Operations that do not disturb partially known quantum states

Masato Koashi and Nobuyuki Imoto
CREST Research Team for Interacting Carrier Electronics, School of Advanced Sciences, The Graduate University for Advanced Studies (SOKEN), Hayama, Kanagawa, 240-0193, Japan
(Received 17 January 2002; published 30 August 2002)

Consider a situation in which a quantum system is secretly prepared in a state chosen from the known set of states. We present a principle that gives a definite distinction between the operations that preserve the states of the system and those that disturb the states. The principle is derived by alternately applying a fundamental property of classical signals and a fundamental property of quantum ones. The principle can be cast into a simple form by using a decomposition of the relevant Hilbert space, which is uniquely determined by the set of possible states. The decomposition implies the classification of the degrees of freedom of the system into three parts depending on how they store the information on the initially chosen state: one storing it classically, one storing it nonclassically, and the other one storing no information. Then the principle states that the nonclassical part is inaccessible and the classical part is read-only if we are to preserve the state of the system. From this principle, many types of no-cloning, no-broadcasting, and no-imprinting conditions can easily be derived in general forms including mixed states. It also gives a unified view on how various schemes of quantum cryptography work. The principle helps one to derive optimum amount of resources (bits, qubits, and ebits) required in data compression or in quantum teleportation of mixed-state ensembles.

DOI: 10.1103/PhysRevA.66.022318 PACS number(s): 03.67.Dd, 03.65.Ta, 89.70.+c

I. INTRODUCTION

Quantum mechanics pose fundamental restrictions when one reads out information from a quantum system. The most basic rule is well known—if one reads out information from a quantum system in an unknown initial state, the quantum state of the system will change [1]. Recent development of quantum information theory proposes various schemes of handling information through quantum systems, and understanding of more detailed rules seems to become an important issue. One particular direction of such investigation is the cases when the initial state is partially known [2–5]. In such situations, some operations can be done without introducing any disturbance in the original quantum system. One of the fundamental questions here is the following: What kind of information can be extracted, and what cannot be, without changing the state? This problem is important in quantum cryptography, since the initial state is chosen by the sender among a few definite states. The problem is also directly related to the physical feasibility of cloning (making a copy of the original) and imprinting (catching a trail without affecting the original) of partially known quantum states. So far, the conditions for the initial states allowing such tasks were derived, such as broadcasting of mixed states [4] and cloning of pure entangled states [5]. The proofs were based on the complicated series of inequalities related to the fidelity, and it is not always easy to infer the conditions even for slightly different tasks.

In this paper, we present a principle that gives a definite distinction between what one can do and what one cannot do without changing given states of a system. Given a set of possible initial states, we propose a particular decomposition [Eq. (86)] of the system, which classifies the degrees of freedom of the system into three parts, based on how they hold the information on which one of the states is chosen as the initial state. The principle is then stated as the restriction to the access to each part. We provide a proof that clarifies the physical origin of the principle—it is obtained by simply applying two fundamental theorems alternately, which respectively, reflect the basic property of classical signals (Theorem 1) and that of quantum signals (Theorem 2). This principle can be applied to various problems of cloning and imprinting of quantum states, and reveals conditions for feasibility of various tasks, such as no-imprinting condition of mixed states. It also gives a good insight into the basic concepts of quantum cryptography, and helps us to solve problems related to quantum data compression and quantum teleportation. Note that our approach takes just the opposite direction to the one by Lindblad [6], where the latter answers what are the states that are invariant under given operations.

This paper is organized as follows. In Sec. II, we formulate the problem considered in this paper. In Sec. III, we derive two theorems that reflect the basic property of classical signals and that of quantum signals. The latter one suggests a structure of Hilbert space in which tensor products and direct sums are involved, and we discuss notations to treat such structures in Sec. IV. In Sec. V, we repeatedly use the two basic theorems and derive the main result, the property of the operations preserving a set of states. Section VI discusses properties of the decomposition used in stating the main theorem, such as its uniqueness and relation to the well-known mathematical concepts. In Sec. VII, the main theorem is restated in a scenario of faithful transfer, which makes it convenient to apply the theorem to communication problems. In Sec. VIII, we give applications of the theorem to various problems of cloning, imprinting, quantum cryptography, quantum data compression, and teleportation.

II. FORMULATION OF THE PROBLEM

The main problem considered in this paper is described as follows. Consider a quantum system A, which is described by a Hilbert space $\mathcal{H}'_A$. Initially system A is secretly prepared in a state described by a normalized density operator ρ_s, one in the known set of states $\{\rho_s\}_{s\in S}$. Here S is the set of possible values of index s. For example, if the initial state is chosen from n states, S is assumed be $\{1,2,...,n\}$. S can also be an infinite set. We assume that $\{\rho_s\}_{s\in S}$ is supported by a subspace with a finite dimension. This assumption is more precisely stated as follows. Let us write the support of ρ_s as $\mathrm{supp}(\rho_s)$, and define

$$\mathcal{H}_A \equiv \bigcup_{s\in S} \mathrm{supp}(\rho_s). \tag{1}$$

Then, the said assumption is that the dimension of $\mathcal{H}_A$ is finite.

Next, we prepare an ancilla (an auxiliary system) E, described by a Hilbert space $\mathcal{H}_E$, in a standard quantum state $\Sigma_E = |u\rangle_E\langle u|$, and apply a unitary operation U on $\mathcal{H}'_A \otimes \mathcal{H}_E$. After this operation, the marginal density operator of $\mathcal{H}'_A$ becomes

$$\mathcal{T}_U(\rho_s) \equiv \mathrm{Tr}_E[U(\rho_s \otimes \Sigma_E)U^\dagger]. \tag{2}$$

What we seek is the requirement for U to preserve the marginal density operator of A, namely, $\mathcal{T}_U(\rho_s)=\rho_s$ for all $s \in S$. Note that what we concern here is not the whole property of $U:\mathcal{H}'_A\otimes\mathcal{H}_E \to \mathcal{H}'_A\otimes\mathcal{H}_E$, but that of the isometry given as its restriction, $U:\mathcal{H}_A\otimes|u\rangle_E \to \mathcal{H}'_A\otimes\mathcal{H}_E$. Let $\mathcal{U}_{\mathrm{all}}$ be the set of all isometries from $\mathcal{H}_A\otimes|u\rangle_E$ to $\mathcal{H}'_A\otimes\mathcal{H}_E$. The problem here is thus to identify the subset

$$\mathcal{U}_{ND} \equiv \{U \in \mathcal{U}_{\mathrm{all}} | \mathcal{T}_U(\rho_s)=\rho_s, \quad {}^\forall s\in S\}. \tag{3}$$

It is convenient to construct a density operator ρ_{all} from $\{\rho_s\}_{s\in S}$, satisfying the following conditions:

$$\mathrm{Tr}(\rho_{\mathrm{all}})=1, \tag{4}$$

$$\mathcal{T}_U(\rho_{\mathrm{all}})=\rho_{\mathrm{all}}, \quad {}^\forall U\in\mathcal{U}_{ND}, \tag{5}$$

and

$$\mathrm{supp}(\rho_{\mathrm{all}})=\mathcal{H}_A. \tag{6}$$

When a probability distribution $p(s)(s\in S)$ over S satisfying $p(s)>0$ for all $s\in S$ is assigned to the set $\{\rho_s\}_{s\in S}$, ρ_{all} can be constructed as an averaged state, namely, by a sum $\rho_{\mathrm{all}} = \Sigma_{s\in S} p(s)\rho_s$, or by an integral $\rho_{\mathrm{all}} = \int ds\, p(s)\rho_s$. Alternatively, we can always pick up $n(\leqslant \dim \mathcal{H}_A)$ states $\{\rho_1,\rho_2,\ldots,\rho_n\}$ from the set $\{\rho_s\}_{s\in S}$ such that $\mathrm{supp}(\Sigma_{i=1}^n \rho_i) = \mathcal{H}_A$. Then, setting $\rho_{\mathrm{all}} = \Sigma_{i=1}^n \rho_i/n$ satisfies Eqs. (4)–(6).

III. BASIC PROPERTY OF CLASSICAL AND QUANTUM SIGNALS

A. Useful lemmas

In this section, we introduce two lemmas that will be frequently used in this paper.

Lemma 1. Let O be a Hermitian operator acting on $\mathcal{H}$, and U be an unitary operator on $\mathcal{H}\otimes\mathcal{H}_E$ (or an isometry from $\mathcal{H}\otimes|u\rangle_E$ to $\mathcal{H}\otimes\mathcal{H}_E$) satisfying $\mathcal{T}_U(O)=O$. Then,

$$[P_+\otimes \mathbf{1}_E, U](P_+\otimes\Sigma_E)=\mathbf{0}, \tag{7}$$

where P_+ is the projection onto the space spanned by the eigenvectors of O with positive eigenvalues.

This lemma implies that an operation preserving a Hermitian operator O does not transfer the eigenvectors of O with positive eigenvalues to the space for nonpositive eigenvalues. A proof is given as follows. Let us define $\overline{P}_+ \equiv \mathbf{1}-P_+$. The operator O can be decomposed as $O=O_+-O_-$ by a positive definite operator $O_+\equiv P_+O$ and a positive semidefinite operator $O_-\equiv -\overline{P}_+O$. Since $\mathcal{T}_U$ is linear,

$$\begin{aligned}\mathrm{Tr}[P_+\mathcal{T}_U(O)] &= \mathrm{Tr}[P_+\mathcal{T}_U(O_+)] - \mathrm{Tr}[P_+\mathcal{T}_U(O_-)]\\ &= \mathrm{Tr}[\mathcal{T}_U(O_+)] - \mathrm{Tr}[\overline{P}_+\mathcal{T}_U(O_+)]\\ &\quad - \mathrm{Tr}[P_+\mathcal{T}_U(O_-)].\end{aligned} \tag{8}$$

From $\mathcal{T}_U(O)=O$, we have

$$\mathrm{Tr}[P_+\mathcal{T}_U(O)] = \mathrm{Tr}[P_+O] = \mathrm{Tr}[O_+]. \tag{9}$$

On the other hand, since $\mathcal{T}_U$ is a trace-preserving map, we have

$$\mathrm{Tr}[\mathcal{T}_U(O_+)] = \mathrm{Tr}[O_+]. \tag{10}$$

Combining Eqs. (8)–(10), we obtain

$$\mathrm{Tr}[\overline{P}_+\mathcal{T}_U(O_+)] + \mathrm{Tr}[P_+\mathcal{T}_U(O_-)] = 0. \tag{11}$$

Since $\mathcal{T}_U$ is a complete positive map, $\mathrm{Tr}[\overline{P}_+\mathcal{T}_U(O_+)]\geqslant 0$ and $\mathrm{Tr}[P_+\mathcal{T}_U(O_-)]\geqslant 0$. This means that both terms in the left-hand side (lhs) of Eq. (11) are non-negative, and we obtain $\mathrm{Tr}[\overline{P}_+\mathcal{T}_U(O_+)]=0$. This relation is also written as $\mathrm{Tr}[QQ^\dagger]=0$ with $Q=(\overline{P}_+\otimes 1_E)U(\sqrt{O_+}\otimes\Sigma_E)$. This means $Q=\mathbf{0}$, or equivalently,

$$(\overline{P}_+\otimes\mathbf{1}_E)U(P_+\otimes\Sigma_E)=\mathbf{0}. \tag{12}$$

Substituting $\overline{P}_+=\mathbf{1}-P_+$ completes the proof of Lemma 1.

Lemma 2. Let ρ be a positive semidefinite operator acting on $\mathcal{H}$. Suppose that its support $\mathrm{supp}(\rho)$ is written as a direct sum of two subspaces as $\mathrm{supp}(\rho)=\mathcal{H}_1\oplus\mathcal{H}_2$, and let P_i be the projection onto $\mathcal{H}_i (i=1, 2)$. *Let* U be an unitary operator on $\mathcal{H}\otimes\mathcal{H}_E$ (or an isometry from $\mathcal{H}\otimes|u\rangle_E$ to $\mathcal{H}\otimes\mathcal{H}_E$) satisfying $\mathcal{T}_U(\rho)=\rho$ and $[P_1\otimes\mathbf{1}_E, U](P_1\otimes\Sigma_E)=\mathbf{0}$. Then

$$[P_2\otimes\mathbf{1}_E, U](P_2\otimes\Sigma_E)=\mathbf{0}. \tag{13}$$

This lemma implies that if U does not transfer the vectors in subspace $\mathcal{H}_1$ to subspace $\mathcal{H}_2$, U does not include the transfer in the opposite way ($\mathcal{H}_2$ to $\mathcal{H}_1$). Lemma 2 is proved as follows. The assumption $[P_1\otimes\mathbf{1}_E, U](P_1\otimes\Sigma_E)=\mathbf{0}$ implies that $(P_2\otimes\mathbf{1}_E)U(P_1\otimes\Sigma_E)=\mathbf{0}$. Using this, we have

$$\begin{aligned}\mathrm{Tr}[P_2\mathcal{T}_U(\rho)] &= \mathrm{Tr}\{P_2\mathcal{T}_U[(P_1+P_2)\rho(P_1+P_2)]\}\\ &= \mathrm{Tr}[P_2\mathcal{T}_U(P_2\rho P_2)].\end{aligned} \tag{14}$$

From $\mathcal{T}_U(\rho)=\rho$, we have

$$\mathrm{Tr}[P_2\mathcal{T}_U(\rho)]=\mathrm{Tr}[P_2\rho]. \tag{15}$$

Since $\mathcal{T}_U$ is a trace-preserving map,

$$\mathrm{Tr}[\mathcal{T}_U(P_2\rho P_2)]=\mathrm{Tr}[P_2\rho]. \tag{16}$$

Combining Eqs. (14)–(16), we obtain $\mathrm{Tr}[\mathcal{T}_U(P_2\rho P_2)]=\mathrm{Tr}[P_2\mathcal{T}_U(P_2\rho P_2)]$, or equivalently, $\mathrm{Tr}[\overline{P_2}\mathcal{T}_U(P_2\rho P_2)]=\mathbf{0}$ with $\overline{P_2}\equiv\mathbf{1}-P_2$. This relation is also written as $\mathrm{Tr}[QQ^\dagger]=0$ with $Q=(\overline{P_2}\otimes\mathbf{1}_E)U(\sqrt{P_2\rho P_2}\otimes\Sigma_E)$. This means $Q=\mathbf{0}$, or equivalently,

$$(\overline{P_2}\otimes\mathbf{1}_E)U(P_2\otimes\Sigma_E)=\mathbf{0}. \tag{17}$$

Substituting $\overline{P_2}=\mathbf{1}-P_2$ completes the proof of Lemma 2.

