\sum_{k_1=0}^{d_1-1} \sum_{k'_1=0}^{d'_1-1} \cdots \sum_{k_l=0}^{d_l-1} \sum_{k'_l=0}^{d'_l-1} \sum_{\lambda'=1}^l \sqrt{\frac{1}{d_1 d'_1 \cdots d_l d'_l}} \cdot \sum_{\lambda=1}^l \sqrt{\frac{d_\lambda d'_\lambda}{\sum_{\lambda''=1}^l d_{\lambda''} d'_{\lambda''}}} e^{2\pi \lambda \lambda' i/l} |\psi_{\lambda,k_\lambda,k'_\lambda}\rangle |e_{B,k_1,k'_1,\dots,k_l,k'_l}, \lambda'\rangle, \tag{99}$$

which satisfies Condition (C1).

The reduced density matrix of

$$\sum_{\lambda'=1}^l \sqrt{\frac{1}{l}} \sum_{\lambda=1}^l \sqrt{\frac{d_\lambda d'_\lambda}{\sum_{\lambda''=1}^l d_{\lambda''} d'_{\lambda''}}} e^{2\pi \lambda \lambda' i/l} |\psi_{\lambda,k_\lambda,k'_\lambda}\rangle |e_{B,k_1,k'_1,\dots,k_l,k'_l}, \lambda'\rangle.$$

on \mathcal{H}_A is

$$\sum_{\lambda=1}^l \frac{d_\lambda d'_\lambda}{\sum_{\lambda''=1}^l d_{\lambda''} d'_{\lambda''}} |\psi_{\lambda, k_\lambda, k'_\lambda}\rangle \langle \psi_{\lambda, k_\lambda, k'_\lambda}|. \tag{100}$$

Therefore, the reduced density matrix of the vector (99) on \mathcal{H}_A is

$$\sum_{\lambda=1}^l \sum_{k_\lambda=0}^{d_\lambda-1} \sum_{k'_\lambda=0}^{d'_\lambda-1} \frac{1}{\sum_{\lambda''=1}^l d_{\lambda''} d'_{\lambda''}} |\psi_{\lambda, k_\lambda, k'_\lambda}\rangle \langle \psi_{\lambda, k_\lambda, k'_\lambda}|, \tag{101}$$

which is the completely mixed state on \mathcal{H}_A . Therefore, a maximally entangled state $|\Phi\rangle$ has the form to satisfy Condition (C1). Hence, we obtain the “if” part. \square

6 Implications to quantum illumination

As one of the settings of physical significance, quantum illumination investigates whether a low-reflective target object is present by shooting light and collecting the signal. The problem of target detection can be reduced to the channel discrimination problem to identify whether the given channel is a replacement channel that prepares the thermal state or a thermal attenuator channel. In this scenario, it has been shown that entanglement in the input state can enhance the discrimination performance in symmetric and asymmetric channel discrimination settings [37–39].

Here, we consider a variant of quantum illumination, where instead of detecting the thermal noise, we are to detect the existence of a certain noise channel.² Namely, we consider the asymmetric channel discrimination task where the null hypothesis is error-free, i.e., $\Gamma_1 = \text{id}$, and the alternative hypothesis is to have a group twirling channel as noise, i.e., $\Gamma_2 = \mathcal{G}$. One can then ask whether entanglement in a given input state ψ helps the hypothesis testing, i.e., whether one would like to hold a local quantum memory to utilize the entanglement in ψ .

This problem is formulated as follows. Let $\eta_j := \Gamma_j \otimes \text{id}(\psi)$ be the output states with an input state ψ for $j = 1, 2$. In general, one is allowed to make a collective POVM measurement $\{E_n, I - E_n\}$ on multiple copies $\eta_j^{\otimes n}$ of output states. We define the type-I error by $\alpha_n(E) := \text{Tr}((I - E) \eta_1^{\otimes n})$ and type-II error by $\beta_n(E) := \text{Tr}(E \eta_2^{\otimes n})$. In the asymmetric channel discrimination task, we aim to minimize the type-II error under the condition that type-I error is upper bounded by a constant ϵ . The Stein’s lemma [35, 60] tells that for all $0 < \epsilon < 1$, the error exponent of the type-II error is characterized by the relative entropy between two output states, i.e.,

$$-\lim_{n \rightarrow \infty} \frac{1}{n} \log \inf_{0 \leq E_n \leq I} \{\beta_n(E_n) : \alpha_n(E_n) \leq 1 - \epsilon\}$$

