Private and quantum capacities of more capable and less noisy quantum channels

Shun Watanabe*
Department of Information Science and Intelligent Systems, University of Tokushima, 2-1, Minami-josanjima, Tokushima, 770-8506 Japan
(Received 26 October 2011; published 24 January 2012)

Two classes of quantum channels, which we call *more capable* and *less noisy*, are introduced. The more capable class consists of channels such that the quantum capacities of the complementary channels to the environments are zero. The less noisy class consists of channels such that the private capacities of the complementary channels to the environment are zero. For the more capable class, it is clarified that the private capacity and quantum capacity coincide. For the less noisy class, it is clarified that the private capacity and quantum capacity can be single letter characterized.

DOI: 10.1103/PhysRevA.85.012326 PACS number(s): 03.67.Dd, 89.70.−a

I. INTRODUCTION

One of the most important problem in quantum information theory is to determine the quantum capacity of a noisy quantum channel. The capacity is defined as the transmission rate optimized over all possible quantum error correcting codes such that decoding errors vanish in the limit of asymptotically many uses of the channel.

Mathematically, a quantum channel can be described by the trace-preserving completely positive (TPCP) map from the input system to the output system. By using the Stinespring dilation of the TPCP map, we can naturally define a complementary channel to an environment system, and we can regard the noisy quantum channel as a wiretap channel [1,2] from the sender to the legitimate receiver and the eavesdropper, who can observe the environment system of the channel (e.g., see [3]). Then we can define the private capacity of the noisy quantum channel as the transmission rate optimized over all possible wiretap codes such that decoding errors and information leakage vanish in the limit of asymptotically many uses of the channel.

The private capacity and quantum capacity of noisy quantum channels were established in [4–7]. However, unlike the capacity formula of a classical noisy channel or the private-capacity formula of a classical wiretap channel, the private-capacity and quantum-capacity formulas are not single letter characterized; i.e., the formulas involve the limit with respect to the number of channel uses, and they are not computable. Indeed, some numerical evidence clarified that the expressions in the capacity formulas are not additive [8–11], and the single-letter characterization is not possible in general, at least by using the same expressions.

A quantum channel is called degradable if there exists another degrading channel such that the conjunction of the channel to the legitimate receiver and the degrading channel coincide with the complementary channel to the eavesdropper. In such a case, the single-letter characterizations of the private capacity and quantum capacity were established [3,12].

A quantum channel is called conjugate degradable if there exists another degrading channel such that the conjunction of the channel to the legitimate receiver and the degrading channel coincide with the complementary channel to the eavesdropper up to complex conjugation. In such a case, the single-letter characterizations were also established [13].

To date, all quantum channels whose capacities are single letter characterized are degradable or conjugate degradable, and it is important to clarify a broader class of quantum channels such that the single-letter characterizations are possible.[1]

Aside from the possibility of the single-letter characterizations, there is also another interesting problem. In the quantum information theory, the private information transmission and the quantum information transmission are closely related [4,14–16], and the possibility of the latter implies the possibility of the former. However, the private information transmission and the quantum information transmission are not exactly equivalent. Indeed, although the private capacity and quantum capacity coincide for degradable quantum channels [17], the former can be strictly larger than the latter in general. Particularly, the private capacity can be positive even if the quantum capacity is zero [18]. Thus it is important to clarify a condition on quantum channels such that the private capacity and quantum capacity either do or do not coincide.

To shed light on the two above-mentioned problems, we introduce two classes of quantum channels, which we call *more capable* and *less noisy*. The more capable class consists of channels such that the quantum capacities of the complementary channels are zero. The less noisy class consists of channels such that the private capacities of the complementary channels are zero. Later, these definitions turn out to be natural analogies of the partial orderings, more capable and less noisy, between classical channels [19].

The inclusive relation of the degradable, the conjugate degradable, the less noisy, and the more capable classes is summarized in Fig. 1. In this paper, we show that the private capacity and quantum capacity coincide for channels in the more capable class. Furthermore, we also show that the private capacity and quantum capacity can be single letter characterized for channels in the less noisy class. These

*shun-wata@is.tokushima-u.ac.jp

[1]There are also channels called antidegradable or conjugate antidegradable. The capacities of those channels are also single letter characterized, but the capacities are equal to zero.