B. Property of classical signals

In this section, we derive a theorem that stems from a general property of classical signals. Before the derivation of the theorem, it is instructive to consider an example in the purely classical situation. A classical counterpart of the problem considered here is obtained by replacing the requirement of preserving density operators by that of preserving probability distributions. Consider a purely classical example in which a signal X is drawn from either of the two probability distributions $p_1(x)$ and $p_2(x)$, according to the value of $s(=1,2)$, and a signal $\tilde{X}$ is then produced from the value of X according to a rule that is independent of the value of s. Namely, if $X=x$, $\tilde{X}$ is set to $\tilde{X}=y$ with probability $p(y|x)$. The probability distribution for $\tilde{X}$ is then given by $\tilde{p}_s(x)=\Sigma_{x'}p(x|x')p_s(x')$. Let $K_0=\{x|p_1(x)+p_2(x)>0\}$ be the set of the possible values of X. Let us divide K_0 into two sets, $K_a\equiv\{x|p_1(x)>p_2(x)\}$ and $K_b\equiv\{x|p_2(x)\geqslant p_1(x),p_2(x)>0\}$. A necessary condition for the transition matrix $p(y|x)$ in order that $\tilde{p}_s(x)$ coincides with $p_s(x)$ for either value of s is that the transition must be made within each of the two sets K_a and K_b, which is proved as follows.

Let us define $p^{(s)}(Z\in K)\equiv\Sigma_{x\in K}\mathrm{Prob}\{Z=x\}(Z=X,\tilde{X},K=K_a,K_b)$ as the probability that the value of Z belongs to K. Consider quantities $d_a(X)\equiv p^{(1)}(X\in K_a)-p^{(2)}(X\in K_a)$ and $p_b(X)\equiv p^{(1)}(X\in K_b)+p^{(2)}(X\in K_b)$, and their changes in the transition $p(y|x)$, namely, $\Delta d_a\equiv d_a(\tilde{X})-d_a(X)$ and $\Delta p_b\equiv p_b(\tilde{X})-p_b(X)$. In order for $\tilde{p}_s(x)=p_s(x)$, these changes must be zero. These changes are caused by the transition from K_a to K_b or vice versa, and Δd_a is written as the sum of two nonpositive parts,

$$\Delta d_a=-\sum_{y\in K_b}\sum_{x\in K_a}p(y|x)[p_1(x)-p_2(x)]$$
$$-\sum_{y\in K_a}\sum_{x\in K_b}p(y|x)[p_2(x)-p_1(x)]. \tag{18}$$

In order to satisfy $\Delta d_a=0$, either part must be zero. Since $p_1(x)-p_2(x)>0$ in the first part, $p(y|x)$ with $y\in K_b$ and $x\in K_a$ must vanish. Under this condition, Δp_b is contributed only by the transition from K_b to K_a, and is given by

$$\Delta p_b=-\sum_{y\in K_a}\sum_{x\in K_b}p(y|x)[p_1(x)+p_2(x)]. \tag{19}$$

Since $p_1(x)+p_2(x)>0$, $p(y|x)$ with $y\in K_a$ and $x\in K_b$ must also vanish in order to satisfy $\Delta p_b=0$. Hence, preserving $p_1(x)$ and $p_2(x)$ requires that for any $y\in K_b$ and $x\in K_a$, $p(y|x)$ and $p(x|y)$ should vanish. The transition must be made within each of the two sets K_a and K_b.

This argument almost directly applies to the quantum case, that is, we can show that any operation that preserves two different density operators ρ and ρ', must act on two subspaces independently. In order to represent this property in a simple form, we write the set of all isometries from $\mathcal{H}\otimes|u\rangle_E$ to $\mathcal{H}\otimes\mathcal{H}_E$ as $\mathcal{U}(\mathcal{H})$, where $\mathcal{H}$ is an arbitrary subspace. Then, the property is described by the following theorem.

Theorem 1. Let ρ and ρ' be two density operators for different states. Let $\mathcal{H}$ be the support of $\rho+\rho'$, and take the decomposition $\mathcal{H}=\mathcal{H}_1\oplus\mathcal{H}_2$ where $\mathcal{H}_1$ is the space spanned by the eigenvectors of $O\equiv\rho/\mathrm{Tr}(\rho)-\rho'/\mathrm{Tr}(\rho')$ with positive eigenvalues. Then, $\mathcal{H}_1$ and $\mathcal{H}_2$ are nonzero subspaces, and any $U\in\mathcal{U}(\mathcal{H})$ that satisfies $\mathcal{T}_U(\rho)=\rho$ and $\mathcal{T}_U(\rho')=\rho'$ can be written as $U=U_1\oplus U_2$ with $U_i\in\mathcal{U}(\mathcal{H}_i)$ $(i=1,2)$.

For later convenience, the theorem allows for the possibility that ρ and ρ' are un-normalized. Theorem 1 is proved as follows. Since ρ and ρ' represent different states, O is nonzero. The form of O implies that O is a traceless Hermitian operator. Hence O has positive and negative eigenvalues, and $\mathcal{H}_1$ and $\mathcal{H}_2$ are nonzero spaces. Next, suppose that $U\in\mathcal{U}(\mathcal{H})$ satisfies $\mathcal{T}_U(\rho)=\rho$ and $\mathcal{T}_U(\rho')=\rho'$. Let P_i be the projection onto $\mathcal{H}_i$ $(i=1,2)$. Since $\mathcal{T}_U$ is linear, $\mathcal{T}_U(O)=O$ and $\mathcal{T}_U(\rho+\rho')=\rho+\rho'$. From $\mathcal{T}_U(O)=O$, Lemma 1 leads to

$$[P_1\otimes\mathbf{1}_E,U](P_1\otimes\Sigma_E)=\mathbf{0}. \tag{20}$$

This relation and $\mathcal{T}_U(\rho+\rho')=\rho+\rho'$ fulfill the requisite of Lemma 2 (with ρ replaced by $\rho+\rho'$), and we obtain

$$[P_2\otimes\mathbf{1}_E,U](P_2\otimes\Sigma_E)=\mathbf{0}. \tag{21}$$

Using Eqs. (20) and (21), we have $U=U(P_1\otimes\Sigma_E)+U(P_2\otimes\Sigma_E)=\Sigma_{i=1,2}(P_i\otimes\mathbf{1}_E)U(P_i\otimes\Sigma_E)$. This implies that U is written as $U=U_1\oplus U_2$ with $U_i\in\mathcal{U}(\mathcal{H}_i)$ $(i=1,2)$.

Now let us turn back to the classical example of preserving $p_1(x)$ and $p_2(x)$. We have seen that the transition $p(y|x)$ must occur within the sets K_a and K_b independently. We can then consider each set separately. For example, let us consider the conditional probability distributions for $x\in K_a$, namely, $p_s(x|x\in K_a)\equiv p_s(x)/\Sigma_{x\in K_a}p_s(x)$ $(s=1,2)$. The operation of $p(y|x)$ on the set K_a should preserve these two probability distributions. Then, if $p_1(x|x\in K_a)$ and $p_2(x|x\in K_a)$ are different, the above argument can be applied again, namely, K_a is separated into two subsets, within which the transition $p(y|x)$ should occur independently. These new sets and K_b may be further separated into smaller ones by repeating similar procedures. This refinement continues and should finally stop, as long as the set of all possible values (K_0) is a finite set. In order to identify the final form of the refinement, let us introduce the functions $f_s(x) \equiv p_s(x)/\Sigma_s p_s(x)$. In a refinement process in which a subset Y is divided into two subsets, the criteria of this division is whether $p_1(x|x\in Y) - p_2(x|x\in Y)$ is positive or not. This function can be written in the form $[\alpha_1 f_1(x) - \alpha_2 f_2(x)]\Sigma_s p_s(x)$. Hence any two elements x and x' that satisfy $f_s(x) = f_s(x')$ for all s are always classified into the same subset. If we write the final form as $K = \cup_l K^{(l)}$ with $K^{(l)} \cap K^{(l')} = \emptyset$ for $l \neq l'$, $p_1(x|x\in K^{(l)})$ and $p_2(x|x\in K^{(l)})$ should be identical for each subset $K^{(l)}$, since otherwise a further refinement would be possible. This condition means that $f_s(x) = f_s(x')$ for all s and for any x, $x' \in K^{(l)}$. Therefore, the final form is the classification of the elements x according to the set of values (a vector indexed by s) $\{f_s(x)\}$, and hence it is unique. This statement also holds for the cases when more than two probability distributions are preserved.

In quantum cases, we can similarly conduct the refinement of the decomposition of the Hilbert space into a direct sum of subspaces by repeated uses of Theorem 1. The final form of the decomposition, however, is not unique in contrast to the classical cases. One reason for this difference is that the preservation of quantum states requires another type of conditions, which will be described in the following section.

C. Property of quantum signals

In this section, we describe another basic theorem that applies when a state ρ is preserved by an operation that affects two subspaces, $\mathcal{H}_1$ and $\mathcal{H}_2$, independently. In order to preserve the off-diagonal part $P_2\rho P_1$, the operation on $\mathcal{H}_1$ and that on $\mathcal{H}_2$ must satisfy a kind of "similarity." This requirement is stated in the form of the following theorem.

Theorem 2. Let P_1 and P_2 be the projections onto orthogonal subspaces $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Let ρ be a density operator whose support is $\mathcal{H}_1 \oplus \mathcal{H}_2$. Suppose that $P_2\rho P_1 \neq \mathbf{0}$. Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be the support and the image of $P_2\rho P_1$, respectively, and $\mathcal{K}_i^\perp \equiv \mathcal{H}_i - \mathcal{K}_i$ $(i=1,2)$. Take the polar decomposition $P_2\rho P_1 = WN$, where N is a positive operator on $\mathcal{K}_1$ and W is a unitary operator from $\mathcal{K}_1$ to $\mathcal{K}_2$. Then, any pair of $U_i \in \mathcal{U}(\mathcal{H}_i)$ $(i=1,2)$ that satisfies $\mathcal{T}_{U_1\oplus U_2}(\rho) = \rho$ can be written as $U_i = V_i \oplus \tilde{V}_i$, where $V_i \in \mathcal{U}(\mathcal{K}_i)$, $\tilde{V}_i \in \mathcal{U}(\mathcal{K}_i^\perp)$, and

$$V_2 = (W \otimes \mathbf{1}_E) V_1 (W^\dagger \otimes \Sigma_E). \tag{22}$$

An intuitive explanation for this theorem is as follows. The polar decomposition of $P_2\rho P_1$ means that it is written as $P_2\rho P_1 = \Sigma_k a_k |k\rangle_2\, {}_1\langle k|$, where a_k are positive numbers, and $\{|k\rangle_i\}$ is a basis of $\mathcal{K}_i$ $(i=1,2)$. This implies that the coherence in ρ is held in the pair $(|k\rangle_1, |k\rangle_2)$. In order to retain this coherence, the operation $\mathcal{T}_{U_1\oplus U_2}$ should not change this pairing relation, namely, if the operation V_1 on $\mathcal{K}_1$ changes $|k\rangle_1$ to $|k'\rangle_1$, the operation V_2 on $\mathcal{K}_2$ should also change $|k\rangle_2$ to $|k'\rangle_2$. In addition, the change in the ancilla system E caused by the operation V_1 must be identical to that by V_2 in order to avoid decoherence in the marginal state for $\mathcal{H}_1 \oplus \mathcal{H}_2$. Therefore, V_1 and V_2 must operate on $\mathcal{K}_1 \otimes \mathcal{H}_E$ and $\mathcal{K}_2 \otimes \mathcal{H}_E$ identically under the isomorphism W, which is implied by Eq. (22).

Theorem 2 is proved as follows. Let us regard N and W as operators from $\mathcal{H}_{12} \equiv \mathcal{H}_1 \oplus \mathcal{H}_2$ to $\mathcal{H}_{12}$ by extending the domain and the range. Note that $N:\mathcal{H}_{12} \to \mathcal{H}_{12}$ is a positive semidefinite operator with its support $\mathcal{K}_1$ and its image $\mathcal{K}_1$, and $W:\mathcal{H}_{12} \to \mathcal{H}_{12}$ is a partial isometry with its support $\mathcal{K}_1$ and its image $\mathcal{K}_2$. The operator W satisfies $W^2 = \mathbf{0}$, $W^\dagger W$ is the projection onto $\mathcal{K}_1$, and $WW^\dagger$ is the projection onto $\mathcal{K}_2$. Let us define

$$P_\pm \equiv [W^\dagger W + WW^\dagger \pm (W + W^\dagger)]/2. \tag{23}$$

These two operators are orthogonal projections since we can easily obtain $P_\pm^2 = P_\pm$ and $P_+ P_- = \mathbf{0}$. Note that $P_+ + P_-$ is the projection onto $\mathcal{K}_1 \oplus \mathcal{K}_2$. Using these projections, define

$$O \equiv 4(P_+ \sqrt{N} P_+)^2 - 4(P_- \sqrt{N} P_-)^2. \tag{24}$$

Substituting Eq. (23) and using relations such as $W^2 = NW = \mathbf{0}$ and $W^\dagger W \sqrt{N} = \sqrt{N}$, we obtain $O = WN + NW^\dagger = P_2\rho P_1 + P_1\rho P_2$. Since $O^2 = WN^2W^\dagger + N^2$, the support of O is $\mathcal{K}_1 \oplus \mathcal{K}_2$. Let us suppose that $U_1 \in \mathcal{U}(\mathcal{H}_1)$ and $U_2 \in \mathcal{U}(\mathcal{H}_2)$ satisfy $\mathcal{T}_{U_1\oplus U_2}(\rho) = \rho$. Noting that

$$[P_i \otimes \mathbf{1}_E, U_1 \oplus U_2](P_i \otimes \Sigma_E) = \mathbf{0} \quad (i=1,2), \tag{25}$$

we have

$$\mathcal{T}_{U_1\oplus U_2}(P_i\rho P_j) = P_i \mathcal{T}_{U_1\oplus U_2}(\rho) P_j = P_i\rho P_j \tag{26}$$

for any $i=1$, 2 and $j=1$, 2. From this relation, we have $\mathcal{T}_{U_1\oplus U_2}(O) = O$. The form of Eq. (24), together with the fact that the support of O coincides with the support of $P_+ + P_-$, means that P_+ is the projection onto the space spanned by the eigenvectors of O with positive eigenvalues. Then, using Lemma 1, we obtain

$$[P_+ \otimes \mathbf{1}_E, U_1 \oplus U_2](P_+ \otimes \Sigma_E) = \mathbf{0}. \tag{27}$$

Similarly, noting that $\mathcal{T}_{U_1\oplus U_2}(-O) = -O$ and that P_- is the projection onto the space spanned by the eigenvectors of $-O$ with positive eigenvalues, we have

$$[P_- \otimes \mathbf{1}_E, U_1 \oplus U_2](P_- \otimes \Sigma_E) = \mathbf{0}. \tag{28}$$

Combining Eqs. (27) and (28) with $W^\dagger W + WW^\dagger = P_+ + P_-$, we obtain $[(W^\dagger W + WW^\dagger)\otimes \mathbf{1}_E, U_1 \oplus U_2][(W^\dagger W + WW^\dagger)\otimes \Sigma_E] = \mathbf{0}$, or equivalently,

$$[W^\dagger W \otimes \mathbf{1}_E, U_1](W^\dagger W \otimes \Sigma_E) = \mathbf{0} \tag{29}$$

and

$$[WW^\dagger \otimes \mathbf{1}_E, U_2](WW^\dagger \otimes \Sigma_E) = \mathbf{0}. \tag{30}$$