² Our setting can also be considered as a variant of quantum reading [59] in the sense that the reflectivity of the target is not small.

$$=D(\Gamma_1 \otimes \text{id}(\psi) \parallel \Gamma_2 \otimes \text{id}(\psi)). \tag{102}$$

We can address this question for the case of asymmetric channel discrimination by employing the framework established above. Since Stein’s lemma assures that the performance of the hypothesis testing is characterized by the relative entropy as in (102), entanglement in ψ is helpful (one would like to retain local quantum memory) if and only if the equality in (20) with $\rho_{AB} = \psi$ holds. We can also carry over the characterization of the resource state in Theorem 8 and Corollary 9 for the local memory to be useless.

As a typical example, we choose $G = \mathbb{Z}_d$ with a representation $U_g = \sum_{t=0}^{d-1} |t + g \bmod d\rangle\langle t|$. This representation can be decomposed into $U_g = \bigoplus_{\lambda=0}^{d-1} U_{\lambda,g}$ where $U_{\lambda,g} := e^{2\pi i g \lambda/d} |+\lambda\rangle\langle +\lambda|$ and $|+\lambda\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{2\pi i j \lambda/d} |j\rangle$. Then, Theorem 8, as well as a consequence from Sect. 5.1, implies that the maximally entangled input $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} |tt\rangle = \frac{1}{\sqrt{d}} \sum_{\lambda=0}^{d-1} |+\lambda\rangle|+d-\lambda-1\rangle$ does not require the local quantum memory to achieve the optimal performance for the noise detection task. Indeed, the Gram matrix $J(\mathbf{v})$ in Theorem 8 is the $d \times d$ identity matrix, as $\{|+\lambda\rangle\}_\lambda$ constructs an orthonormal basis. Therefore, by taking $P_K(k) = 1/d$ and $\theta_{\lambda,k} = 2\pi \lambda k/d$ in (F4) of Theorem 8, we can check that (85) is indeed satisfied. This makes a stark contrast to the case of the original quantum illumination, in which the two-mode squeezed state, which is the infinite-dimensional correspondence of the maximally entangled state, serves as the optimal input with the help of quantum memory [39].

7 Discussion

We have introduced the new concept of q-memory uselessness and usefulness of a preshared bipartite state in the dense-coding task based on a given group representation. We have derived various conditions for q-memory uselessness for general mixed and pure states. Using our general conditions, we have presented an example of a mixed entangled state that is q-memory useless. In addition, we have revealed a notable relation between q-memory uselessness of pure states and the resource theory of coherence. This relation is useful when the state is pure, the group is abelian, and the representation is multiplicity-free. Under this condition, we have shown that any pure state is q-memory useless when the given group representation consists of at most three irreducible representations. We also have presented a systematic way to construct a pure q-memory useful state when the group representation consists of more than three irreducible representations. Finally, we have discussed the relations between our framework and quantum illumination. We have considered a variant of quantum illumination that aims to distinguish the noiseless and the group twirling channels and employed our conditions to characterize the usefulness of quantum memory in enhancing the performance.

An interesting future direction is to find whether there exists a separable q-memory useful state. The class of q-memory useless states represented by the form in (40) is known to have zero quantum discord [61]. This implies that q-memory useful separable states, if any, should have nonzero quantum discord. Establishing the quantitative rela-

tion between quantum discord and q-memory usefulness may provide further insights into the role of quantum correlation in dense coding.

Appendix A Derivation from (C1) to (A2)

We demonstrate how to derive from (C1) to (A2) in the pure state case. That is, we check that a pure state $\rho_{AB} = |\Psi\rangle\langle\Psi|$ that satisfies (68) and (69) indeed satisfies (23) as follows.