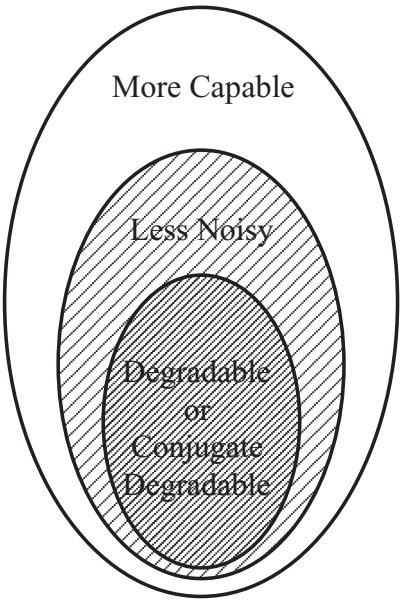

FIG. 1. The inclusive relation of the degradable, the conjugate degradable, the less noisy, and the more capable classes of quantum channels.

results provide partial solutions to the two above-mentioned problems.

The rest of the paper is organized as follows. In Sec. II, we review some known results on the private capacity and quantum capacity of quantum channels. In Sec. III, the more capable and less noisy classes are introduced, and we state our main results. In Sec. IV, we summarize certain properties implied by the more capable and less noisy classes and show proofs of our main results. We finalize the paper with a conclusion in Sec. IV.

II. PRELIMINARIES

Let $\mathcal{N}_B$ be a quantum channel from an input system $\mathcal{H}_A$ to an output system $\mathcal{H}_B$. By using the Stinespring dilation (e.g., see [3]), there exist an environment system $\mathcal{H}_E$ and an isometry U_{BE} from $\mathcal{H}_A$ to the joint system $\mathcal{H}_B \otimes \mathcal{H}_E$ such that

$$\mathcal{N}_B(\rho) = \mathrm{Tr}_E[U_{BE}\rho U_{BE}^*]$$

for every input ρ, where Tr_E is the partial trace with respect to the environment system. By using this representation, we can naturally define another channel:

$$\mathcal{N}_E(\rho) = \mathrm{Tr}_B[U_{BE}\rho U_{BE}^*],$$

which is usually called the complementary channel of $\mathcal{N}_B$. Although the Stinespring dilation is not unique, the following arguments do not depend on the choice of the dilation because two dilations can be converted to each other by applying a local unitary to the environment systems.

Throughout the paper, we basically follow the notations from [3,20]. The von Neumann entropy of a density matrix ρ is defined by $H(\rho) = -\mathrm{Tr}\rho\log_2\rho$, and the quantum relative entropy between ρ and σ is defined by $D(\rho\|\sigma) = \mathrm{Tr}\rho(\log_2\rho - \log_2\sigma)$. For input state ρ_A to the channel $\mathcal{N}_B$, the coherent information is defined by $I_c(A\rangle B)_\rho = H(\mathcal{N}_B(\rho_A)) - H(\mathcal{N}_E(\rho_A))$. When the input state is clear from the context, we omit the subscript and denote $I_c(A\rangle B)$. The quantum mutual information of ρ_{XB} on the joint system is defined by $I(X;B) = H(\rho_X) + H(\rho_B) - H(\rho_{XB})$. Particularly, when ρ_{XB} is classical with respect to X, i.e., ρ_{XB} is of the form

$$\rho_{XB} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_B^x,$$

then the quantum mutual information can be written as

$$I(X;B) = H(\rho_B) - \sum_x P_X(x)H(\rho_B^x).$$

When the legitimate receiver can observe the output of $\mathcal{N}_B$ and the eavesdropper can observe the output of $\mathcal{N}_E$, the private capacity is characterized by [4,5]

$$C_p(\mathcal{N}_B) = \lim_{n\to\infty}\frac{1}{n}C_p^{(1)}\left(\mathcal{N}_B^{\otimes n}\right), \tag{1}$$

where

$$C_p^{(1)}(\mathcal{N}_B) := \max_{P_U,\{\rho_A^u\}}[I(U;B) - I(U;E)],$$

where $\{\rho_A^u\}$ are states (not necessarily pure states) on $\mathcal{H}_A$ indexed by $u \in \mathcal{U}$ and P_U is a probability distribution on a finite set $\mathcal{U}$.