From Eq. (26), we have $\mathcal{T}_{U_1\oplus U_2}(P_1\rho P_1)=\mathcal{T}_{U_1}(P_1\rho P_1)=P_1\rho P_1$. Applying this and Eq. (29) to Lemma 2 (note that the support of $P_1\rho P_1$ is $\mathcal{H}_1=\mathcal{K}_1\oplus\mathcal{K}_1^{\perp}$), we obtain

$$[(P_1-W^{\dagger}W)\otimes\mathbf{1}_E, U_1][(P_1-W^{\dagger}W)\otimes\Sigma_E]=\mathbf{0}. \tag{31}$$

Equations (29) and (31) imply that U_1 can be written as $U_1=V_1\oplus\tilde{V}_1$, where $V_1\in\mathcal{U}(\mathcal{K}_1)$ and $\tilde{V}_1\in\mathcal{U}(\mathcal{K}_1^{\perp})$ are related to U_1 as $V_1=U_1|\mathcal{K}_1$ and $\tilde{V}_1=U_1|\mathcal{K}_1^{\perp}$. The same argument applies to Eq. (30), leading to the conclusion that U_2 can be written as $U_2=V_2\oplus\tilde{V}_2$, where $V_2\in\mathcal{U}(\mathcal{K}_2)$ and $\tilde{V}_2\in\mathcal{U}(\mathcal{K}_2^{\perp})$ are related to U_2 as $V_2=U_2|\mathcal{K}_2$ and $\tilde{V}_2=U_2|\mathcal{K}_2^{\perp}$. Finally, combining Eqs. (27) and (28) with $W+W^{\dagger}=P_+-P_-$, we obtain $[(W+W^{\dagger})\otimes\mathbf{1}_E, U_1\oplus U_2][(W+W^{\dagger})\otimes\Sigma_E]=\mathbf{0}$. Expanding this leads to

$$(W\otimes\mathbf{1}_E)U_1(W^{\dagger}\otimes\Sigma_E)+(W^{\dagger}\otimes\mathbf{1}_E)U_2(W\otimes\Sigma_E)-U_1(W^{\dagger}W\otimes\Sigma_E)-U_2(WW^{\dagger}\otimes\Sigma_E)=\mathbf{0}. \tag{32}$$

Applying $P_2\otimes\mathbf{1}_E$ from the right (and restricting the domain to $\mathcal{K}_2$), we obtain Eq. (22), which completes the proof.

IV. STRUCTURE OF HILBERT SPACE

The requirement coming from Theorem 2 introduces a structure in the Hilbert space, which is more complicated than a direct-sum decomposition into subspaces, namely, some of the subspaces (e.g., $\mathcal{K}_1$ and $\mathcal{K}_2$) are isometrically isomorphic through unitary operators (e.g., W) connecting them. To handle such a structure in general, we introduce a way of decomposing a Hilbert space $\mathcal{H}$ as follows. First, $\mathcal{H}$ is decomposed to a direct sum of its orthogonal subspaces $\mathcal{H}^{(1)}$, $\mathcal{H}^{(2)},\ldots,\mathcal{H}^{(l_{\max})}$, namely,

$$\mathcal{H}=\bigoplus_{l=1}^{l_{\max}}\mathcal{H}^{(l)}. \tag{33}$$

The size of each subspace is arbitrary. Then, each subspace $\mathcal{H}^{(l)}$ is further decomposed to a direct sum of its orthogonal subspaces $\mathcal{H}_1^{(l)}$, $\mathcal{H}_2^{(l)},\ldots,\mathcal{H}_{j_{\max}^{(l)}}^{(l)}$, namely,

$$\mathcal{H}^{(l)}=\bigoplus_{j=1}^{j_{\max}^{(l)}}\mathcal{H}_j^{(l)}. \tag{34}$$

Here the subspaces $\{\mathcal{H}_j^{(l)}\}$ $(j=1,2,...,j_{\max}^{(l)})$ are of the same size, and an isometrically isomorphic relation is defined among them through a set of unitary operators $\{W_{j'j}^{(l)}:\mathcal{H}_j^{(l)}\rightarrow\mathcal{H}_{j'}^{(l)}\}$ satisfying $W_{kj}^{(l)}W_{ji}^{(l)}=W_{ki}^{(l)}$. The numbers $l_{\max}$ and $j_{\max}^{(l)}$ should satisfy

$$\dim\ \mathcal{H}=\sum_{l=1}^{l_{\max}} j_{\max}^{(l)}\dim\ \mathcal{H}_1^{(l)}. \tag{35}$$

The above decomposition can be completely specified by a set of partial isometries $\{W_{j'j}^{(l)}\}$ acting on $\mathcal{H}$ satisfying the following three conditions:

$$W_{j'j}^{(l)\dagger}=W_{jj'}^{(l)}, \tag{36}$$

$$W_{j'i'}^{(l')}W_{ij}^{(l)}=\delta_{l,l'}\delta_{i,i'}W_{j'j}^{(l)}, \tag{37}$$

and

$$\sum_{l=1}^{l_{\max}}\sum_{j=1}^{j_{\max}^{(l)}} W_{jj}^{(l)}=\mathbf{1}, \tag{38}$$

where $\mathbf{1}$ is the projection onto $\mathcal{H}$. Given such $\{W_{j'j}^{(l)}\}$, we can determine $\{\mathcal{H}_j^{(l)}\}$ as follows. From Eq. (37), we have $W_{j'j'}^{(l')}W_{jj}^{(l)}=\delta_{l,l'}\delta_{j,j'}W_{jj}^{(l)}$. This means that $\{W_{jj}^{(l)}\}$ are projection operators orthogonal to each other. If we take $\mathcal{H}_j^{(l)}$ as the support of $W_{jj}^{(l)}$, Eq. (38) assures that Eqs. (33) and (34) are satisfied. For $j\neq j'$, the relation $W_{j'j}^{(l)\dagger}W_{j'j}^{(l)}=W_{jj}^{(l)}$ and $W_{j'j}^{(l)}W_{j'j}^{(l)\dagger}=W_{j'j'}^{(l)}$, resulting from Eqs. (36) and (37) means that the support and the image of $W_{j'j}^{(l)}$ are $\mathcal{H}_j^{(l)}$ and $\mathcal{H}_{j'}^{(l)}$, respectively. The map $W_{j'j}^{(l)}:\mathcal{H}_j^{(l)}\rightarrow\mathcal{H}_{j'}^{(l)}$ is hence unitary and introduces an isometrically isomorphic relation between $\mathcal{H}_j^{(l)}$ and $\mathcal{H}_{j'}^{(l)}$. The compatibility relation $W_{j'i}^{(l)}W_{ij}^{(l)}=W_{j'j}^{(l)}$ coming from Eq. (37) assures that an isometrically isomorphic relation is defined among $\{\mathcal{H}_j^{(l)}\}$ $(j=1,2,...,j_{\max}^{(l)})$.

The isomorphic relation among $\{\mathcal{H}_j^{(l)}\}$ naturally defines an isomorphism (unitary map) $\Gamma^{(l)}$ from $\mathcal{H}^{(l)}$ to a tensor-product Hilbert space $\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$, where dim $\mathcal{H}_J^{(l)}=j_{\max}^{(l)}$ and dim $\mathcal{H}_K^{(l)}=$ dim $\mathcal{H}_1^{(l)}(=$ dim $\mathcal{H}_2^{(l)}=\cdots)$. The unitary map $\Gamma^{(l)}:\mathcal{H}^{(l)}\rightarrow\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ is defined as follows. Take an arbitrary basis $\{|j\rangle_J^{(l)}\}$ $(j=1,2,...,j_{\max}^{(l)})$ for $\mathcal{H}_J^{(l)}$ and an arbitrary unitary operator $\Gamma_1^{(l)}$ from $\mathcal{H}_1^{(l)}$ to $|1\rangle_J^{(l)}\otimes\mathcal{H}_K^{(l)}$. Then, $\Gamma^{(l)}$ is given by

$$\Gamma^{(l)}=\sum_{j=1}^{j_{\max}^{(l)}}(|j\rangle_J^{(l)}\langle 1|\otimes\mathbf{1}_K^{(l)})\Gamma_1^{(l)}W_{1j}^{(l)}. \tag{39}$$

From $\{\Gamma^{(l)}\}$, we can construct an isomorphism (unitary map) Γ from $\mathcal{H}$ to $\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ as

$$\Gamma=\bigoplus_l\Gamma^{(l)}. \tag{40}$$

Conversely, given a unitary map $\Gamma:\mathcal{H}\rightarrow\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$, we can construct a set of partial isometries $\{W_{j'j}^{(l)}\}$ in $\mathcal{H}$ satisfying Eqs. (36)–(38) as follows. Take an arbitrary basis $\{|j\rangle_J^{(l)}\}$ $(j=1,2,...,j_{\max}^{(l)})$ for $\mathcal{H}_J^{(l)}$. Then, if we set

$$W_{j'j}^{(l)}=\Gamma^{\dagger}(|j'\rangle_J^{(l)}\langle j|\otimes\mathbf{1}_K^{(l)})\Gamma, \tag{41}$$

Eqs. (36)–(38) are apparently satisfied.

In the above construction of $\{W_{j'j}^{(l)}\}$ from Γ, we see that different decompositions, for example, $\{W_{j'j}^{(l)}\}$ and $\{\tilde{W}_{j'j}^{(l)}\}$, can be derived from the same Γ due to the arbitrariness in the choice of basis $\{|j\rangle_J^{(l)}\}$. This implies that the two different sets $\{W_{j'j}^{(l)}\}$ and $\{\tilde{W}_{j'j}^{(l)}\}$ correspond to the same structure in $\mathcal{H}$. The definition of Γ also has similar degeneracy, e.g., changing the order of the index l merely alters the way of representation and does not change the structure itself. It is thus natural to define a *structure* in $\mathcal{H}$ as an equivalence class defined among the sets $\{\tilde{W}_{j'j}^{(l)}\}$ or among the isometries Γ in the following way. Two decompositions specified by $\{W_{j'j}^{(l)}\}$ and $\{\tilde{W}_{j'j}^{(l)}\}$ are equivalent and correspond to the same structure if

$$\tilde{W}_{j'j}^{[P(l)]}=\sum_{i,i'} u_{j'i'}^{(l)} W_{i'i}^{(l)} u_{ji}^{(l)*}, \tag{42}$$

where $P(l)$ is a permutation of the index l and $u_{ij}^{(l)}$ is the (i,j) element of a unitary matrix $u^{(l)}$. Two decompositions specified by $\Gamma:\mathcal{H}\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ and $\tilde{\Gamma}:\mathcal{H}\to\oplus_l\tilde{\mathcal{H}}_J^{(l)}\otimes\tilde{\mathcal{H}}_K^{(l)}$ are equivalent and correspond to the same structure if $\tilde{\Gamma}\Gamma^\dagger$ is written as

$$\tilde{\Gamma}\Gamma^\dagger=\bigoplus_l v_J^{(l)}\otimes v_K^{(l)}, \tag{43}$$

where $v_J^{(l)}$ is a unitary map from $\mathcal{H}_J^{(l)}$ to $\tilde{\mathcal{H}}_J^{[P(l)]}$, and $v_K^{(l)}$ is a unitary map from $\mathcal{H}_K^{(l)}$ to $\tilde{\mathcal{H}}_K^{[P(l)]}$.

The relation among the definitions made so far is summarized as follows. A structure D is specified if a set $\{W_{j'j}^{(l)}\}$ or a map Γ is given. Given a structure D, the set $\{W_{j'j}^{(l)}\}$ and the map Γ are not uniquely determined, and are only determined up to the conditions (42) and (43). The quantity $l_{\max}$ is uniquely determined, and $\{j_{\max}^{(l)}\}$ are unique up to the permutation of the index l.

In the rest of the paper, we represent the isomorphic relation defined from $\Gamma:\mathcal{H}\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ simply by

$$\mathcal{H}=\bigoplus_l \mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}. \tag{44}$$

An operator A acting on $\mathcal{H}$ and an operator A_{JK} acting on $\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ is regarded as the same if

$$A_{JK}=\Gamma A\Gamma^\dagger \tag{45}$$

holds. We also simply write this relation as

$$A_{JK}=A, \tag{46}$$

whenever the identity of Γ is obvious in the context.

V. OPERATION PRESERVING A SET OF STATES

In this section, we give a solution to the problem formulated in Sec. II, namely, we identify the set $\mathcal{U}_{ND}$ given in Eq. (3). We first define a set of isometries $\mathcal{V}(D)$ associated with a structure D in $\mathcal{H}_A$, and define an index $r(D)$ that gives the degree of refinement of D. Then we apply Theorems 1 and 2 repeatedly to refine the structure in $\mathcal{H}_A$, obtaining a series of structures $D_0,D_1,\ldots,D_{\rm fin}$ satisfying $r(D_0)<r(D_1)<\cdots<r(D_{\rm fin})$ and $\mathcal{V}(D_0)\supset\mathcal{V}(D_1)\supset\mathcal{V}(D_{\rm fin})\supset\mathcal{U}_{ND}$. It will be shown that under the final structure $D_{\rm fin}$, the states $\{\rho_s\}$ have a simple form [Eq. (85)], and we can easily identify the set $\mathcal{U}_{ND}$.

We first define a set of isometries $\mathcal{V}(D)$ associated with a structure D in $\mathcal{H}_A$. Let $\mathcal{W}_D=\{W_{j'j}^{(l)}\}$ be a set of isometries that specifies D. With this notation, we define the set $\mathcal{V}(D)$ as

$$\mathcal{V}(D)\equiv\{U\in\mathcal{U}_{\rm all}|{}^\forall W_{j'j}^{(l)}\in\mathcal{W}_D, U(W_{j'j}^{(l)}\otimes\Sigma_E) =(W_{j'j}^{(l)}\otimes\mathbf{1}_E)U\}. \tag{47}$$

This definition is consistent with the arbitrariness in the choice of $\mathcal{W}_D$, namely, $\mathcal{V}(D)$ depends only on D. Let $\Gamma_D:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be the isomorphism determined from $\mathcal{W}_D$ through Eqs. (39) and (40). Under this isomorphism, let O_A be an operator acting on $\mathcal{H}_A$ that is written as

$$O_A=\bigoplus_l O_J^{(l)}\otimes\mathbf{1}_K^{(l)}, \tag{48}$$

where $O_J^{(l)}$ operates on $\mathcal{H}_J^{(l)}$. Using Eq. (41), O_A is written as a linear combination $O_A=\Sigma_l\Sigma_{j,j'}c_{j'j}^{(l)}W_{j'j}^{(l)}$. Hence, $U(O_A\otimes\Sigma_E)=(O_A\otimes\mathbf{1}_E)U$ holds for any $U\in\mathcal{V}(D)$. Since U satisfies this equation for any O_A in the form of Eq. (48), we conclude that any $U\in\mathcal{V}(D)$ can be written in a simple form,

$$U=\bigoplus_l \mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}, \tag{49}$$

where $U_{KE}^{(l)}\in\mathcal{U}(\mathcal{H}_K^{(l)})$. Conversely, any isometry written in the form (49) belongs to $\mathcal{V}(D)$, because any $W_{j'j}^{(l)}$ has a form of O_A in Eq. (48).