Let $|\psi_{\lambda,k}\rangle = \sum_j \sqrt{c_{\lambda,k,j}} |r_{\lambda,k,j}\rangle_{\mathcal{H}_\lambda} |m_{\lambda,k,j}\rangle_{\mathcal{M}_\lambda}$ be a Schmidt decomposition of $|\psi_{\lambda,k}\rangle$, where $\{|r_{\lambda,k,i}\rangle\}_i$ and $\{|m_{\lambda,k,i}\rangle\}_i$ are orthonormal bases on \mathcal{H}_λ and \mathcal{M}_λ . Then, the condition (69) ensures that

$$\sum_j c_{\lambda,k,j} |r_{\lambda,k,j}\rangle\langle r_{\lambda,k,j}| = \sum_j c_{\lambda,k',j} |r_{\lambda,k',j}\rangle\langle r_{\lambda,k',j}|, \quad \forall k, k'. \tag{A1}$$

Substituting this into the form (68) yields

$$\begin{aligned} |\Psi\rangle &= \sum_\lambda \sqrt{P_\Lambda(\lambda)} \sum_k \sqrt{P_K(k)} e^{i\theta_{\lambda,k}} \\ &\quad \cdot \sum_j \sqrt{c_{\lambda,k,j}} |r_{\lambda,k,j}\rangle_{\mathcal{H}_\lambda} |m_{\lambda,k,j}\rangle_{\mathcal{M}_\lambda} |k\rangle_B. \end{aligned} \tag{A2}$$

Using this expression, we can write

$$\mathcal{B}(\rho_{AB}) = \sum_{\lambda\lambda'k} \sqrt{P_\Lambda(\lambda)P_\Lambda(\lambda')} P_K(k) e^{i\theta_{\lambda,k} - i\theta_{\lambda',k}} |\psi_{\lambda,k}\rangle\langle\psi_{\lambda',k}| \otimes |k\rangle\langle k|. \tag{A3}$$

$$\mathcal{G} \circ \mathcal{B}(\rho_{AB}) = \sum_{\lambda k} P_\Lambda(\lambda) P_K(k) \sum_j c_{\lambda,k,j} \frac{I}{d_{\mathcal{H}_\lambda}} \otimes |m_{\lambda,k,j}\rangle\langle m_{\lambda,k,j}| \otimes |k\rangle\langle k| \tag{A4}$$

$$\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1} = \sum_{\lambda k} \sqrt{P_\Lambda(\lambda)P_K(k)}^{-1} \sum_{j:c_{\lambda,k,j} \neq 0} \sqrt{\frac{d_{\mathcal{H}_\lambda}}{c_{\lambda,k,j}}} I \otimes |m_{\lambda,k,j}\rangle\langle m_{\lambda,k,j}| \otimes |k\rangle\langle k|. \tag{A5}$$

We then have

$$\begin{aligned} &\sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1} \mathcal{B}(\rho_{AB}) \sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1} \\ &= \sum_{\lambda\lambda'k} e^{i\theta_{\lambda,k} - i\theta_{\lambda',k}} d_{\mathcal{H}_\lambda} |\tilde{\Phi}_{\lambda,k}\rangle\langle\tilde{\Phi}_{\lambda',k}| \otimes |k\rangle\langle k| \end{aligned} \tag{A6}$$

where $|\tilde{\Phi}_{\lambda,k}\rangle := \sum_{j:c_{\lambda,k,j} \neq 0} |r_{\lambda,k,j}\rangle |m_{\lambda,k,j}\rangle$.

We also have

$$\mathcal{G}(\rho_{AB}) = \sum_{\lambda} P_{\Lambda}(\lambda) \frac{I}{d_{\mathcal{H}_{\lambda}}} \otimes \text{Tr}_{\mathcal{H}_{\lambda}} |\phi_{\lambda}\rangle\langle\phi_{\lambda}| \tag{A7}$$

and

$$\sqrt{\mathcal{G}(\rho_{AB})} = \sum_{\lambda} \sqrt{P_{\Lambda}(\lambda)} \frac{I}{\sqrt{d_{\mathcal{H}_{\lambda}}}} \otimes \sqrt{\text{Tr}_{\mathcal{H}_{\lambda}} |\phi_{\lambda}\rangle\langle\phi_{\lambda}|} \tag{A8}$$

where $|\phi_{\lambda}\rangle := \sum_k \sqrt{P_K(k)} e^{i\theta_{\lambda,k}} \sum_j \sqrt{c_{\lambda,k,j}} |r_{\lambda,k,j}\rangle_{\mathcal{H}_{\lambda}} |m_{\lambda,k,j}\rangle_{\mathcal{M}_{\lambda}} |k\rangle_B$.