On the other hand, when the sender wants to transmit quantum information to the receiver through channel $\mathcal{N}_B$, the quantum capacity is characterized by [4,6]

$$Q(\mathcal{N}_B) = \lim_{n\to\infty}\frac{1}{n}Q^{(1)}\left(\mathcal{N}_B^{\otimes n}\right), \tag{2}$$

where

$$Q^{(1)}(\mathcal{N}_B) := \max_{\rho_A} I_c(A\rangle B)_\rho.$$

Neither Eq. (1) nor Eq. (2) can be single letter characterized; i.e., $C_p(\mathcal{N}_B) > C_p^{(1)}(\mathcal{N})$ and $Q(\mathcal{N}) > Q^{(1)}(\mathcal{N})$ in general [8–11]. Furthermore, the private capacity can be strictly larger than the quantum capacity; i.e., $C_p(\mathcal{N}_B) > Q(\mathcal{N}_B)$ for some channels [18].

Channel $\mathcal{N}_B$ is said to be degradable if there exists a TPCP map $\mathcal{D}$ such that $\mathcal{D}\circ\mathcal{N}_B = \mathcal{N}_E$. This is a quantum analog of a degraded broadcast channel [21]. When $\mathcal{N}_B$ is degradable, then it is known [3,12] that the single-letter formulas hold; i.e., $C_p(\mathcal{N}_B) = C_p^{(1)}(\mathcal{N}_B)$ and $Q(\mathcal{N}_B) = Q^{(1)}(\mathcal{N}_B)$. Furthermore, it is also known that $C_p(\mathcal{N}_B) = Q(\mathcal{N}_B)$ for degradable channel $\mathcal{N}_B$ [17].

Let $\mathcal{C}$ denote entrywise complex conjugation with respect to a fixed basis of $\mathcal{H}_E$. Then, channel $\mathcal{N}_B$ is said to be conjugate degradable if there exists a TPCP map $\mathcal{D}$ such that $\mathcal{D}\circ\mathcal{N}_B = \mathcal{C}\circ\mathcal{N}_E$. When $\mathcal{N}_B$ is conjugate degradable, it is known that $Q(\mathcal{N}_B) = Q^{(1)}(\mathcal{N}_B)$ [13]. Later, it will turn out that $C_p(\mathcal{N}_B) = Q(\mathcal{N}_B) = Q^{(1)}(\mathcal{N}_B)$ also holds.

III. MAIN STATEMENTS

In this section, we introduce two classes of quantum channels and show our main results.

Definition 1. The quantum channel $\mathcal{N}_B$ is said to be *more capable* than the environment, or just more capable,

if the quantum capacity of the complementary channel to the environment is zero, i.e.,

$$Q(\mathcal{N}_E) = 0. \tag{3}$$

Definition 2. The quantum channel $\mathcal{N}_B$ is said to be *less noisy* than the environment, or just less noisy, if the private capacity of the complementary channel to the environment is zero, i.e.,

$$C_p(\mathcal{N}_E) = 0. \tag{4}$$

Since $C_p(\mathcal{N}_E) \geqslant Q(\mathcal{N}_E)$, less noisy implies more capable. By using the eigenvalue decomposition

$$\rho_{A^n} = \sum_{x^n \in \mathcal{X}^n} P_{X^n}(x^n) |\psi_{x^n}\rangle\langle\psi_{x^n}|$$

of ρ_{A^n}, we can rewrite the coherent information as

$$I_c(A^n\rangle B^n) = I(X^n; B^n) - I(X^n; E^n), \tag{5}$$

where we set $|\mathcal{X}| = \dim \mathcal{H}_A$. Thus, by noting Eq. (2), the quantum channel $\mathcal{N}_B$ is more capable if and only if

$$I(X^n; B^n) \geqslant I(X^n; E^n), \forall (P_{X^n}\{|\psi_{x^n}\rangle\}), \tag{6}$$

holds for every $n \geqslant 1$. Furthermore, by noting Eq. (1), the quantum channel $\mathcal{N}_B$ is less noisy if and only if

$$I(U^n; B^n) \geqslant I(U^n; E^n), \forall \left(P_{U^n}\left\{\rho_{A^n}^{u^n}\right\}\right), \tag{7}$$

holds for every $n \geqslant 1$. Equations (6) and (7) resemble the definitions of more capable and less noisy for classical channels [19], and it is justified to call quantum channels satisfying Eq. (3) or Eq. (4) more capable or less noisy.