Next, we introduce an index $r(D)$ that represents the degree of refinement of the structure D, defined as

$$r(D)\equiv\frac{1}{2}\left(\sum_{l=1}^{l_{\max}} j_{\max}^{(l)}\right)\left(\sum_{l=1}^{l_{\max}} j_{\max}^{(l)}+1\right)-l_{\max}+1. \tag{50}$$

This quantity takes an integer value in the following range:

$$1\leqslant r\leqslant\frac{1}{2}(\dim\mathcal{H}_A)(\dim\mathcal{H}_A+1). \tag{51}$$

This bound ensures that, when $\dim\mathcal{H}_A$ is finite, any procedure of finding a series of structures with increasing degree of refinement will halt within a finite number of steps.

The starting point of the refinement is to show that the trivial structure D_0 in $\mathcal{H}_A$, for which $l_{\max}=1$, and $j_{\max}^{(1)}=1$, satisfies $\mathcal{U}_{ND}\subset\mathcal{V}(D_0)$. Applying $\rho_{\rm all}$ to Lemma 1 and noting Eq. (6), we obtain

$$[\mathbf{1}_A\otimes\mathbf{1}_E,U](\mathbf{1}_A\otimes\Sigma_E)=\mathbf{0} \tag{52}$$

for any isometry $U\in\mathcal{U}_{\rm all}$ that satisfies $\mathcal{T}_U(\rho_{\rm all})=\rho_{\rm all}$. Here $\mathbf{1}_A$ is the projection onto $\mathcal{H}_A$. This equation implies that the image of any $U\in\mathcal{U}_{ND}$ is a subspace of $\mathcal{H}_A\otimes\mathcal{H}_E$, namely,

$\mathcal{U}_{ND}\subset\mathcal{U}(\mathcal{H}_A)$. Since the set $\mathcal{W}_{D_0}$ consists of only one element, $W_{11}^{(1)}=\mathbf{1}_A$, it is obvious from the definition (47) that $\mathcal{U}_{ND}\subset\mathcal{V}(D_0)$.

Next, we state two lemmas to show that applying Theorems 1 and 2 generally advances the refinement.

Lemma 3. Let $\Gamma:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be a unitary map that specifies a structure D. Suppose that $\mathcal{U}_{ND}\subset\mathcal{V}(D)$ and there exist $s\in S$, l', a pure state $|a\rangle\in\mathcal{H}_J^{(l')}$, and a unitary operator V acting on $\mathcal{H}_J^{(l')}$ such that for any $c\geqslant 0$,

$$
\begin{aligned}
&(|a\rangle\langle a|V\otimes\mathbf{1}_K^{(l')})\rho_s(V^\dagger|a\rangle\langle a|\otimes\mathbf{1}_K^{(l')})\\
&\quad\neq c(|a\rangle\langle a|\otimes\mathbf{1}_K^{(l')})\rho_{\mathrm{all}}(|a\rangle\langle a|\otimes\mathbf{1}_K^{(l')}). \qquad (53)
\end{aligned}
$$

Then, there exists a structure $\tilde{D}$ such that $r(\tilde{D})>r(D)$ and $\mathcal{U}_{ND}\subset\mathcal{V}(\tilde{D})$.

For the proof, we actually construct $\tilde{D}$ assuming that $\rho\equiv(|a\rangle\langle a|V\otimes\mathbf{1}_K^{(1)})\rho_s(V^\dagger|a\rangle\langle a|\otimes\mathbf{1}_K^{(1)})$ and $\rho'\equiv(|a\rangle\langle a|\otimes\mathbf{1}_K^{(1)})\rho_{\mathrm{all}}(|a\rangle\langle a|\otimes\mathbf{1}_K^{(1)})$ are different states (here we have assumed that $l'=1$, without loss of generality). Let $\mathcal{H}=|a\rangle\otimes\mathcal{H}_K^{(1)}$. Equation (6) assures that $\mathcal{H}$ is the support of ρ', and hence is the support of $\rho+\rho'$. Then, using Theorem 1, we can find the decomposition $\mathcal{H}=\mathcal{H}_1\oplus\mathcal{H}_2$, where $\mathcal{H}_1$ and $\mathcal{H}_2$ are nonzero subspaces. Next, take a basis $\{|j\rangle_J^{(l)}\}$ $(j=1,2,\ldots,j_{\max}^{(l)})$ for $\mathcal{H}_J^{(l)}$, such that $|1\rangle_J^{(1)}=|a\rangle$, and construct a set $\mathcal{W}=\{W_{j'j}^{(l)}\}$ by using Eq. (41). Let P_1 and P_2 be the projections onto $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, and define a new set $\tilde{\mathcal{W}}=\{\tilde{W}_{j'j}^{(l)}\}$ as follows:

$$\tilde{W}_{j'j}^{(1)}\equiv W_{j'1}^{(1)}P_1W_{1j}^{(1)}, \qquad (54)$$

$$\tilde{W}_{j'j}^{(l_{\max}+1)}\equiv W_{j'1}^{(1)}P_2W_{1j}^{(1)}, \qquad (55)$$

$$\tilde{W}_{j'j}^{(l)}=W_{j'j}^{(l)}, \quad (2\leqslant l\leqslant l_{\max}). \qquad (56)$$

Noting that $P_1+P_2=W_{11}^{(1)}$, we can easily confirm that the conditions (36)–(38) are satisfied by this new set $\tilde{\mathcal{W}}$, and hence $\tilde{\mathcal{W}}$ specifies a structure of $\mathcal{H}_A$. Let us denote this structure by $\tilde{D}$.

The quantities $\tilde{l}_{\max}$ and $\tilde{j}_{\max}^{(l)}$ for $\tilde{\mathcal{W}}$ are related to $l_{\max}$ and $j_{\max}^{(l)}$ for $\mathcal{W}$ as

$$\tilde{l}_{\max}=l_{\max}+1, \qquad (57)$$

$$\tilde{j}_{\max}^{(1)}=\tilde{j}_{\max}^{(l_{\max}+1)}=j_{\max}^{(1)}, \qquad (58)$$

$$\tilde{j}_{\max}^{(l)}=j_{\max}^{(l)} \quad (2\leqslant l\leqslant l_{\max}). \qquad (59)$$

Then, from Eq. (50) and $j_{\max}^{(1)}\geqslant 1$, we have

$$r(\tilde{D})-r(D)=\frac{j_{\max}^{(1)}}{2}\left(2\sum_{l=1}^{l_{\max}}j_{\max}^{(l)}+j_{\max}^{(1)}+1\right)-1\geqslant 1. \qquad (60)$$

Hence $r(\tilde{D})>r(D)$.

Since $\mathcal{U}_{ND}\subset\mathcal{V}(D)$, any $U\in\mathcal{U}_{ND}$ can be written as $U=\oplus_l\mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}$ [Eq. (49)]. From this form and the relations $\mathcal{T}_U(\rho_s)=\rho_s$ and $\mathcal{T}_U(\rho_{\mathrm{all}})=\rho_{\mathrm{all}}$, we have $\mathcal{T}_{U_0}(\rho)=\rho$ and $\mathcal{T}_{U_0}(\rho')=\rho'$, where $U_0\equiv|a\rangle\langle a|\otimes U_{KE}^{(1)}\in\mathcal{U}(\mathcal{H})$. Then, from Theorem 1, U_0 is written as $U_0=U_1\oplus U_2$ with $U_i\in\mathcal{U}(\mathcal{H}_i)$ $(i=1,2)$. This form implies that $U(P_i\otimes\Sigma_E)=U_0(P_i\otimes\Sigma_E)=(P_i\otimes\mathbf{1}_E)U_0=(P_i\otimes\mathbf{1}_E)U$ for $i=1$, 2. Since $U\in\mathcal{V}(D)$, $U(W_{j'j}^{(l)}\otimes\Sigma_E)=(W_{j'j}^{(l)}\otimes\mathbf{1}_E)U$ for any $W_{j'j}^{(l)}\in\mathcal{W}$. Combining these commuting relations and Eqs. (54)–(56), we have

$$U(\tilde{W}_{j'j}^{(l)}\otimes\Sigma_E)=(\tilde{W}_{j'j}^{(l)}\otimes\mathbf{1}_E)U \qquad (61)$$

for any $\tilde{W}_{j'j}^{(l)}\in\tilde{\mathcal{W}}$. Hence $U\in\mathcal{V}(\tilde{D})$, and we obtain $\mathcal{U}_{ND}\subset\mathcal{V}(\tilde{D})$. This completes the proof of Lemma 3.

Lemma 4. Let $\Gamma:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be a unitary map that specifies a structure D. Suppose that $\mathcal{U}_{ND}\subset\mathcal{V}(D)$ and there exist $s\in S$, l', $l''(\neq l')$, a pure state $|a\rangle$ in $\mathcal{H}_J^{(l')}$, and a pure state $|b\rangle$ in $\mathcal{H}_J^{(l'')}$ satisfying the following conditions:

$$\mathrm{supp}[(|a\rangle\langle a|\otimes\mathbf{1}_K^{(l')})\rho_s(|a\rangle\langle a|\otimes\mathbf{1}_K^{(l')})]=|a\rangle\otimes\mathcal{H}_K^{(l')}, \qquad (62)$$

$$\mathrm{supp}[(|b\rangle\langle b|\otimes\mathbf{1}_K^{(l'')})\rho_s(|b\rangle\langle b|\otimes\mathbf{1}_K^{(l'')})]=|b\rangle\otimes\mathcal{H}_K^{(l'')}, \qquad (63)$$

and

$$(|b\rangle\langle b|\otimes\mathbf{1}_K^{(l'')})\rho_s(|a\rangle\langle a|\otimes\mathbf{1}_K^{(l')})\neq\mathbf{0}. \qquad (64)$$

Then, there exists a structure $\tilde{D}$ such that $r(\tilde{D})>r(D)$ and $\mathcal{U}_{ND}\subset\mathcal{V}(\tilde{D})$.

For the proof, we actually construct $\tilde{D}$ assuming that conditions (62)–(64) are satisfied for $l'=1$ and $l''=2$, without loss of generality. Let $\mathcal{H}_1=|a\rangle\otimes\mathcal{H}_K^{(1)}$, $\mathcal{H}_2=|b\rangle\otimes\mathcal{H}_K^{(2)}$, and P_i be the projection onto $\mathcal{H}_i$ $(i=1,2)$. Then, we can apply Theorem 2 by choosing $\rho=(P_1+P_2)\rho_s(P_1+P_2)$, and obtain the decomposition $\mathcal{H}_i=\mathcal{K}_i\oplus\mathcal{K}_i^\perp$ $(i=1,2)$ where $\mathcal{K}_1$ and $\mathcal{K}_2$ are nonzero subspaces, and the unitary operator $W:\mathcal{K}_1\to\mathcal{K}_2$. Without loss of generality, we assume that $\dim\mathcal{K}_1^\perp\geqslant\dim\mathcal{K}_2^\perp$. Note that $\mathcal{K}_i^\perp$ $(i=1,2)$ may be zero. Next, take a basis $\{|j\rangle_J^{(l)}\}$ $(j=1,2,\ldots,j_{\max}^{(l)})$ for $\mathcal{H}_J^{(l)}$ $(l=1,2)$ such that $|1\rangle_J^{(1)}=|a\rangle$ and $|1\rangle_J^{(2)}=|b\rangle$, and construct a set $\mathcal{W}=\{W_{j'j}^{(l)}\}$ by using Eq. (41). Let Q_i and $Q_i^\perp$ be the projections onto $\mathcal{K}_i$ and $\mathcal{K}_i^\perp$ $(i=1,2)$, respectively, and define a new set $\tilde{\mathcal{W}}=\{\tilde{W}_{j'j}^{(l)}\}$ as follows:

$$\tilde{W}_{j'j}^{(1)}\equiv W_{j'1}^{(1)}Q_1W_{1j}^{(1)}, \qquad (65)$$

$$\tilde{W}_{j',\beta+j}^{(1)}\equiv W_{j'1}^{(1)}Q_1W^\dagger Q_2W_{1j}^{(2)}, \qquad (66)$$

$$\tilde{W}_{\beta+j',j}^{(1)}\equiv W_{j'1}^{(2)}Q_2WQ_1W_{1j}^{(1)}, \qquad (67)$$

$$\tilde{W}_{\beta+j',\beta+j}^{(1)}\equiv W_{j'1}^{(2)}Q_2W_{1j}^{(2)}, \qquad (68)$$

$$\tilde{W}^{(l-1)}_{j'j} \equiv W^{(l)}_{j'j} \quad (3 \leqslant l \leqslant l_{\max}), \tag{69}$$

$$\tilde{W}^{(l_{\max})}_{j'j} \equiv W^{(1)}_{j'1} Q_1^{\perp} W^{(1)}_{1j} \quad \text{if } \dim \ \mathcal{K}_1^{\perp} \neq 0, \tag{70}$$

$$\tilde{W}^{(l_{\max}+1)}_{j'j} \equiv W^{(2)}_{j'1} Q_2^{\perp} W^{(2)}_{1j} \quad \text{if } \dim \ \mathcal{K}_2^{\perp} \neq 0, \tag{71}$$

where $\beta \equiv j^{(1)}_{\max}$. Noting that $Q_i + Q_i^{\perp} = W^{(i)}_{11}$ $(i=1,2)$, we can easily confirm that the conditions (36)–(38) are satisfied by this new set $\tilde{\mathcal{W}}$, and hence $\tilde{\mathcal{W}}$ specifies a structure of $\mathcal{H}_A$. Let us denote this structure by $\tilde{D}$.

The quantities $\tilde{l}_{\max}$ and $\tilde{j}^{(l)}_{\max}$ for $\tilde{\mathcal{W}}$ are related to $l_{\max}$ and $j^{(l)}_{\max}$ for $\mathcal{W}$ as

$$\tilde{l}_{\max} = l_{\max} - 1 + s_1 + s_2, \tag{72}$$

$$\tilde{j}^{(1)}_{\max} = j^{(1)}_{\max} + j^{(2)}_{\max}, \tag{73}$$

$$\tilde{j}^{(l-1)}_{\max} = j^{(l)}_{\max} \quad (3 \leqslant l \leqslant l_{\max}), \tag{74}$$

$$\tilde{j}^{(l_{\max})}_{\max} = j^{(1)}_{\max} \quad \text{if } \dim \ \mathcal{K}_1^{\perp} \neq 0, \tag{75}$$

$$\tilde{j}^{(l_{\max}+1)}_{\max} = j^{(2)}_{\max} \quad \text{if } \dim \ \mathcal{K}_2^{\perp} \neq 0, \tag{76}$$

where $s_i = 1$ if $\dim \mathcal{K}_i^{\perp} \neq 0$, and $s_i = 0$ if $\dim \mathcal{K}_i^{\perp} = 0$. Then, from Eq. (50), we have

$$r(\tilde{D}) - r(D) = \frac{s}{2}\left(2\sum_{l=1}^{l_{\max}} j^{(l)}_{\max} + s + 1\right) + 1 - s_1 - s_2, \tag{77}$$

where $s \equiv s_1 j^{(1)}_{\max} + s_2 j^{(2)}_{\max}$. Since $s \geqslant s_1 + s_2 \geqslant 0$, we obtain $r(\tilde{D}) - r(D) \geqslant 1$. Hence $r(\tilde{D}) > r(D)$.