The fact that

$$\begin{aligned} \sqrt{\text{Tr}_{\mathcal{H}_{\lambda}} |\phi_{\lambda}\rangle\langle\phi_{\lambda}|} &= \sum_{kk'} \sqrt{P_K(k)P_K(k')} e^{i\theta_{\lambda,k} - i\theta_{\lambda,k'}} \sum_{jj'} (c_{\lambda,k,j} c_{\lambda,k',j'})^{1/4} \\ &\quad \langle r_{\lambda,k',j'} | r_{\lambda,k,j} \rangle |m_{\lambda,k,j}\rangle \langle m_{\lambda,k',j'}| \otimes |k\rangle \langle k'| \end{aligned} \tag{A9}$$

can be seen as follows. The square of the right-hand side becomes

$$\begin{aligned} &\sum_{kk'k''} \sqrt{P_K(k)P_K(k'')P_K(k')} e^{i\theta_{\lambda,k} - i\theta_{\lambda,k''}} \sum_{jj'j''} (c_{\lambda,k,j} c_{\lambda,k'',j''})^{1/4} \sqrt{c_{\lambda,k',j'}} \\ &\quad \langle r_{\lambda,k',j'} | r_{\lambda,k,j} \rangle \langle r_{\lambda,k'',j''} | r_{\lambda,k',j'} \rangle |m_{\lambda,k,j}\rangle \langle m_{\lambda,k'',j''}| \otimes |k\rangle \langle k''| \\ &= \sum_{kk'k''} \sqrt{P_K(k)P_K(k'')P_K(k')} e^{i\theta_{\lambda,k} - i\theta_{\lambda,k''}} \sum_{jj''} (c_{\lambda,k,j} c_{\lambda,k'',j''})^{1/4} \\ &\quad \langle r_{\lambda,k'',j''} | \left(\sum_{j'} \sqrt{c_{\lambda,k',j'}} |r_{\lambda,k',j'}\rangle \langle r_{\lambda,k',j'}| \right) |r_{\lambda,k,j}\rangle |m_{\lambda,k,j}\rangle \langle m_{\lambda,k'',j''}| \otimes |k\rangle \langle k''|. \end{aligned} \tag{A10}$$

Taking the matrix power in both sides of (A1) results in

$$\sum_j (c_{\lambda,k,j})^a |r_{\lambda,k,j}\rangle \langle r_{\lambda,k,j}| = \sum_j (c_{\lambda,k',j})^a |r_{\lambda,k',j}\rangle \langle r_{\lambda,k',j}|, \quad \forall k, k' \tag{A11}$$

for every real number a . This implies

$$\begin{aligned} &\sum_{j'} \sqrt{c_{\lambda,k',j'}} |r_{\lambda,k',j'}\rangle \langle r_{\lambda,k',j'}| \\ &= \left(\sum_{j'} (c_{\lambda,k',j'})^{1/4} |r_{\lambda,k',j'}\rangle \langle r_{\lambda,k',j'}| \right) \left(\sum_{j'} (c_{\lambda,k',j'})^{1/4} |r_{\lambda,k',j'}\rangle \langle r_{\lambda,k',j'}| \right) \\ &= \left(\sum_{j'} (c_{\lambda,k'',j'})^{1/4} |r_{\lambda,k'',j'}\rangle \langle r_{\lambda,k'',j'}| \right) \left(\sum_{j'} (c_{\lambda,k,j})^{1/4} |r_{\lambda,k,j}\rangle \langle r_{\lambda,k,j}| \right). \end{aligned} \tag{A12}$$

Substituting (A12) into (A10) gives

$$\begin{aligned}
 & \sum_{kk''} \sqrt{P_K(k)P_K(k'')} P_K(k') e^{i\theta_{\lambda,k} - i\theta_{\lambda,k''}} \sum_{jj''} \sqrt{c_{\lambda,k,j} c_{\lambda,k'',j''}} \\
 & \quad \langle r_{\lambda,k'',j''} | r_{\lambda,k,j} \rangle |m_{\lambda,k,j}\rangle \langle m_{\lambda,k'',j''} | \otimes |k\rangle \langle k''| \\
 & = \sum_{kk''} \sqrt{P_K(k)P_K(k'')} e^{i\theta_{\lambda,k} - i\theta_{\lambda,k''}} \sum_{jj''} \sqrt{c_{\lambda,k,j} c_{\lambda,k'',j''}} \\
 & \quad \langle r_{\lambda,k'',j''} | r_{\lambda,k,j} \rangle |m_{\lambda,k,j}\rangle \langle m_{\lambda,k'',j''} | \otimes |k\rangle \langle k''| \\
 & = \text{Tr}_{\mathcal{H}_\lambda} |\phi_\lambda\rangle \langle \phi_\lambda|,
 \end{aligned} \tag{A13}$$

which confirms (A9).