In [19], an alternative description of less noisy, less divergence contracting, was introduced, and we can also extend such a description to the quantum channel. The quantum channel $\mathcal{N}_B$ is said to be less divergence contracting if

$$\begin{aligned} &D\left(\mathcal{N}_B^{\otimes n}(\rho_{A^n}) \| \mathcal{N}_B^{\otimes n}(\hat{\rho}_{A^n})\right) \\ &\quad \geqslant D\left(\mathcal{N}_E^{\otimes n}(\rho_{A^n}) \| \mathcal{N}_E^{\otimes n}(\hat{\rho}_{A^n})\right), \quad \forall \rho_{A^n}, \hat{\rho}_{A^n} \end{aligned} \tag{8}$$

holds for every $n \geqslant 1$. Later, we will show that the quantum channel is less noisy if and only if it is less divergence contracting (Proposition 4). This alternative description plays a crucial role when we prove Theorem 2.

The following are our main results.

Theorem 1. Suppose that the quantum channel $\mathcal{N}_B$ is more capable. Then, we have

$$C_p(\mathcal{N}_B) = Q(\mathcal{N}_B).$$

Theorem 2. Suppose that the quantum channel $\mathcal{N}_B$ is less noisy. Then, we have

$$C_p(\mathcal{N}_B) = Q(\mathcal{N}_B) = Q^{(1)}(\mathcal{N}_B).$$

When $\mathcal{N}_B$ is conjugate degradable, we can show that $C_p(\mathcal{N}_E) = 0$ as follows. Suppose that the sender sends a state ρ_i that corresponds to the message i and the eavesdropper uses a positive operator-valued measure (POVM) $\{M_i\}$.[2] Then, for the entrywise complex conjugate POVM $\{\bar{M}_i\}$, we have

$$\begin{aligned} \mathrm{Tr}\left[\bar{M}_i \mathcal{D}^{\otimes n} \circ \mathcal{N}_B^{\otimes n}(\rho_i)\right] &= \mathrm{Tr}\left[\bar{M}_i \mathcal{C}^{\otimes n} \circ \mathcal{N}_E^{\otimes n}(\rho_i)\right] \\ &= \mathrm{Tr}\left[M_i \mathcal{N}_E^{\otimes n}(\rho_i)\right], \end{aligned}$$

where the last equality follows because $\bar{M}_i^T = M_i$ and $[\mathcal{C}^{\otimes n} \circ \mathcal{N}_E^{\otimes n}(\rho_i)]^T = \mathcal{N}_E^{\otimes n}(\rho_i)$. Thus, the legitimate receiver can get exactly the same information as the eavesdropper, and private information transmission to the eavesdropper is impossible. From this argument, conjugate degradable implies less noisy.

When the quantum capacity of the channel is 0 but it can be used to share bound entanglement, then the channel is called a binding-entanglement channel [22]. Particularly, when the channel produces a positive partial transpose (PPT) bound entanglement, the channel is called a PPT binding-entanglement channel. If a complementary channel is a binding-entanglement channel, then the main channel obviously belongs to the more capable class. Since the complementary channel of the conjugate degradable channel can only produce a PPT bipartite state [13], if there exists a conjectured negative partial transpose (NPT) binding-entanglement channel, the complementary of such a channel belongs to the more capable class but not to the conjugate degradable class.

It is known that there exists a channel such that the quantum capacity is zero (PPT binding-entanglement channel) but the private capacity is strictly positive [18]. Let the complementary channel $\mathcal{N}_E$ be such a channel. Then channel $\mathcal{N}_B$ is more capable but not less noisy.[3] Thus, the more capable class is strictly broader than the less noisy class. However, it is not yet clear whether the less noisy class is strictly broader than the degradable or conjugate degradable classes.