Since $\mathcal{U}_{ND} \subset \mathcal{V}(D)$, any $U \in \mathcal{U}_{ND}$ can be written as $U = \oplus_l \mathbf{1}^{(l)}_J \otimes U^{(l)}_{KE}$. From this form and the relations $\mathcal{T}_U(\rho_s) = \rho_s$, we have $\mathcal{T}_{U_1 \oplus U_2}(\rho) = \rho$, where $U_1 \equiv |a\rangle\langle a| \otimes U^{(1)}_{KE} \in \mathcal{U}(\mathcal{H}_1)$ and $U_2 \equiv |b\rangle\langle b| \otimes U^{(2)}_{KE} \in \mathcal{U}(\mathcal{H}_2)$. Then from Theorem 2 $U_i = V_i \oplus \tilde{V}_i$, where $V_i \in \mathcal{U}(\mathcal{K}_i)$, $\tilde{V}_i \in \mathcal{U}(\mathcal{K}_i^{\perp})$ $(i=1,2)$, and $V_2 = (W \otimes \mathbf{1}_E) V_1 (W^{\dagger} \otimes \Sigma_E)$. This form implies that for $i=1,2$, $U(Q_i \otimes \Sigma_E) = V_i(Q_i \otimes \Sigma_E) = (Q_i \otimes \mathbf{1}_E) V_i = (Q_i \otimes \mathbf{1}_E) U$ and $U(Q_i^{\perp} \otimes \Sigma_E) = \tilde{V}_i (Q_i^{\perp} \otimes \Sigma_E) = (Q_i^{\perp} \otimes \mathbf{1}_E) \tilde{V}_i = (Q_i^{\perp} \otimes \mathbf{1}_E) U$. We can also show that $U(W \otimes \Sigma_E) = V_2(W \otimes \Sigma_E) = (W \otimes \mathbf{1}_E) V_1 = (W \otimes \mathbf{1}_E) U$ and $U(W^{\dagger} \otimes \Sigma_E) = V_1(W^{\dagger} \otimes \Sigma_E) = (W^{\dagger} \otimes \mathbf{1}_E) V_2 = (W^{\dagger} \otimes \mathbf{1}_E) U$. Since $U \in \mathcal{V}(D)$, $U(W^{(l)}_{j'j} \otimes \Sigma_E) = (W^{(l)}_{j'j} \otimes \mathbf{1}_E) U$ for any $W^{(l)}_{j'j} \in \mathcal{W}$. Combining these commuting relations and Eqs. (65)–(71), we have

$$U(\tilde{W}^{(l)}_{j'j} \otimes \Sigma_E) = (\tilde{W}^{(l)}_{j'j} \otimes \mathbf{1}_E) U \tag{78}$$

for any $\tilde{W}^{(l)}_{j'j} \in \tilde{\mathcal{W}}$. Hence $U \in \mathcal{V}(\tilde{D})$, and we obtain $\mathcal{U}_{ND} \subset \mathcal{V}(\tilde{D})$. This completes the proof of Lemma 4.

Lemmas 3 and 4 mean that starting from D_0, we can find a sequence $D_0, D_1, D_2, \ldots, D_n, \ldots$ that satisfies $r(D_0) < r(D_1) < r(D_2) < \cdots$ and $\mathcal{U}_{ND} \subset \mathcal{V}(D_n)$. Since the integer value $r(D_n)$ has an upper bound as shown in Eq. (51), the sequence must end at some point. Let D_{fin} be the last one in the sequence, and consider an isomorphism $\Gamma_{\text{fin}}: \mathcal{H}_A \to \oplus_l \mathcal{H}^{(l)}_J \otimes \mathcal{H}^{(l)}_K$ corresponding to D_{fin}. D_{fin} should not satisfy the prerequisites of Lemmas 3 and 4. From the prerequisite of Lemma 3, we see that D_{fin} satisfies the following: for any $s \in S, l$, a pure state $|a\rangle \in \mathcal{H}^{(l)}_J$, and any unitary operator V acting on $\mathcal{H}^{(l)}_J$, there exists $c \geqslant 0$ such that

$$(|a\rangle\langle a| V \otimes \mathbf{1}^{(l)}_K) \rho_s (V^{\dagger} |a\rangle\langle a| \otimes \mathbf{1}^{(l)}_K) = c(|a\rangle\langle a| \otimes \mathbf{1}^{(l)}_K) \rho_{\text{all}} (|a\rangle \times \langle a| \otimes \mathbf{1}^{(l)}_K). \tag{79}$$

Let us fix l and $|a\rangle$ for the moment. Because of Eq. (6), $Z \equiv \mathrm{Tr}[(|a\rangle\langle a| \otimes \mathbf{1}^{(l)}_K) \rho_{\text{all}} (|a\rangle\langle a| \otimes \mathbf{1}^{(l)}_K)] \neq 0$. Let us define a normalized density operator $\rho^{(l)}_K$ acting on $\mathcal{H}^{(l)}_K$ as

$$\rho^{(l)}_K \equiv (\langle a| \otimes \mathbf{1}^{(l)}_K) \rho_{\text{all}} (|a\rangle \otimes \mathbf{1}^{(l)}_K)/Z. \tag{80}$$

Equation (6) also assures that

$$\mathrm{supp}(\rho^{(l)}_K) = \mathcal{H}^{(l)}_K. \tag{81}$$

The condition (79) can be stated as, for any $s \in S$ and any unitary operator V, there exists $c' \geqslant 0$ such that

$$(|a\rangle\langle a| V \otimes \mathbf{1}^{(1)}_K) \rho_s (V^{\dagger} |a\rangle\langle a| \otimes \mathbf{1}^{(l)}_K) = c' |a\rangle\langle a| \otimes \rho^{(l)}_K. \tag{82}$$

This is satisfied if and only if $\{\rho_s\}_{s \in S}$ are written in the form

$$(\mathbf{1}^{(l)}_J \otimes \mathbf{1}^{(l)}_K) \rho_s (\mathbf{1}^{(l)}_J \otimes \mathbf{1}^{(l)}_K) = p^{(s,l)} \rho^{(s,l)}_J \otimes \rho^{(l)}_K, \tag{83}$$

where $p^{(s,l)} \geqslant 0$ and $\rho^{(s,l)}_J$, which is defined only when $p^{(s,l)} > 0$, is a normalized density operator acting on $\mathcal{H}^{(l)}_J$. Note that $\rho^{(l)}_K$ is independent of s.

Next, let us consider the prerequisites (62)–(64) of Lemma 4. If Eq. (64) is satisfied, $(|a\rangle\langle a| \otimes \mathbf{1}^{(l')}_K) \rho_s (|a\rangle\langle a| \otimes \mathbf{1}^{(l')}_K) \neq \mathbf{0}$. Then, the form (83) and Eq. (81) implies that Eq. (62) is also satisfied. Similarly, Eq. (63) is also satisfied and all the prerequisites are met. Therefore, the condition that D_{fin} should not satisfy the prerequisite of Lemma 4 means that

$$(\mathbf{1}^{(l')}_J \otimes \mathbf{1}^{(l')}_K) \rho_s (\mathbf{1}^{(l)}_J \otimes \mathbf{1}^{(l)}_K) = \mathbf{0} \tag{84}$$

for any l and $l' (\neq l)$.

Now we can state the main conclusion of this paper. From Eqs. (1), (83), and (84), we conclude that ρ_s is written as

$$\rho_s = \bigoplus_l p^{(s,l)} \rho^{(s,l)}_J \otimes \rho^{(l)}_K \tag{85}$$

under the decomposition of their support $\mathcal{H}_A$,

$$\mathcal{H}_A = \bigoplus_l \mathcal{H}^{(l)}_J \otimes \mathcal{H}^{(l)}_K, \tag{86}$$

which corresponds to D_{fin}. Here $\rho^{(s,l)}_J$ and $\rho^{(l)}_K$ are normalized density operators acting on $\mathcal{H}^{(l)}_J$ and $\mathcal{H}^{(l)}_K$, respectively, and $p^{(s,l)}$ is the probability for the state ρ_s to be in the subspace $\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$. Note that $\rho_K^{(l)}$ is independent of s. Since $\mathcal{U}_{ND}\subset\mathcal{V}(D_{\text{fin}})$, any $U\in\mathcal{U}_{ND}$ should be written as

$$U=\bigoplus_l \mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}, \tag{87}$$

where $U_{KE}^{(l)}\in\mathcal{U}(\mathcal{H}_K^{(l)})$. It is obvious that $U_{KE}^{(l)}$ must obey

$$\mathrm{Tr}_E[U_{KE}^{(l)}(\rho_K^{(l)}\otimes\Sigma_E)U_{KE}^{(l)\dagger}]=\rho_K^{(l)}. \tag{88}$$

The condition expressed by Eqs. (87) and (88) together is an equivalent condition for the condition $\mathcal{T}_U(\rho_s)=\rho_s$, since the sufficiency is apparently satisfied.

The condition (87), which is applied for an isometry $U:\mathcal{H}_A\otimes|u\rangle_E\to\mathcal{H}_A'\otimes\mathcal{H}_E$, can be rewritten in the form that applies to a unitary operator acting on $\mathcal{H}_A'\otimes\mathcal{H}_E$ as follows. Any unitary operator U acting on $\mathcal{H}_A'\otimes\mathcal{H}_E$ that preserves $\{\rho_s\}_{s\in S}$ is expressed in the following form:

$$U(\mathbf{1}_A\otimes\Sigma_E)=\bigoplus_l \mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}(\mathbf{1}_K^{(l)}\otimes\Sigma_E), \tag{89}$$

where $U_{KE}^{(l)}$ are unitary operators acting on the combined space $\mathcal{H}_K^{(l)}\otimes\mathcal{H}_E$.

From the decomposition (85), we can classify the degrees of freedom of the system into three types:

(a) The index l. The information on s is stored classically, since there are no off-diagonal elements and everything is expressed by the probability distribution $p^{(s,l)}$. The operation U, which preserves $\{\rho_s\}$, must act independently on each subspace $\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$. With such U one can establish classical correlations between the system and the ancilla through l, but not quantum correlations.

(b) The inner degree of freedom for each $\mathcal{H}_J^{(l)}$. The information on s is stored nonclassically, in the sense that there are nonvanishing off-diagonal elements for any nontrivial observables. The operation U must not act on this degree of freedom.

(c) The inner degree of freedom for each $\mathcal{H}_K^{(l)}$. No information on s is stored here. The operation U can do anything as long as it leaves the system in the known state $\rho_K^{(l)}$. For example, one can establish quantum correlation between the system and the ancilla.

In short, the principle derived here is stated as follows. In order to preserve the state of a system, no access is allowed to the part with quantum information, classical access is allowed to the part with classical information, and quantum access is allowed to the part with no information.

VI. PROPERTIES OF STRUCTURE

In the last section, we introduced a procedure to actually construct a structure D_{fin}, and stated the principle for the operations preserving $\{\rho_s\}$ using D_{fin}. In this section, we will show that the structure D_{fin} derived from the procedure is unique. We will also give a criteria of determining whether a given structure is equivalent to D_{fin} or not, without doing the procedure in Sec. V.

We first define a property of structure called "maximal," which is, as will soon be shown, the property possessed by D_{fin}.

Definition 1. Let $\Gamma:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be a unitary isomorphism corresponding to a structure D. We call D maximal if the following three conditions are met:

(i) $\Gamma\rho_s\Gamma^\dagger$ is written as

$$\Gamma\rho_s\Gamma^\dagger=\bigoplus_l p^{(s,l)}\rho_J^{(s,l)}\otimes\rho_K^{(l)}, \tag{90}$$

where $\rho_J^{(s,l)}$ and $\rho_K^{(l)}$ are normalized density operators acting on $\mathcal{H}_J^{(l)}$ and $\mathcal{H}_K^{(l)}$, respectively.

(ii) If a projection $P:\mathcal{H}_J^{(l)}\to\mathcal{H}_J^{(l)}$ satisfies

$$Pp^{(s,l)}\rho_J^{(s,l)}=p^{(s,l)}\rho_J^{(s,l)}P \tag{91}$$

for all $s\in S$, then $P=\mathbf{1}_J^{(l)}$ or $P=\mathbf{0}$.

(iii) No unitary operator $V:\mathcal{H}_J^{(l)}\to\mathcal{H}_J^{(l')}$ $(l\neq l')$ exists that satisfies

$$Vp^{(s,l)}\rho_J^{(s,l)}=\alpha p^{(s,l')}\rho_J^{(s,l')}V \tag{92}$$

for all $s\in S$ and for a positive number α.

We will then prove that the structure derived and used in the preceding section satisfies the above conditions.

Lemma 5. Any structure D_{fin} derived by the procedure in Sec. V is maximal.