Combining this with (A6) and noting that

$$\begin{aligned}
 I \otimes \sqrt{\text{Tr}_{\mathcal{H}_\lambda} |\phi_\lambda\rangle \langle \phi_\lambda|} |\tilde{\Phi}_{\lambda,k}\rangle |k\rangle & = \sum_{k'} \sqrt{P_K(k')} P_K(k) e^{i\theta_{\lambda,k'} - i\theta_{\lambda,k}} \sum_{jj'} (c_{\lambda,k,j} c_{\lambda,k',j'})^{1/4} \\
 & \quad \langle r_{\lambda,k,j} | r_{\lambda,k',j'} \rangle |r_{\lambda,k,j}\rangle |m_{\lambda,k',j'}\rangle \otimes |k'\rangle,
 \end{aligned} \tag{A14}$$

we get

$$\begin{aligned}
 & \sqrt{\mathcal{G}(\rho_{AB})} \sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1} \mathcal{B}(\rho_{AB}) \sqrt{\mathcal{G} \circ \mathcal{B}(\rho_{AB})}^{-1} \sqrt{\mathcal{G}(\rho_{AB})} \\
 & = \sum_{\lambda\lambda'} \sqrt{P_\Lambda(\lambda)P_\Lambda(\lambda')} e^{i\theta_{\lambda,k} - i\theta_{\lambda',k}} \sum_{k'k''} \sqrt{P_K(k')P_K(k'')} P_K(k) e^{i\theta_{\lambda,k'} - i\theta_{\lambda,k} + i\theta_{\lambda',k} - i\theta_{\lambda',k''}} \\
 & \quad \sum_{jj'} (c_{\lambda,k,j} c_{\lambda,k',j'})^{1/4} \langle r_{\lambda,k,j} | r_{\lambda,k',j'} \rangle \sum_{lj''} (c_{\lambda',k,l} c_{\lambda',k'',j''})^{1/4} \langle r_{\lambda',k'',j''} | r_{\lambda',k,l} \rangle \\
 & \quad |r_{\lambda,k,j}\rangle \langle r_{\lambda',k,l} | \otimes |m_{\lambda,k',j'}\rangle \langle m_{\lambda',k'',j''} | \otimes |k'\rangle \langle k''| \\
 & = \sum_{\lambda\lambda'} \sqrt{P_\Lambda(\lambda)P_\Lambda(\lambda')} \sum_{k'k''} \sqrt{P_K(k')P_K(k'')} e^{i\theta_{\lambda,k'} - i\theta_{\lambda',k''}} \\
 & \quad \sum_{j'j''} \sqrt{c_{\lambda,k',j'} c_{\lambda',k'',j''}} |r_{\lambda,k',j'}\rangle \langle r_{\lambda',k'',j''} | \otimes |m_{\lambda,k',j'}\rangle \langle m_{\lambda',k'',j''} | \otimes |k'\rangle \langle k''| \\
 & = |\Psi\rangle \langle \Psi|,
 \end{aligned} \tag{A15}$$

where in the second equality we used (A11). This confirms (23).

Acknowledgements M.H. is very grateful to Dr. Jiawei Wu for helpful discussions for the usefulness of quantum memory in private dense coding. We also thank an anonymous reviewer for suggesting a simpler Proof of Proposition 3. R.T. acknowledges the support of the Lee Kuan Yew Postdoctoral Fellowship at Nanyang Technological University Singapore. M.H. is supported in part by the National Natural Science Foundation of China (Grant No. 62171212).

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest There are no conflict of interest.