IV. PROOF OF THEOREMS

A. Properties of $C_p^{(1)}(\mathcal{N}_B)$ and $Q^{(1)}(\mathcal{N}_B)$

In this section, we summarize the properties of $C_p^{(1)}(\mathcal{N}_B)$ and $Q^{(1)}(\mathcal{N}_B)$ when Eq. (6) or Eq. (7) holds for $n = 1$. For $n \geqslant 2$, we can also show similar properties of $C_p^{(1)}(\mathcal{N}_B^{\otimes n})$ and $Q^{(1)}(\mathcal{N}_B^{\otimes n})$ when Eq. (6) or Eq. (7) holds for each n by considering n times extension of $\mathcal{N}_B$. The following properties can be regarded as quantum extensions of the properties shown for classical channels in the literature [2,19,23,24]

Proposition 1. Suppose that Eq. (6) holds for $n = 1$. Then we have

$$C_p^{(1)}(\mathcal{N}_B) = Q^{(1)}(\mathcal{N}_B).$$

[2]The role of the legitimate receiver and the eavesdropper is interchanged because we are considering the private capacity of $\mathcal{N}_E$.

[3]Note that the private and quantum capacities of this channel are strictly positive, which can be checked as follows. If $Q(\mathcal{N}_B) = 0$, then the complementary channel $\mathcal{N}_E$ is more capable. Then, Theorem 1 implies that $Q(\mathcal{N}_E) = C_p(\mathcal{N}_E)$, which contradicts the fact that $C_p(\mathcal{N}_E) > Q(\mathcal{N}_E) = 0$.

Proof. For any P_U and $\{\rho_A^u\}$, let

$$\rho_A^u = \sum_x \alpha_{u,x} |\psi_{u,x}\rangle\langle\psi_{u,x}|$$

be an eigenvalue decomposition. Let $\tilde{X}$ be the random variable on $\mathcal{U}\times\mathcal{X}$ such that

$$P_{\tilde{X}|U}(u',x|u) = \begin{cases} \alpha_{u,x} & \text{if } u = u', \\ 0 & \text{otherwise.} \end{cases}$$

Then, we have

$$\begin{aligned} I(U;B) - I(U;E) = [I(\tilde{X};B) - I(\tilde{X};E)] \\ - [I(\tilde{X};B|U) - I(\tilde{X};E|U)]. \end{aligned} \tag{9}$$

Since Eq. (6) holds for $n = 1$, we have

$$I(\tilde{X};B|U=u) - I(\tilde{X};E|U=u) \geqslant 0$$

for every u, which means that the second set of brackets in Eq. (9) is nonnegative. Furthermore, by noting that $\{|\psi_{u,x}\rangle\}$ are pure, we have

$$I(\tilde{X};B) - I(\tilde{X};E) = I_c(A\rangle B),$$

where

$$\rho_A = \sum_{u,x} P_U(u) P_{\tilde{X}|U}(u,x|u) |\psi_{u,x}\rangle\langle\psi_{u,x}|.$$

Since P_U and $\{\rho_A^u\}$ are arbitrary, we have

$$C_p^{(1)}(\mathcal{N}_B) \leqslant Q^{(1)}(\mathcal{N}_B).$$

The opposite inequality is obvious from the definitions of $C_p^{(1)}(\mathcal{N}_B)$, $Q^{(1)}(\mathcal{N}_B)$, and Eq. (5). ■

Proposition 2. Suppose that Eq. (6) does not hold for $n = 1$ and the density operator ρ_A^* maximizing $I_c(A\rangle B)$ is full rank. Then, we have

$$C_p^{(1)}(\mathcal{N}_B) > Q^{(1)}(\mathcal{N}_B).$$

Particularly when $\dim \mathcal{H}_A = 2$ and $C_p^{(1)}(\mathcal{N}_B) > 0$, the sufficient and required condition on

$$C_p^{(1)}(\mathcal{N}_B) = Q^{(1)}(\mathcal{N}_B)$$

is that Eq. (6) holds for $n = 1$.