Let $\Gamma_{\text{fin}}:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be an isomorphism corresponding to D_{fin}. The condition (i) in Definition 1 is apparently satisfied. For the condition (ii), suppose that a projection $P:\mathcal{H}_J^{(l)}\to\mathcal{H}_J^{(l)}$ satisfies $Pp^{(s,l)}\rho_J^{(s,l)}=p^{(s,l)}\rho_J^{(s,l)}P$ for any $s\in S$. Construct an isometry $U_1\in\mathcal{U}(\mathcal{H}_A)$ such that it operates on $\mathcal{H}^{(l)}$ as

$$U_1[(\mathbf{1}_J^{(l)}\otimes\mathbf{1}_K^{(l)})\otimes|u\rangle_E\langle u|]=(P\otimes\mathbf{1}_K^{(l)})\otimes|u^\perp\rangle_E\langle u|+[(\mathbf{1}_J^{(l)}-P)\otimes\mathbf{1}_K^{(l)}]\otimes|u\rangle_E\langle u|, \tag{93}$$

where $|u^\perp\rangle_E$ is a state orthogonal to $|u\rangle_E$, and U_1 leaves the other subspaces unaltered. It is easy to show that $U_1\in\mathcal{U}_{ND}$ using the relation $Pp^{(s,l)}\rho_J^{(s,l)}=p^{(s,l)}\rho_J^{(s,l)}P$. This means that U_1 should be written in the form of Eq. (87), which is only possible when $P=\mathbf{1}_J^{(l)}$ or $P=\mathbf{0}$. For the condition (iii), we will show that the existence of V leads to a contradiction. Without loss of generality, assume that there exists a unitary operator $V:\mathcal{H}_J^{(1)}\to\mathcal{H}_J^{(2)}$ that satisfies $p^{(s,1)}V\rho_J^{(s,1)}V^\dagger=\alpha p^{(s,2)}\rho_J^{(s,2)}$. We can construct an isometry $U_2\in\mathcal{U}_{ND}$ in the following way. Let $\mathcal{H}_E^{(1)}$ and $\mathcal{H}_E^{(2)}$ be orthogonal subspaces of $\mathcal{H}_E$ that are also orthogonal to $|u\rangle_E$. There exists an isometry $V_{KE}^{(21)}:\mathcal{H}_K^{(1)}\otimes|u\rangle_E\to\mathcal{H}_K^{(2)}\otimes\mathcal{H}_E^{(2)}$ satisfying $\mathrm{Tr}_E[V_{KE}^{(21)}(\rho_K^{(1)}\otimes\Sigma_E)V_{KE}^{(21)\dagger}]=\rho_K^{(2)}$. Physically, a simple example is the operation that discards the input state away and prepares the system in $\rho_K^{(2)}$. Similarly, let $V_{KE}^{(12)}:\mathcal{H}_K^{(2)}\otimes|u\rangle_E\to\mathcal{H}_K^{(1)}\otimes\mathcal{H}_E^{(1)}$ be an isometry satisfying $\mathrm{Tr}_E[V_{KE}^{(12)}(\rho_K^{(2)}\otimes\Sigma_E)V_{KE}^{(12)\dagger}]=\rho_K^{(1)}$. Then, we can construct a unitary operator U_2 such that it acts on $\mathcal{H}^{(1)}\oplus\mathcal{H}^{(2)}$ as

$$U_2[(P^{(1)}+P^{(2)})\otimes\Sigma_E]=\beta(P^{(1)}\otimes\Sigma_E+V^\dagger\otimes V_{KE}^{(12)})+\sqrt{1-\beta^2}(V\otimes V_{KE}^{(21)}+P^{(2)}\otimes\Sigma_E), \tag{94}$$

where $P^{(l)}\equiv\mathbf{1}_J^{(l)}\otimes\mathbf{1}_K^{(l)}$ $(l=1,\,2)$ and $\beta=\sqrt{\alpha/(1+\alpha)}$, and it does nothing on the other subspaces with $l>2$. It is then easy to show that $U_2\in\mathcal{U}_{ND}$ using the relation $p^{(s,1)}V\rho_J^{(s,1)}V^\dagger=\alpha p^{(s,2)}\rho_J^{(s,2)}$. On the other hand, because of the cross terms $V^\dagger\otimes V_{KE}^{(12)}$ and $V\otimes V_{KE}^{(21)}$, U_2 cannot be written in the form of Eq. (87), leading to a contradiction. The lemma is thus proved.

It is convenient to give a lemma showing that the conditions (ii) and (iii) in Definition 1 are equivalent to slightly stronger conditions.

Lemma 6. Let $\Gamma:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be a unitary isomorphism that corresponds to a maximal structure D, and $\Gamma\rho_s\Gamma^\dagger=\oplus_l p^{(s,l)}\rho_J^{(s,l)}\otimes\rho_K^{(l)}$. Then

(a) if an operator $\Lambda:\mathcal{H}_J^{(l)}\to\mathcal{H}_J^{(l)}$ satisfies

$$\Lambda p^{(s,l)}\rho_J^{(s,l)}=\beta p^{(s,l)}\rho_J^{(s,l)}\Lambda \tag{95}$$

for all $s\in S$ and for a complex number β, then $\Lambda=c\mathbf{1}_J^{(l)}$, where c is a complex number. Especially, $\Lambda=\mathbf{0}$ when $\beta\neq1$.

(b) If an operator $\Lambda:\mathcal{H}_J^{(l)}\to\mathcal{H}_J^{(l')}$ $(l\neq l')$ satisfies

$$\Lambda p^{(s,l)}\rho_J^{(s,l)}=\alpha p^{(s,l')}\rho_J^{(s,l')}\Lambda \tag{96}$$

for all $s\in S$ and for a positive number α, then $\Lambda=\mathbf{0}$.

First, we prove condition (a). If Λ is invertible in $\mathcal{H}_J^{(l)}$, operating Λ^{-1} from the left and taking the trace for both sides of Eq. (95), we have $p^{(s,l)}=\beta p^{(s,l)}$ for any s and hence $\beta=1$. Λ is thus not invertible if $\beta\neq1$. Let c be an eigenvalue of Λ when $\beta=1$, and let $c=0$ when $\beta\neq1$. Define $\Lambda'\equiv\Lambda-c\mathbf{1}_J^{(l)}$. Then, Λ' is not invertible in $\mathcal{H}_J^{(l)}$ for any value of β. From Eq. (95), we have $\Lambda' p^{(s,l)}\rho_J^{(s,l)}=\beta p^{(s,l)}\rho_J^{(s,l)}\Lambda'$. Let P be the projection onto $\ker\Lambda'$, the kernel of Λ'. For any vector $|a\rangle\in\ker\Lambda'$, $\Lambda' p^{(s,l)}\rho_J^{(s,l)}|a\rangle=\beta p^{(s,l)}\rho_J^{(s,l)}\Lambda'|a\rangle=0$, and hence $p^{(s,l)}\rho_J^{(s,l)}|a\rangle\in\ker\Lambda'$. We thus have $Pp^{(s,l)}\rho_J^{(s,l)}=p^{(s,l)}\rho_J^{(s,l)}P$. Since Λ' is not invertible in $\mathcal{H}_J^{(l)}$, $P\neq\mathbf{0}$. From (ii) in Definition 1, we have $P=\mathbf{1}_J^{(l)}$ and $\Lambda'=\mathbf{0}$, hence $\Lambda=c\mathbf{1}_J^{(l)}$. For the proof of (b), suppose that Eq. (96) holds. Together with its Hermite conjugate, we have $\Lambda^\dagger\Lambda p^{(s,l)}\rho_J^{(s,l)}=p^{(s,l)}\rho_J^{(s,l)}\Lambda^\dagger\Lambda$ for all s. From (b), $\Lambda^\dagger\Lambda=c\mathbf{1}_J^{(l)}$. A similar argument gives $\Lambda\Lambda^\dagger=c'\mathbf{1}_J^{(l')}$. If $\Lambda\neq\mathbf{0}$, $c>0$ and $\Lambda/\sqrt{c}:\mathcal{H}_J^{(l)}\to\mathcal{H}_J^{(l')}$ is unitary, but this conflicts with (iii) in Definition 1. Hence $\Lambda=\mathbf{0}$.

The conditions (ii) and (iii) for maximal structures have a simple meaning when we consider the algebra over C generated by the set of operators $\{\rho_s\}_{s\in S}$. Let us denote this algebra by $\mathcal{X}$. $\mathcal{H}_A$ is then regarded as a $\mathcal{X}$ module. Let $\Gamma:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be an isomorphism corresponding to a maximal structure D. Let us write a diagonalization of $\rho_K^{(l)}$, as

$$\rho_K^{(l)}=\sum_k q_k^{(l)}|a_k\rangle_K^{(l)}\langle a_k|, \tag{97}$$

where $\{|a_k\rangle_K^{(l)}\}$ $(k=1,\,2,...,\,\dim\mathcal{H}_K^{(l)})$ is a basis of $\mathcal{H}_K^{(l)}$, and $q_k^{(l)}>0$ since $\mathrm{supp}(\rho_{\mathrm{all}})=\mathcal{H}_A$. Consider a direct-sum decomposition $\mathcal{H}_A=\oplus_l(\oplus_k\mathcal{H}^{(l,k)})$, where $\mathcal{H}^{(l,k)}=\mathcal{H}_J^{(l)}\otimes|a_k\rangle_K^{(l)}$ under the isomorphism Γ. $\mathcal{H}^{(l,k)}$ are then the $\mathcal{X}$ submodules, namely, $A|x\rangle\in\mathcal{H}^{(l,k)}$ for any $A\in\mathcal{X}$ and for any $|x\rangle\in\mathcal{H}^{(l,k)}$. The condition (ii) or (a) implies that $\mathcal{H}^{(l,k)}$ is simple, namely, it has no submodules other than zero and $\mathcal{H}^{(l,k)}$ itself. The condition (iii) or (b) means that two submodules $\mathcal{H}^{(l,k)}$ and $\mathcal{H}^{(l',k')}$ with $l\neq l'$ are not $\mathcal{X}$ isomorphic. To show it, suppose that $\mathcal{H}^{(l,k)}$ and $\mathcal{H}^{(l',k')}$ are $\mathcal{X}$ isomorphic, namely, there exists a linear invertible map $\Lambda:\mathcal{H}^{(l,k)}\to\mathcal{H}^{(l',k')}$ satisfying $\Lambda A|x\rangle=A\Lambda|x\rangle$ for any $A\in\mathcal{X}$ and for any $|x\rangle\in\mathcal{H}^{(l,k)}$. $\Gamma\Lambda\Gamma^\dagger$ is written as $\Gamma\Lambda\Gamma^\dagger=\Lambda'\otimes|a_{k'}\rangle_K^{(l')}\,{}_K^{(l)}\langle a_k|$, where Λ' is a nonzero operator from $\mathcal{H}_J^{(l)}$ to $\mathcal{H}_J^{(l')}$. Since $\Lambda\rho_s=\rho_s\Lambda$ for any $s\in S$, we have

$$q_k^{(l)}\Lambda' p^{(s,l)}\rho_J^{(s,l)}=q_{k'}^{(l')}p^{(s,l')}\rho_J^{(s,l')}\Lambda'. \tag{98}$$

Lemma 6 implies that this happens only when $l=l'$.

While $\mathcal{H}^{(l,k)}$ and $\mathcal{H}^{(l',k')}$ are not $\mathcal{X}$ isomorphic when $l\neq l'$, $\mathcal{H}^{(l,k)}$ and $\mathcal{H}^{(l,k')}$ are $\mathcal{X}$ isomorphic only when $q_k^{(l)}=q_{k'}^{(l)}$, and not $\mathcal{X}$ isomorphic when $q_k^{(l)}\neq q_{k'}^{(l)}$. It may be convenient if we can construct an algebra $\tilde{\mathcal{X}}$ such that $\mathcal{H}^{(l,k)}$ and $\mathcal{H}^{(l',k')}$ are $\tilde{\mathcal{X}}$ isomorphic iff $l=l'$. We will show that such an algebra can be constructed by "normalizing" $\{\rho_s\}$ relative to ρ_{all}. First, take a decomposition of $\mathcal{H}_A$ into simple $\mathcal{X}$ submodules, $\mathcal{H}_A=\oplus_m(\oplus_i\mathcal{H}_{mi})$, where $\mathcal{H}_{mi}$ and $\mathcal{H}_{m'i'}$ are $\mathcal{X}$ isomorphic iff $m=m'$. Let P_{mi} be the projection onto $\mathcal{H}_{mi}$, and $P_m\equiv\Sigma_iP_{mi}$. Then, we define $\tilde{\rho}_s$ as

$$\tilde{\rho}_s=\sum_{m,i}\rho_sP_{mi}[\mathrm{Tr}(\rho_{\mathrm{all}}P_{mi})]^{-1}=\sum_m[\mathrm{Tr}(\rho_{\mathrm{all}}P_{m1})]^{-1}\rho_sP_m, \tag{99}$$

where we have used the fact that $\mathrm{Tr}(\rho_{\mathrm{all}}P_{mi})$ is independent of i since $\rho_{\mathrm{all}}\in\mathcal{X}$. Let $\tilde{\mathcal{X}}$ be the algebra over C generated by the set of operators $\{\tilde{\rho}_s\}_{s\in S}$. This definition is independent of the choice of the decomposition $\mathcal{H}_A=\oplus_m(\oplus_i\mathcal{H}_{mi})$. To prove it, take another decomposition $\mathcal{H}_A=\oplus_m(\oplus_i\mathcal{H}'_{mi})$ and define P'_{mi} and P'_m in the same way as before. The number of submodules are the same in the two decompositions, and we can make $\mathcal{H}_{mi}$ and $\mathcal{H}'_{mi}$ to be $\mathcal{X}$ isomorphic by appropriately arranging the order of summation (Jordan-Hölder theorem). Let $V_{mi}:\mathcal{H}_{mi}\to\mathcal{H}'_{mi}$ be a $\mathcal{X}$ isomorphism. Then, $P_{m'j}V_{mi}$ is a $\mathcal{X}$ homomorphism from $\mathcal{H}_{mi}$ to $\mathcal{H}_{m'j}$ and hence $P_{m'j}V_{mi}=0$ if $m\neq m'$ (Schur's lemma). This implies that $\mathcal{H}'_{mi}$ is a subspace of $\oplus_i\mathcal{H}_{mi}$. We thus have $P'_mP_m=P'_m$, and similarly, $P'_mP_m=P_m$, hence $P_m=P'_m$. Since $\mathcal{H}_{m1}$ and $\mathcal{H}'_{m1}$ are $\mathcal{X}$ isomorphic, $\mathrm{Tr}(\rho_{\mathrm{all}}P_{m1})=\mathrm{Tr}(\rho_{\mathrm{all}}P'_{m1})$. The algebra $\tilde{\mathcal{X}}$ and $\{\tilde{\rho}_s\}$ are thus uniquely defined by Eq. (99) when $\{\rho_s\}$ and ρ_{all} are given.

Since $\mathcal{H}_A=\oplus_l(\oplus_k\mathcal{H}^{(l,k)})$ is also a decomposition of $\mathcal{H}_A$ into simple $\mathcal{X}$ submodules, we can calculate $\tilde{\rho}_s$ as follows. The form (90) of ρ_s assures that $\rho_{\rm all}$ is written as

$$\Gamma\rho_{\rm all}\Gamma^\dagger=\bigoplus_l p_{\rm all}^{(l)}\rho_J^{({\rm all},l)}\otimes\rho_K^{(l)}, \tag{100}$$

where $\rho_J^{({\rm all},l)}$ are normalized density operators acting on $\mathcal{H}_J^{(l)}$. Equation (6) assures that $p_{\rm all}^{(l)}>0$. If we write the projection onto $\mathcal{H}^{(l,k)}$ as $P^{(l,k)}$, we have $\mathrm{Tr}(\rho_{\rm all}P^{(l,k)})=p_{\rm all}^{(l)}q_k^{(l)}$. Then we obtain

$$\Gamma\tilde{\rho}_s\Gamma^\dagger=\bigoplus_l \frac{p^{(s,l)}}{p_{\rm all}^{(l)}}\rho_J^{(s,l)}\otimes\mathbf{1}_K^{(l)}. \tag{101}$$

It is now obvious that $\mathcal{H}^{(l,k)}$ and $\mathcal{H}^{(l',k')}$ are $\tilde{\mathcal{X}}$ isomorphic when $l=l'$. It is also easy to show that they are not $\tilde{\mathcal{X}}$ isomorphic when $l\neq l'$, using a similar argument as above [Eq. (98) changes to $\Lambda'(p^{(s,l)}/p_{\rm all}^{(l)})\rho_J^{(s,l)}=(p^{(s,l')}/p_{\rm all}^{(l')})\rho_J^{(s,l')}\Lambda'$ in this case].

Using the property of the algebra $\tilde{\mathcal{X}}$, we can prove the following lemma.

Lemma 7. The maximal structure is unique.