References

1. Bennett, C.H., Wiesner, S.J.: Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992). <https://doi.org/10.1103/PhysRevLett.69.2881>
2. Hiroshima, T.: Optimal dense coding with mixed state entanglement. *J. Phys. A: Math. Gen.* **34**(35), 6907 (2001). <https://doi.org/10.1088/0305-4470/34/35/316>
3. Bowen, G.: Classical information capacity of superdense coding. *Phys. Rev. A* **63**, 022302 (2001). <https://doi.org/10.1103/PhysRevA.63.022302>
4. Horodecki, M., Horodecki, P., Horodecki, R., Leung, D., Terhal, B.: Classical capacity of a noiseless quantum channel assisted by noisy entanglement. *Quantum Inf. Comput.* **1**, 70 (2001)
5. Winter, A.: Scalable programmable quantum gates and a new aspect of the additivity problem for the classical capacity of quantum channels. *J. Math. Phys.* **43**(9), 4341–4352 (2002) https://pubs.aip.org/aip/jmp/article-pdf/43/9/4341/8171944/4341_1_online.pdf. <https://doi.org/10.1063/1.1498489>
6. Bruß, D., D’Ariano, G.M., Lewenstein, M., Macchiavello, C., Sen(De), A., Sen, U.: Distributed quantum dense coding. *Phys. Rev. Lett.* **93**, 210501 (2004). <https://doi.org/10.1103/PhysRevLett.93.210501>
7. Beran, M.R., Cohen, S.M.: Nonoptimality of unitary encoding with quantum channels assisted by entanglement. *Phys. Rev. A* **78**, 062337 (2008). <https://doi.org/10.1103/PhysRevA.78.062337>
8. Horodecki, M., Piani, M.: On quantum advantage in dense coding. *J. Phys. A: Math. Theor.* **45**(10), 105306 (2012). <https://doi.org/10.1088/1751-8113/45/10/105306>
9. Datta, N., Leditzky, F.: Second-order asymptotics for source coding, dense coding, and pure-state entanglement conversions. *IEEE Trans. Inf. Theory* **61**(1), 582–608 (2015). <https://doi.org/10.1109/TIT.2014.2366994>
10. Das, S., Wilde, M.M.: Quantum rebound capacity. *Phys. Rev. A* **100**, 030302 (2019). <https://doi.org/10.1103/PhysRevA.100.030302>
11. Laurenza, R., Lupo, C., Lloyd, S., Pirandola, S.: Dense coding capacity of a quantum channel. *Phys. Rev. Res.* **2**, 023023 (2020). <https://doi.org/10.1103/PhysRevResearch.2.023023>
12. Wakakuwa, E.: Superdense coding in the resource theory of asymmetry. *Phys. Rev. A* **104**, 042413 (2021). <https://doi.org/10.1103/PhysRevA.104.042413>
13. Hayashi, M., Wang, K.: Dense coding with locality restriction on decoders: Quantum encoders versus superquantum encoders. *PRX Quantum* **3**, 030346 (2022). <https://doi.org/10.1103/PRXQuantum.3.030346>
14. Zhao, R., Dudin, Y.O., Jenkins, S.D., Campbell, C.J., Matsukevich, D.N., Kennedy, T. a B., Kuzmich, A.: Long-lived quantum memory. *Nature Phys.* **5**(2), 100–104 (2009). <https://doi.org/10.1038/nphys1152>
15. Heshami, K., England, D.G., Humphreys, P.C., Bustard, P.J., Acosta, V.M., Nunn, J., Sussman, B.J.: Quantum memories: emerging applications and recent advances. *J. Mod. Opt.* **63**(20), 2005–2028 (2016). <https://doi.org/10.1080/09500340.2016.1148212>
16. Korzekwa, K., Puchała, Z., Tomamichel, M., Życzkowski, K.: Encoding classical information into quantum resources. *IEEE Trans. Inf. Theory* **68**(7), 4518–4530 (2022). <https://doi.org/10.1109/TIT.2022.3157440>
17. Delsarte, P., Piret, P.: Algebraic constructions of shannon codes for regular channels. *IEEE Trans. Inf. Theory* **28**(4), 593–599 (1982). <https://doi.org/10.1109/TIT.1982.1056525>
18. Hayashi, M.: Exponential decreasing rate of leaked information in universal random privacy amplification. *IEEE Trans. Inf. Theory* **57**(6), 3989–4001 (2011). <https://doi.org/10.1109/TIT.2011.2110950>
19. Hayashi, M.: Quantum wiretap channel with non-uniform random number and its exponent and equivocation rate of leaked information. *IEEE Trans. Inf. Theory* **61**(10), 5595–5622 (2015). <https://doi.org/10.1109/TIT.2015.2464215>