Proof. Since Eq. (6) does not hold for $n = 1$, there exists $\hat{\rho}_A$ such that

$$I_c(A\rangle B)_{\hat{\rho}} < 0.$$

Since ρ_A^* is full rank, there exists $0 < \lambda < 1$ such that $\rho_A^* - \lambda\hat{\rho}_A$ is positive semidefinite. We construct P_U and $\{\rho_A^u\}$ as follows. Let

$$\hat{\rho}_A = \sum_x \hat{P}_X(x) |\hat{\psi}_x\rangle\langle\hat{\psi}_x|,$$

$$\rho_A^* - \lambda\hat{\rho}_A = \sum_x \beta_x |\phi_x\rangle\langle\phi_x|$$

be eigenvalue decompositions. Let $\mathcal{U} = \{0\}\cup\mathcal{X}$. Then, we set $P_U(0) = \lambda$, $P_U(u) = \beta_u$ for $u \in \mathcal{X}$, $\rho_A^0 = \hat{\rho}_A$, and $\rho_A^u = |\phi_u\rangle\langle\phi_u|$ for $u \in \mathcal{X}$. Let $\tilde{X}$ be the random variable on $\mathcal{U}\times\mathcal{X}$ such that

$$P_{\tilde{X}|U}(u',x|u) = \begin{cases} \hat{P}_X(x) & \text{if } u = u' = 0, \\ 1 & \text{if } x = u = u' \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then, we have

$$\begin{aligned} I(U;B) - I(U;E) &= I(\tilde{X};B) - I(\tilde{X};E) - [I(\tilde{X};B|U) \\ &\quad - I(\tilde{X};E|U)] = I(\tilde{X};B) - I(\tilde{X};E) \\ &\quad - \lambda[I(\tilde{X};B|U=0) - I(\tilde{X};E|U=0)] \\ &> I(\tilde{X};B) - I(\tilde{X};E) \qquad (10) \\ &= I_c(A\rangle B)_{\rho^*}, \qquad (11) \end{aligned}$$

where Eq. (10) follows from

$$I(\tilde{X};B|U=0) - I(\tilde{X};E|U=0) = I_c(A\rangle B)_{\hat{\rho}} < 0$$

and Eq. (11) follows from

$$\begin{aligned} &\sum_x P_U(0) P_{\tilde{X}|U}(0,x|0) |\hat{\psi}_x\rangle\langle\hat{\psi}_x| \\ &\quad + \sum_{u,x\in\mathcal{X}} P_U(u) P_{\tilde{X}|U}(u,x|u) |\phi_x\rangle\langle\phi_x| = \rho_A^*. \end{aligned}$$

Next, we show the latter statement of the proposition. The sufficient condition follows from Proposition 1. Suppose that

$$I_c(A\rangle B) \leqslant 0, \forall \rho_A \tag{12}$$

holds. Since $C_p^{(1)}(\mathcal{N}_B) > 0$, there exists P_U and $\{\rho_A^u\}$ such that

$$I(U;B) - I(U;E) > 0,$$

which implies the required condition. Next, we consider the case such that Eq. (12) does not hold. In this case, we have

$$\max_{\rho_A} I_c(A\rangle B) > 0.$$

Then, since $\dim \mathcal{H}_A = 2$, ρ_A^* must be full rank. Thus, the required condition follows from the former statement of the proposition. ■

Proposition 3. Equation (7) holds for $n = 1$ if and only if the coherent information is concave.[4] That is,

$$I_c(A\rangle B)_\rho \geqslant \sum_{i=1}^m p_i I_c(A\rangle B)_{\rho_i},$$

where $\rho = \sum_{i=1}^m p_i \rho_i$.

Proof. Let

$$\rho_i = \sum_x p_{i,x} |\psi_{i,x}\rangle\langle\psi_{i,x}|$$

be an eigenvalue decomposition. Then, let $\mathcal{U} = \{1,\ldots,m\}$, $P_U(u) = p_i$, $\tilde{X}$ be the random variable on $\mathcal{U}\times\mathcal{X}$ such that

$$P_{\tilde{X}|U}(u',x|u) = \begin{cases} p_{i,x} & \text{if } u' = u, \\ 0 & \text{otherwise.} \end{cases}$$

[4]It should be noted that the coherent information is known to be concave if the quantum channel $\mathcal{N}_B$ is degradable [Ref. [3], Eq. (9.89)].