Let $\Gamma:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be an isomorphism corresponding to a maximal structure D, and $\bar{\Gamma}:\mathcal{H}_A\to\oplus_l\bar{\mathcal{H}}_J^{(l)}\otimes\bar{\mathcal{H}}_K^{(l)}$ be an isomorphism corresponding to a maximal structure $\bar{D}$. Take bases $\{|b_k\rangle_K^{(l)}\}$ for $\mathcal{H}_K^{(l)}$ and $\{|\bar{b}_k\rangle_K^{(l)}\}$ for $\bar{\mathcal{H}}_K^{(l)}$. Let $\mathcal{H}^{(l,k)}$ be the image of $\mathcal{H}_J^{(l)}\otimes|b_k\rangle_K^{(l)}$ by $\Gamma^\dagger$, and $\bar{\mathcal{H}}^{(l,k)}$ be the image of $\bar{\mathcal{H}}_J^{(l)}\otimes|\bar{b}_k\rangle_K^{(l)}$ by $\bar{\Gamma}^\dagger$. By appropriately choosing the order of the index l, we can make $\dim\bar{\mathcal{H}}_K^{(l)}=\dim\mathcal{H}_K^{(l)}$, and $\mathcal{H}^{(l,k)}$ is $\tilde{\mathcal{X}}$ isomorphic to $\bar{\mathcal{H}}^{(l,k')}$ if and only if $l=l'$ (Jordan-Hölder theorem). Through the isomorphisms Γ and $\bar{\Gamma}$, $\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ and $\oplus_l\bar{\mathcal{H}}_J^{(l)}\otimes\bar{\mathcal{H}}_K^{(l)}$ can be regarded as $\tilde{\mathcal{X}}$ modules. Two $\tilde{\mathcal{X}}$ submodules $\mathcal{H}_J^{(l)}\otimes|b_k\rangle_K^{(l)}$ and $\bar{\mathcal{H}}_J^{(l')}\otimes|\bar{b}_{k'}\rangle_K^{(l')}$ are $\tilde{\mathcal{X}}$ isomorphic if and only if $l=l'$. Since $\bar{\Gamma}\Gamma^\dagger$ is a unitary $\tilde{\mathcal{X}}$ isomorphism, it is a direct sum of unitary $\tilde{\mathcal{X}}$ isomorphisms $V^{(l)}:\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}\to\bar{\mathcal{H}}_J^{(l)}\otimes\bar{\mathcal{H}}_K^{(l)}$ (Schur's lemma). Note that $V^{(l)\dagger}[=(V^{(l)})^{-1}]$ is also a $\tilde{\mathcal{X}}$ isomorphism. Let $P_k^{(l)}$ be the projection onto $\mathcal{H}_J^{(l)}\otimes|b_k\rangle_K^{(l)}$, and $\bar{P}_k^{(l)}$ be the projection onto $\bar{\mathcal{H}}_J^{(l)}\otimes|\bar{b}_k\rangle_K^{(l)}$. Without loss of generality, we assume that $\vec{P}_1^{(l)}V^{(l)}P_1^{(l)}\neq 0$. Since $\bar{P}_1^{(l)}V^{(l)}P_1^{(l)}$ and $(\vec{P}_1^{(l)}V^{(l)}P_1^{(l)})^\dagger$ are $\tilde{\mathcal{X}}$ homomorphisms, $(\bar{P}_1^{(l)}V^{(l)}P_1^{(l)})^\dagger(\bar{P}_1^{(l)}V^{(l)}P_1^{(l)})=(c_{11})^2P_1^{(l)}$ with $c_{11}>0$ (Schur's lemma) and hence $\bar{P}_1^{(l)}V^{(l)}P_1^{(l)}=c_{11}V_J^{(l)}\otimes|\bar{b}_1\rangle_K^{(l)}\langle b_1|$, where $V_J^{(l)}$ is a unitary map from $\mathcal{H}_J^{(l)}$ to $\bar{\mathcal{H}}_J^{(l)}$. Since $\mathbf{1}_J^{(l)}\otimes|b_1\rangle_K^{(l)}\langle b_k|$ and $\bar{\mathbf{1}}_J^{(l)}\otimes|\bar{b}_{k'}\rangle_K^{(l)}\langle\bar{b}_1|$ are $\tilde{\mathcal{X}}$ isomorphisms, $V_J^{(l)}\otimes|\bar{b}_{k'}\rangle_K^{(l)}\langle b_k|$ is also a $\tilde{\mathcal{X}}$ isomorphism for any k and k'. Then, from Schur's Lemma $(V_J^{(l)}\otimes|\bar{b}_{k'}\rangle_K^{(l)}\times\langle b_k|)^\dagger\vec{P}_{k'}^{(l)}V^{(l)}P_k^{(l)}=c_{k'k}P_k^{(l)}$, and we obtain $\bar{P}_{k'}^{(l)}V^{(l)}P_k^{(l)}=c_{k'k}V_J^{(l)}\otimes|\bar{b}_{k'}\rangle_K^{(l)}\langle b_k|$. We thus obtain

$$\bar{\Gamma}\Gamma^\dagger=\bigoplus_l V^{(l)}=\bigoplus_l\bigoplus_{k,k'}\bar{P}_{k'}^{(l)}V^{(l)}P_k^{(l)}=\bigoplus_l V_J^{(l)}\otimes V_K^{(l)}, \tag{102}$$

where $V_K^{(l)}:\mathcal{H}_K^{(l)}\to\bar{\mathcal{H}}_K^{(l)}$ is unitary since $\bar{\Gamma}\Gamma^\dagger$ and $V_K^{(l)}$ are unitary. This means that the two structures, D and $\bar{D}$, are equivalent [see Eq. (43)], and the lemma is proved.

Let us write this maximal structure as $D_{\rm max}(\{\rho_s\})$ that is uniquely determined when $\{\rho_s\}$ is given. Lemmas 5 and 7 mean that the procedure described in Sec. V always yields a unique maximal structure. This also means that if a structure is found to be maximal, it must satisfy the properties of $D_{\rm fin}$ derived in Sec. V. It will be convenient to state this in the form of a theorem.

Theorem 3. Let $\{\rho_s\}_{s\in S}$ be a set of density operators acting on $\mathcal{H}_A'$. Suppose that the dimension of $\mathcal{H}_A\equiv\cup_{s\in S}\mathrm{supp}(\rho_s)$ is finite. Let $\Gamma:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be a unitary isomorphism that corresponds to a maximal structure $D_{\rm max}(\{\rho_s\}_{s\in S})$. Then, any unitary operator U acting on $\mathcal{H}_A'\otimes\mathcal{H}_E$ that satisfies $\mathcal{T}_U(\rho_s)=\rho_s$ for any $s\in S$ is expressed in the following form under the isomorphism Γ:

$$U(\mathbf{1}_A\otimes\Sigma_E)=\bigoplus_l\mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}(\mathbf{1}_K^{(l)}\otimes\Sigma_E), \tag{103}$$

where $U_{KE}^{(l)}$ are unitary operators acting on the combined space $\mathcal{H}_K^{(l)}\otimes\mathcal{H}_E$.

Finally, let us consider the situation in which system A is made up of subsystems such that $\mathcal{H}_A=\mathcal{H}_{A1}\otimes\mathcal{H}_{A2}\otimes\cdots$, and the preparation of the initial state of system A is independently done for each subsystem $\mathcal{H}_{Ai}$. In this case, the maximal structure for $\mathcal{H}_A$ is simply given by the "direct product" of the maximal structures for each subsystem, as shown by the following theorem.

Theorem 4. Let $\{\rho_s\}_{s\in S_1}$ be density operators acting on $\mathcal{H}_{A1}$ and $\{\sigma_s\}_{s\in S_2}$ be density operators acting on $\mathcal{H}_{A2}$. Suppose that the dimensions of $\mathcal{H}_{A1}\equiv\cup_{s\in S_1}\mathrm{supp}(\rho_s)$ and $\mathcal{H}_{A2}\equiv\cup_{s\in S_2}\mathrm{supp}(\rho_s)$ are finite. Let $\Gamma_1:\mathcal{H}_{A1}\to\oplus_{l_1}\mathcal{H}_{J1}^{(l_1)}\otimes\mathcal{H}_{K1}^{(l_1)}$ be a unitary isomorphism that corresponds to a maximal structure $D_{\rm max}(\{\rho_s\}_{s\in S_1})$, and $\Gamma_2:\mathcal{H}_{A2}\to\oplus_{l_2}\mathcal{H}_{J2}^{(l_2)}\otimes\mathcal{H}_{K2}^{(l_2)}$ be a unitary isomorphism that corresponds to a maximal structure $D_{\rm max}(\{\sigma_s\}_{s\in S_2})$. Define $\mathcal{H}_A\equiv\mathcal{H}_{A1}\otimes\mathcal{H}_{A2}$, $\mathcal{H}_J^{(l)}\equiv\mathcal{H}_{J1}^{(l_1)}\otimes\mathcal{H}_{J2}^{(l_2)}$, and $\mathcal{H}_K^{(l)}\equiv\mathcal{H}_{K1}^{(l_1)}\otimes\mathcal{H}_{K2}^{(l_2)}$, where l represents the double index $\{l_1,l_2\}$. Then, $\Gamma\equiv\Gamma_1\otimes\Gamma_2:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ corresponds to the maximal structure $D_{\rm max}(\{\rho_s\otimes\sigma_t\}_{s\in S_1,t\in S_2})$.

This theorem implies that the collective operation to independently prepared systems has the same power as individual operations. For the proof, we will show that Γ satisfies the three conditions of Definition 1. From $\Gamma_1\rho_s\Gamma_1^\dagger=\oplus_{l_1}p^{(s,l_1)}\rho_{J1}^{(s,l_1)}\otimes\rho_{K1}^{(l_1)}$ and $\Gamma_2\sigma_t\Gamma_2^\dagger=\oplus_{l_2}q^{(t,l_2)}\sigma_{J2}^{(t,l_2)}\otimes\sigma_{K2}^{(l_2)}$, we have

$$\Gamma\rho_s\otimes\sigma_t\Gamma^\dagger=\bigoplus_{l_1,l_2} p^{(s,l_1)}q^{(t,l_2)}(\rho_{J1}^{(s,l_1)}\otimes\sigma_{J2}^{(t,l_2)})\otimes(\rho_{K1}^{(l_1)}\otimes\sigma_{K2}^{(l_2)}), \tag{104}$$

which means Γ satisfies the condition (i) of Definition 1. Next, construct a density operator $\sigma_{\rm all}$ by a linear combination of the states $\{\sigma_t\}_{t\in S_2}$, such that $\mathrm{supp}(\sigma_{\rm all})=\mathcal{H}_{A2}$ (see Sec. II). Then, $\sigma_{\rm all}$ is written as $\Gamma_2\sigma_{\rm all}\Gamma_2^\dagger=\oplus_{l_2}q_{\rm all}^{(l_2)}\sigma_{J2}^{({\rm all},l_2)}\otimes\sigma_{K2}^{(l_2)}$, where $q_{\rm all}^{(l_2)}>0$ [see Eq. (100)]. Take a basis $\{|k\rangle^{(l_2)}\}$ of $\mathcal{H}_{J2}^{(l_2)}$ that diagonalizes $\sigma_{J2}^{({\rm all},l_2)}$, namely, $\sigma_{J2}^{({\rm all},l_2)}|k\rangle^{(l_2)}=c_k^{(l_2)}|k\rangle^{(l_2)}$ with $c_k^{(l_2)}>0$. Suppose that for a value of $l=\{l_1,l_2\}$, a projection operator $P:\mathcal{H}_J^{(l)}\to\mathcal{H}_J^{(l)}$ satisfies $Pp^{(s,l_1)}q^{(t,l_2)}(\rho_{J1}^{(s,l_1)}\otimes\sigma_{J2}^{(t,l_2)})=p^{(s,l_1)}q^{(t,l_2)}(\rho_{J1}^{(s,l_1)}\otimes\sigma_{J2}^{(t,l_2)})P$ for all s and t. Then, $\sigma_{J2}^{({\rm all},l_2)}$ also satisfies

$$P(p^{(s,l_1)}\rho_{J1}^{(s,l_1)}\otimes\sigma_{J2}^{({\rm all},l_2)})=(p^{(s,l_1)}\rho_{J1}^{(s,l_1)}\otimes\sigma_{J2}^{({\rm all},l_2)})P \tag{105}$$

for all s. P can generally be written as $P=\Sigma_{kk'}A_{k'k}\otimes|k'\rangle^{(l_2)}\langle k|$, where $A_{k'k}$ are operators acting on $\mathcal{H}_{J1}^{(l_1)}$. Substituting it into Eq. (105), we have $A_{k'k}p^{(s,l_1)}\rho_{J1}^{(s,l_1)}=\beta p^{(s,l_1)}\rho_{J1}^{(s,l_1)}A_{k'k}$ for all s, where $\beta=c_{k'}^{(l_2)}/c_k^{(l_2)}$, and hence $A_{k'k}=\alpha_{k'k}\mathbf{1}_{J1}^{(l_1)}$ (Lemma 6). P is thus written as $P=\mathbf{1}_{J1}^{(l_1)}\otimes B_{J2}$, where B_{J2} is an operator on $\mathcal{H}_{J2}^{(l_2)}$. A similar argument with $\mathcal{H}_{J1}^{(l_1)}$ and $\mathcal{H}_{J2}^{(l_2)}$ interchanged leads to the form $P=B_{J1}\otimes\mathbf{1}_{J2}^{(l_2)}$, where B_{J1} is an operator on $\mathcal{H}_{J1}^{(l_1)}$. Noting that P is a projector, we conclude that $P=\mathbf{1}_{J1}^{(l_1)}\otimes\mathbf{1}_{J2}^{(l_2)}$ or $P=\mathbf{0}$, which means Γ satisfies the condition (ii) of Definition 1. Finally, suppose that, without loss of generality, an operator $\Lambda:\mathcal{H}_{J1}^{(1)}\otimes\mathcal{H}_{J2}^{(l_2)}\to\mathcal{H}_{J1}^{(2)}\otimes\mathcal{H}_{J2}^{(l_2')}$ satisfies $p^{(s,1)}q^{(t,l_2)}\Lambda(\rho_{J1}^{(s,1)}\otimes\sigma_{J2}^{(t,l_2)})=p^{(s,2)}q^{(t,l_2')}(\rho_{J1}^{(s,2)}\otimes\sigma_{J2}^{(t,l_2')})\Lambda$ for all s and t. Then we have

$$p^{(s,1)}q_{\rm all}^{(l_2)}\Lambda(\rho_{J1}^{(s,1)}\otimes\sigma_{J2}^{({\rm all},l_2)})=p^{(s,2)}q_{\rm all}^{(l_2')}(\rho_{J1}^{(s,2)}\otimes\sigma_{J2}^{({\rm all},l_2')})\Lambda \tag{106}$$

for all s. Λ can generally be written as $\Lambda=\Sigma_{kk'}A_{k'k}\otimes|k'\rangle^{(l_2')(l_2)}\langle k|$, where $A_{k'k}$ are operators from $\mathcal{H}_{J1}^{(1)}$ to $\mathcal{H}_{J1}^{(2)}$. Substituting it into Eq. (106), we have $A_{k'k}p^{(s,1)}\rho_{J1}^{(s,1)}=\alpha p^{(s,2)}\rho_{J1}^{(s,2)}A_{k'k}$ for all s, where $\alpha=q_{\rm all}^{(l_2')}c_{k'}^{(l_2')}/(q_{\rm all}^{(l_2)}c_k^{(l_2)})>0$. From Lemma 6, we have $A_{k'k}=\mathbf{0}$ and hence $\Lambda=\mathbf{0}$, which means Γ satisfies the condition (iii) of Definition 1.