20. Dobrushin, R.: Asymptotic optimality of group and systematic codes for some channels. *Theory Prob. Appl.* **8**(1), 47–60 (1963)
21. Elias, P.: Coding for noisy channels. *IRE Conv. Rec.* **3**, 37–46 (1955)
22. Hayashi, M., Watanabe, S.: Finite-length analyses for source and channel coding on markov chains. *Entropy* **22**(4) (2020). <https://doi.org/10.3390/e22040460>
23. Wu, J., Long, G.-L., Hayashi, M.: Quantum secure direct communication with private dense coding using a general preshared quantum state. *Phys. Rev. Appl.* **17**, 064011 (2022). <https://doi.org/10.1103/PhysRevApplied.17.064011>
24. Streltsov, A., Adesso, G., Plenio, M.B.: Colloquium: Quantum coherence as a resource. *Rev. Mod. Phys.* **89**, 041003 (2017). <https://doi.org/10.1103/RevModPhys.89.041003>
25. Bartlett, S.D., Rudolph, T., Spekkens, R.W.: Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.* **79**, 555–609 (2007). <https://doi.org/10.1103/RevModPhys.79.555>
26. Gour, G., Spekkens, R.W.: The resource theory of quantum reference frames: manipulations and monotones. *New J. Phys.* **10**(3), 033023 (2008). <https://doi.org/10.1088/1367-2630/10/3/033023>
27. Gour, G., Marvian, I., Spekkens, R.W.: Measuring the quality of a quantum reference frame: The relative entropy of frameness. *Phys. Rev. A* **80**, 012307 (2009). <https://doi.org/10.1103/PhysRevA.80.012307>
28. Bartlett, S.D., Rudolph, T., Spekkens, R.W., Turner, P.S.: Quantum communication using a bounded-size quantum reference frame. *New J. Phys.* **11**(6), 063013 (2009). <https://doi.org/10.1088/1367-2630/11/6/063013>
29. Marvian Mashhad, I.: Symmetry, asymmetry and quantum information. PhD Thesis (2012)
30. Marvian, I., Spekkens, R.W.: The theory of manipulations of pure state asymmetry: I. basic tools, equivalence classes and single copy transformations. *New J. Phys.* **15**(3), 033001 (2013). <https://doi.org/10.1088/1367-2630/15/3/033001>
31. Marvian, I., Spekkens, R.W.: Asymmetry properties of pure quantum states. *Phys. Rev. A* **90**, 014102 (2014). <https://doi.org/10.1103/PhysRevA.90.014102>
32. Marvian, I., Spekkens, R.W.: Extending noether’s theorem by quantifying the asymmetry of quantum states. *Nat. Commun.* **5**(1), 1–8 (2014). <https://doi.org/10.1038/ncomms4821>
33. Marvian, I., Spekkens, R.W.: Modes of asymmetry: The application of harmonic analysis to symmetric quantum dynamics and quantum reference frames. *Phys. Rev. A* **90**, 062110 (2014). <https://doi.org/10.1103/PhysRevA.90.062110>
34. Wakakuwa, E.: Symmetrizing cost of quantum states. *Phys. Rev. A* **95**, 032328 (2017). <https://doi.org/10.1103/PhysRevA.95.032328>
35. Hiai, F., Petz, D.: The proper formula for relative entropy and its asymptotics in quantum probability. *Commun. Math. Phys.* **143**(1), 99–114 (1991). <https://doi.org/10.1007/BF02100287>
36. Hayashi, M.: *A Group Theoretic Approach to Quantum Information*. Springer, Switzerland (2017). <https://doi.org/10.1007/978-3-319-45241-8>
37. Lloyd, S.: Enhanced sensitivity of photodetection via quantum illumination. *Science* **321**(5895), 1463–1465 (2008). <https://doi.org/10.1126/science.1160627>
38. Tan, S.-H., Erkmen, B.I., Giovannetti, V., Guha, S., Lloyd, S., Maccone, L., Pirandola, S., Shapiro, J.H.: Quantum illumination with gaussian states. *Phys. Rev. Lett.* **101**, 253601 (2008). <https://doi.org/10.1103/PhysRevLett.101.253601>
39. De Palma, G., Borregaard, J.: Minimum error probability of quantum illumination. *Phys. Rev. A* **98**, 012101 (2018). <https://doi.org/10.1103/PhysRevA.98.012101>
40. de Vicente, J.I., Streltsov, A.: Genuine quantum coherence. *J. Phys. A: Math. Theor.* **50**(4), 045301 (2016). <https://doi.org/10.1088/1751-8121/50/4/045301>
41. Holevo, A.S.: The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory* **44**(1), 269–273 (1998). <https://doi.org/10.1109/18.651037>
42. Schumacher, B., Westmoreland, M.D.: Sending classical information via noisy quantum channels. *Phys. Rev. A* **56**, 131–138 (1997). <https://doi.org/10.1103/PhysRevA.56.131>
43. Holevo, A.S.: The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory* **44**(1), 269–273 (1998). <https://doi.org/10.1109/18.651037>
44. Schumacher, B., Westmoreland, M.D.: Sending classical information via noisy quantum channels. *Phys. Rev. A* **56**, 131–138 (1997). <https://doi.org/10.1103/PhysRevA.56.131>
45. Deng, F.-G., Long, G.L., Liu, X.-S.: Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. *Phys. Rev. A* **68**, 042317 (2003). <https://doi.org/10.1103/PhysRevA.68.042317>