Then, we have

$$I(U;B) - I(U;E) = [I(\tilde{X};B) - I(\tilde{X};E)] - [I(\tilde{X};B|U) - I(\tilde{X};E|U)]. \quad (13)$$

We also have

$$I(\tilde{X};B) - I(\tilde{X};E) = I_c(A\rangle B)_\rho$$

and

$$I(\tilde{X};B|U) - I(\tilde{X};E|U) = \sum_{i=1}^{m} p_i I_c(A\rangle B)_{\rho_i}.$$

Thus, from Eq. (13), Eq. (7) holds for $n = 1$ if and only if the coherent information $I_c(A\rangle B)$ is concave. ■

Proposition 4. The following two conditions are equivalent.

(i) Equation (7) holds for $n = 1$.
(ii) Equation (8) holds for $n = 1$.

Proof. We first show that (i) implies (ii). For any ρ_A, $\hat{\rho}_A$ and $0 \leqslant \lambda \leqslant 1$, let $\mathcal{U} = \{0,1\}$, $P_{U_\lambda}(0) = \lambda$, $P_{U_\lambda}(1) = 1 - \lambda$, $\rho_A^0 = \rho_A$, and $\rho_A^1 = \hat{\rho}_A$. Then, let

$$\begin{aligned} f(\lambda) &= I(U_\lambda;B) - I(U_\lambda;E) \\ &= \lambda D(\mathcal{N}_B(\rho_A)\|\mathcal{N}_B(\bar{\rho}_A)) + (1-\lambda) D(\mathcal{N}_B(\hat{\rho}_A)\|\mathcal{N}_B(\bar{\rho}_A)) \\ &\quad - \lambda D(\mathcal{N}_E(\rho_A)\|\mathcal{N}_E(\bar{\rho}_A)) \\ &\quad - (1-\lambda) D(\mathcal{N}_E(\hat{\rho}_A)\|\mathcal{N}_E(\bar{\rho}_A)), \end{aligned}$$

where

$$\bar{\rho}_A = \lambda\rho_A + (1-\lambda)\hat{\rho}_A.$$

By elementary calculation (cf. Ref. [3], Exercise 1.4), we have

$$f'(0) = D(\mathcal{N}_B(\rho_A)\|\mathcal{N}_B(\hat{\rho}_A)) - D(\mathcal{N}_E(\rho_A)\|\mathcal{N}_E(\hat{\rho}_A)).$$

Obviously, we have $f(0) = 0$. Since Eq. (7) holds for $n = 1$, $f(\lambda) \geqslant 0$ for any $0 \leqslant \lambda \leqslant 1$. Thus, $f'(0)$ must be non-negative, which means that Eq. (8) holds for $n = 1$.

Next, we show that (ii) implies (i). For any P_U and $\{\rho_A^u\}$, we have

$$\begin{aligned} I(U;B) &= \sum_u P_U(u) D\big(\mathcal{N}_B\big(\rho_A^u\big)\|\mathcal{N}_B(\bar{\rho}_A)\big), \\ I(U;E) &= \sum_u P_U(u) D\big(\mathcal{N}_E\big(\rho_A^u\big)\|\mathcal{N}_E(\bar{\rho}_A)\big), \end{aligned}$$

where

$$\bar{\rho}_A = \sum_u P_U(u)\rho_A^u.$$

Since Eq. (8) holds for $n = 1$, we have

$$I(U;B) \geqslant I(U;E).$$ ■

B. Proof of Theorem 1

It is a straightforward consequence of Proposition 1. Since $\mathcal{N}_B$ is more capable, Eq. (6) holds for every $n \geqslant 1$. Thus, we have $C_p^{(1)}(\mathcal{N}^{\otimes n}) = Q^{(1)}(\mathcal{N}_B^{\otimes n})$ for every $n \geqslant 1$, and the statement of the theorem follows from Eqs. (1) and (2). ■