46. Petz, D.: Sufficient subalgebras and the relative entropy of states of a von Neumann algebra. *Commun. Math. Phys.* **105**(1), 123 (1986). <https://doi.org/10.1007/BF01212345>
47. Hayden, P., Jozsa, R., Petz, D., Winter, A.: Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Commun. Math. Phys.* **246**(2), 359 (2004). <https://doi.org/10.1007/s00220-004-1049-z>
48. Rains, E.M.: Bound on distillable entanglement. *Phys. Rev. A* **60**, 179–184 (1999). <https://doi.org/10.1103/PhysRevA.60.179>
49. Devetak, I., Shor, P.W.: The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Commun. Math. Phys.* **256**(2), 287–303 (2005). <https://doi.org/10.1007/s00220-005-1317-6>
50. Walgate, J., Short, A.J., Hardy, L., Vedral, V.: Local distinguishability of multipartite orthogonal quantum states. *Phys. Rev. Lett.* **85**, 4972–4975 (2000). <https://doi.org/10.1103/PhysRevLett.85.4972>
51. Ghosh, S., Kar, G., Roy, A., Sen(De), A., Sen, U.: Distinguishability of bell states. *Phys. Rev. Lett.* **87**, 277902 (2001). <https://doi.org/10.1103/PhysRevLett.87.277902>
52. Nathanson, M.: Distinguishing bipartite orthogonal states using LOCC: Best and worst cases. *J. Math. Phys.* **46**(6), 062103 (2005). <https://doi.org/10.1063/1.1914731>
53. Owari, M., Hayashi, M.: Local copying and local discrimination as a study for nonlocality of a set of states. *Phys. Rev. A* **74**, 032108 (2006). <https://doi.org/10.1103/PhysRevA.74.032108>
54. Fan, H.: Distinguishability and indistinguishability by local operations and classical communication. *Phys. Rev. Lett.* **92**, 177905 (2004). <https://doi.org/10.1103/PhysRevLett.92.177905>
55. Hashimoto, T., Horibe, M., Hayashi, A.: Simple criterion for local distinguishability of generalized bell states in prime dimension. *Phys. Rev. A* **103**, 052429 (2021). <https://doi.org/10.1103/PhysRevA.103.052429>
56. Li, M.-S., Shi, F., Wang, Y.-L.: Local discrimination of generalized bell states via commutativity. *Phys. Rev. A* **105**, 032455 (2022). <https://doi.org/10.1103/PhysRevA.105.032455>
57. Yang, Y.-H., Yan, R.-Y., Wang, X.-L., Yuan, J.-T., Zuo, H.-J.: Novel method for one-way local distinguishability of generalized bell states in arbitrary dimension. *J. Phys. A: Math. Theor.* **55**(1), 015301 (2021). <https://doi.org/10.1088/1751-8121/ac38ed>
58. Stanley, R.P.: *Enumerative Combinatorics*, vol. 1, 2nd edn. Cambridge University Press, Cambridge (2011)
59. Pirandola, S.: Quantum reading of a classical digital memory. *Phys. Rev. Lett.* **106**, 090504 (2011). <https://doi.org/10.1103/PhysRevLett.106.090504>
60. Ogawa, T., Nagaoka, H.: Strong converse and stein's lemma in quantum hypothesis testing. *IEEE Trans. Inf. Theory* **46**(7), 2428–2433 (2000). <https://doi.org/10.1109/18.887855>
61. Modi, K., Brodutch, A., Cable, H., Paterek, T., Vedral, V.: The classical-quantum boundary for correlations: Discord and related measures. *Rev. Mod. Phys.* **84**, 1655–1707 (2012). <https://doi.org/10.1103/RevModPhys.84.1655>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.