C. Proof of Theorem 2

Since less noisy implies more capable, by Theorem 1, it suffices to show $Q(\mathcal{N}_B) = Q^{(1)}(\mathcal{N}_B)$. For this purpose, we will show that

$$\max_{\rho_{A^n}} I_c(A^n\rangle B^n) \leqslant n \max_{\rho_A} I_c(A\rangle B) \quad (14)$$

holds for every $n \geqslant 1$. For any input state $\rho_{A^k A^\ell}$ on $\mathcal{H}_A^{\otimes(k+\ell)}$, let ρ_{A^k} and ρ_{A^ℓ} be the partial traces. Then, we have

$$\begin{aligned} &I_c(A^k\rangle B^k) + I_c(A^\ell\rangle B^\ell) - I_c(A^k A^\ell\rangle B^k B^\ell) \\ &\quad = D\big(\mathcal{N}_B^{\otimes(k+\ell)}(\rho_{A^k A^\ell})\|\mathcal{N}_B^{\otimes k}(\rho_{A^k}) \otimes \mathcal{N}_B^{\otimes \ell}(\rho_{A^\ell})\big) \\ &\quad\quad - D\big(\mathcal{N}_E^{\otimes(k+\ell)}(\rho_{A^k A^\ell})\|\mathcal{N}_E^{\otimes k}(\rho_{A^k}) \otimes \mathcal{N}_E^{\otimes \ell}(\rho_{A^\ell})\big). \end{aligned}$$

Since Eq. (7) holds for $n = (k + \ell)$, by (n times extension of) Proposition 4, Eq. (8) also holds for $n = (k + \ell)$, which implies

$$I_c(A^k A^\ell\rangle B^k B^\ell) \leqslant I_c(A^k\rangle B^k) + I_c(A^\ell\rangle B^\ell).$$

Thus, Eq. (14) can be proved by induction. ■

V. CONCLUSION

In this paper, we introduced two classes of quantum channels, which we call more capable and less noisy. For the more capable class, we showed that the private capacity and quantum capacity coincide. For the less noisy class, we showed that the private capacity and quantum capacity can be single letter characterized.

Our results shed light on further understanding the private and quantum capacities of quantum channels. However, the conditions such that a certain channel belongs to the more capable class or the less noisy class are hard to verify in general, and we do not yet know whether there exists a channel that belongs to the less noisy class but not to the degradable or conjugate degradable classes, which is an important future research agenda.

ACKNOWLEDGMENTS

This research is partly supported by a Grant-in-Aid for Young Scientists (B) (Grant No. 2376033700) and a Grant-in-Aid for Scientific Research (A) (Grant No. 2324607101). The author also would like to thank an anonymous reviewer for helpful comments.

[1] A. D. Wyner, Bell Syst. Tech. J. **54**, 1355 (1975).
[2] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1979).
[3] M. Hayashi, *Quantum Information: An Introduction* (Springer, Berlin, 2006).
[4] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[5] N. Cai, A. Winter, and R. W. Yeung, Probl. Inf. Transm. (Engl. Transl.) **40**, 26 (2004).
[6] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).

[7] P. W. Shor, in Lecture Notes, MRSI Workshop on Quantum Computation (2002), [http://www.msri.org/realvideo/ln/msri/2002/quantumcrypto/shor/1/].
[8] G. Smith, J. M. Renes, and J. A. Smolin, Phys. Rev. Lett. **100**, 170502 (2008).
[9] P. W. Shor and J. A. Smolin (1996), e-print arXiv:quant-ph/9604006.
[10] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, Phys. Rev. A **57**, 830 (1998).
[11] G. Smith and J. A. Smolin, Phys. Rev. Lett. **98**, 030501 (2007).
[12] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).
[13] K. Brádler, N. Dutil, P. Hayden, and A. Muhammad, J. Math. Phys. **51**, 072201 (2010).
[14] B. Schumacher and M. D. Westmoreland, Phys. Rev. Lett. **80**, 5695 (1998).
[15] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[16] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).
[17] G. Smith, Phys. Rev. A **78**, 022306 (2008).
[18] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).
[19] J. Körner and K. Marton, *Keszthely Colloquium on Information Theory*, edited by I. Csishar and P. Elias (North-Holland Publishing Co., New York, 1975), pp. 411–423.
[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[21] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (Wiley, New York, 2006).
[22] P. Horodecki, M. Horodecki, and R. Horodecki, J. Mod. Opt. **47**, 347 (2000).
[23] M. van Dijk, IEEE Trans. Inf. Theory **43**, 712 (1997).
[24] O. Ozel and S. Ulukus, e-print arXiv:1110.4613.