To summarize this section, we introduced a structure called "maximal," that is uniquely defined when $\{\rho_s\}$ is given. A set of conditions (see Definition 1) was given to check whether a given structure is maximal or not. Given a maximal structure, requirement for the operations to preserve $\{\rho_s\}$ is stated in a simple manner. The procedure described in Sec. V gives a way to find a maximal structure in finite steps. Alternatively, a maximal structure is obtained by constructing the algebra $\tilde{\mathcal{X}}$ and by decomposing the $\tilde{\mathcal{X}}$ module $\mathcal{H}_A$ into simple $\tilde{\mathcal{X}}$ submodules, just like in finding irreducible representations for a group.

VII. FAITHFUL TRANSFER OF QUANTUM STATES

In the problem considered so far, the initial state of system A and the final state of the same physical system A are required to be identical. In the problems concerning with communication, we often encounter a slightly different situation in which the initial state of system A (held by the sender) and the final state of another physical system B (held by the receiver) are required to be identical. Here we will make a remark that this problem of faithful transfer of quantum states is essentially the same as the problem considered in the preceding sections. The equivalence may be self-evident when the dimensions of system A and that of system B are the same, if we note that we can freely transfer the state from system A to system B or vice versa. When the dimensions of the two systems are different, there is a subtlety in this transfer and it will be worthwhile providing a detailed argument here. The argument may also help clarifying the notations used in Sec. VIII that discusses examples of communication problems.

Let $\mathcal{H}_A'$ and $\mathcal{H}_B'$ be the Hilbert spaces for systems A and B, respectively, and $\mathcal{H}_E$ be the Hilbert space for an auxiliary system E. Initially, system A is secretly prepared in a state $\rho_s(s\in S)$. Systems B and E are prepared in standard states $\Sigma_B\equiv|u\rangle_B\langle u|$ and $\Sigma_E\equiv|u\rangle_E\langle u|$, respectively. In order to define the faithful transfer, we should assume a correspondence between the two physical systems A and B beforehand. This correspondence is given by a unitary map (isomorphism) $W_{B:A}:\mathcal{H}_A\to\mathcal{H}_B$, where $\mathcal{H}_B$ is a subspace of $\mathcal{H}_B'$ with the same dimension as $\mathcal{H}_A\equiv\cup_{s\in S}\mathrm{supp}(\rho_s)$. Any physical operation of the transfer can be described by a unitary operation U_{ABE} acting on $\mathcal{H}_A'\otimes\mathcal{H}_B'\otimes\mathcal{H}_E$. Let σ_s be the reduced state of system B after the operation of U_{ABE}. The requirement for the faithful transfer of $\{\rho_s\}$ is that the relation $\sigma_s=W_{B:A}\rho_sW_{B:A}^\dagger$ should hold for any $s\in S$. As before, the condition for this requirement will be given as a requirement for the isometry $\overline{U}_{ABE}:\mathcal{H}_A\otimes|u\rangle_B\otimes|u\rangle_E\to\mathcal{H}_A'\otimes\mathcal{H}_B'\otimes\mathcal{H}_E$, which is a restriction of U_{ABE}. The condition $\sigma_s=W_{B:A}\rho_sW_{B:A}^\dagger$ is explicitly written as

$$\mathrm{Tr}_{AE}[\overline{U}_{ABE}(\rho_s\otimes\Sigma_B\otimes\Sigma_E)\overline{U}_{ABE}^\dagger]=W_{B:A}\rho_sW_{B:A}^\dagger. \tag{107}$$

In this problem, there is no requirement for the final state of system A, and we can make it in an arbitrary state by applying a unitary operation on systems A and E. We can thus impose an additional requirement that the final state of system A should be a standard state $\Sigma_A\equiv|u\rangle_A\langle u|$, without loss of generality. We thus assume that the image of $\overline{U}_{ABE}$ is contained in $|u\rangle_A\otimes\mathcal{H}_B'\otimes\mathcal{H}_E$. Let us define $V_{B:A}\equiv|u\rangle_A(W_{B:A})_B\langle u|$ that is a unitary map from $\mathcal{H}_A\otimes|u\rangle_B$ to $|u\rangle_A\otimes\mathcal{H}_B$. Since the operator $\overline{U}_{ABE}(V_{B:A}^\dagger\otimes\Sigma_E)$ is an isometry from $|u\rangle_A\otimes\mathcal{H}_B\otimes|u\rangle_E$ to $|u\rangle_A\otimes\mathcal{H}_B'\otimes\mathcal{H}_E$, it can be written as

$$\overline{U}_{ABE}(V^{\dagger}_{B:A}\otimes\Sigma_E)=\Sigma_A\otimes\overline{U}_{BE}, \tag{108}$$

where $\overline{U}_{BE}$ is an isometry from $\mathcal{H}_B\otimes|u\rangle_E$ to $\mathcal{H}'_B\otimes\mathcal{H}_E$. Note that the relation

$$\rho_s\otimes\Sigma_B=V^{\dagger}_{B:A}(\Sigma_A\otimes W_{B:A}\rho_s W^{\dagger}_{B:A})V_{B:A} \tag{109}$$

holds for any ρ_s. Substituting this into Eq. (107) and using Eq. (108), we have

$$\mathrm{Tr}_E[\overline{U}_{BE}(W_{B:A}\rho_s W^{\dagger}_{B:A}\otimes\Sigma_E)\overline{U}^{\dagger}_{BE}]=W_{B:A}\rho_s W^{\dagger}_{B:A}. \tag{110}$$

This means that $\overline{U}_{BE}$ preserves the set of states $\{W_{B:A}\rho_s W^{\dagger}_{B:A}\}$, and the main result of Sec. V or Theorem 3 can be applied. Noting that the isomorphic relation is defined between $\mathcal{H}_A$ and $\mathcal{H}_B$, we can write the result as

$$\overline{U}_{BE}=W_{B:A}\left(\bigoplus_l \mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}\right)W^{\dagger}_{B:A}. \tag{111}$$

Combined with Eq. (108), we arrived at the following theorem.

Theorem 5. Let $\{\rho_s\}_{s\in S}$ be a set of density operators acting on $\mathcal{H}'_A$. Suppose that the dimension of $\mathcal{H}_A\equiv\cup_{s\in S}\mathrm{supp}(\rho_s)$ is finite. Let $\Gamma:\mathcal{H}_A\to\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ be a unitary isomorphism that corresponds to a maximal structure $D_{\max}(\{\rho_s\}_{s\in S})$. Let $W_{B:A}:\mathcal{H}_A\to\mathcal{H}_B$ be a unitary map, where $\mathcal{H}_B$ is a subspace of $\mathcal{H}'_B$. Then, any isometry $\overline{U}_{ABE}:\mathcal{H}_A\otimes|u\rangle_B\otimes|u\rangle_E\to|u\rangle_A\otimes\mathcal{H}'_B\otimes\mathcal{H}_E$ that satisfies

$$\mathrm{Tr}_{AE}[\overline{U}_{ABE}(\rho_s\otimes\Sigma_B\otimes\Sigma_E)\overline{U}^{\dagger}_{ABE}]=W_{B:A}\rho_s W^{\dagger}_{B:A} \tag{112}$$

for any $s\in S$ is expressed in the following form under the isomorphism Γ:

$$\overline{U}_{ABE}=|u\rangle_A(W_{B:A})\left(\bigoplus_l \mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}\right)_B\langle u|, \tag{113}$$

where $U_{KE}^{(l)}$ are isometries from $\mathcal{H}_K^{(l)}\otimes|u\rangle_E$ to $\mathcal{H}_K^{(l)}\otimes\mathcal{H}_E$.

VIII. APPLICATION TO VARIOUS PROBLEMS

In this section, we apply the derived properties of the operations preserving a set of states to various problems such as cloning, cryptography, and data compression.

A. Broadcasting of mixed states

No-broadcasting condition for mixed states, which was derived in Ref. [4], can easily be rederived. The broadcasting is the task of preparing the marginal state of a subsystem of E in ρ_s, and leaving the reduced state of the system A undisturbed as in ρ_s. Since the operations that do not disturb $\{\rho_s\}$ are insensitive to the state changes in the subspaces $\mathcal{H}_J^{(l)}$, complete broadcasting is possible only when the dimensions of the subspaces $\mathcal{H}_J^{(l)}$ are all unity, or equivalently, when $\{\rho_s\}$ can be simultaneously diagonalized.

In addition to rederiving this criteria, the derived principle here can also determine the feasibility of various correlations between the two broadcast systems, which was raised as an open question in Ref. [4]. Let us consider the broadcasting of $\{\rho_s\}$ in system A into the two systems B and C. Let H'_X ($X=A,\ B,\ C$) be the Hilbert space for system X, and suppose that the dimension of $\mathcal{H}_A\equiv\cup_{s\in S}\mathrm{supp}(\rho_s)$ is finite. Take a subspace $H_X\subset H'_X$ ($X=B,\ C$) with the same size as $\mathcal{H}_A$, and let $W_{B:A}:\mathcal{H}_A\to\mathcal{H}_B$ and $W_{C:A}:\mathcal{H}_A\to\mathcal{H}_C$ be unitary maps defining the relation among the three systems. The process of broadcasting is defined as

$$\rho_s\otimes\Sigma_B\otimes\Sigma_C\to\Sigma_A\otimes\chi_{BC}^{(s)} \tag{114}$$

with

$$\mathrm{Tr}_C(\chi_{BC}^{(s)})=W_{B:A}\rho_s W^{\dagger}_{B:A},\quad \mathrm{Tr}_B(\chi_{BC}^{(s)})=W_{C:A}\rho_s W^{\dagger}_{C:A}, \tag{115}$$

where $\Sigma_X\equiv|u\rangle_X\langle u|$ ($X=A,\ B,\ C$) are standard states. When the broadcasting is possible, the supporting space $\mathcal{H}_A$ can be decomposed as $\mathcal{H}_A=\oplus_l\mathcal{H}_K^{(l)}$, since $\mathcal{H}_J^{(l)}$ is one-dimensional and can thus be neglected. Then, by taking appropriate bases $\{|a_k\rangle_K^{(l)}\}$ for $\mathcal{H}_K^{(l)}$, we can write $\rho_s=\oplus_l p^{(s,l)}\rho_K^{(l)}=\Sigma_l\Sigma_k p^{(s,l)}q_k^{(l)}|a_k\rangle_K^{(l)}\langle a_k|$. Let us take bases for $\mathcal{H}_B$ and $\mathcal{H}_C$ by $|a_k\rangle_B^{(l)}\equiv W_{B:A}|a_k\rangle_K^{(l)}$ and $|a_k\rangle_C^{(l)}\equiv W_{C:A}|a_k\rangle_K^{(l)}$. The broadcast state $\chi_{BC}^{(s)}$ satisfying Eq. (115) is not unique and various types of correlations between systems B and C are conceivable. For example, a state with no correlation

$$\chi_{BC}^{(s)}=W_{B:A}\rho_s W^{\dagger}_{B:A}\otimes W_{C:A}\rho_s W^{\dagger}_{C:A}, \tag{116}$$

a state with classical correlations

$$\chi_{BC}^{(s)}=\sum_l\sum_k p^{(s,l)}q_k^{(l)}|a_k\rangle_B^{(l)}\langle a_k|\otimes|a_k\rangle_C^{(l)}\langle a_k|, \tag{117}$$

and a state with quantum correlations $\chi_{BC}^{(s)}=|\chi^{(s)}\rangle\langle\chi^{(s)}|$ with

$$|\chi^{(s)}\rangle=\sum_l\sum_k \exp(i\,\theta_{l,k})\sqrt{p^{(s,l)}q_k^{(l)}}|a_k\rangle_B^{(l)}|a_k\rangle_C^{(l)}, \tag{118}$$

all satisfy Eq. (115). The question here is, among these and other conceivable correlations, what are feasible by a physical process Eq. (114). To answer this problem, let us start by noting that any physical process acting on $\{\rho_s\}$ corresponds to an isometry $\overline{U}_{ABCE}:\mathcal{H}_A\otimes|u\rangle_B\otimes|u\rangle_C\otimes|u\rangle_E\to|u\rangle_A\otimes\mathcal{H}'_B\otimes\mathcal{H}'_C\otimes\mathcal{H}_E$ with an auxiliary system E. Along with the decomposition $\mathcal{H}_A=\oplus_l\mathcal{H}_K^{(l)}$, we can decompose $\overline{U}_{ABCE}$ as $\overline{U}_{ABCE}=\oplus_l\overline{U}_{ABCE}^{(l)}$ by isometries $\overline{U}_{ABCE}^{(l)}:\mathcal{H}_K^{(l)}\otimes|u\rangle_B\otimes|u\rangle_C\otimes|u\rangle_E\to|u\rangle_A\otimes\mathcal{H}'_B\otimes\mathcal{H}'_C\otimes\mathcal{H}_E$. Since ρ_s is exactly transferred from A to B, we have, from Theorem 5,

$$\overline{U}_{ABCE}=|u\rangle_A(W_{B:A})\left(\bigoplus_l \mathbf{1}_J^{(l)}\otimes U_{KCE}^{(l)}\right)_B\langle u|, \tag{119}$$

where $U_{KCE}^{(l)}$ are isometries from $\mathcal{H}_K^{(l)}\otimes|u\rangle_C\otimes|u\rangle_E$ to $\mathcal{H}_K^{(l)}\otimes\mathcal{H}'_C\otimes\mathcal{H}_E$. Noting that we are omitting $\mathcal{H}_J^{(l)}$, we have

$$\bar{U}^{(l)}_{ABCE}=|u\rangle_A(W_{B:A})(U^{(l)}_{KCE})_B\langle u|. \tag{120}$$

This means that the image of $\bar{U}^{(l)}_{ABCE}$ is contained in $|u\rangle_A \otimes\mathcal{H}^{(l)}_B\otimes\mathcal{H}'_C\otimes\mathcal{H}_E$, where $\mathcal{H}^{(l)}_B$ is the image of $\mathcal{H}^{(l)}_K$ by $W_{B:A}$. Similarly, since ρ_s is exactly transferred from A to C, we have another expression,

$$\bar{U}^{(l)}_{ABCE}=|u\rangle_A(W_{C:A})(U^{(l)}_{KBE})_C\langle u|, \tag{121}$$

where $U^{(l)}_{KBE}$ are isometries from $\mathcal{H}^{(l)}_K\otimes|u\rangle_B\otimes|u\rangle_E$ to $\mathcal{H}^{(l)}_K \otimes\mathcal{H}'_B\otimes\mathcal{H}_E$. By this expression, the image of $\bar{U}^{(l)}_{ABCE}$ is further restricted to $|u\rangle_A\otimes\mathcal{H}^{(l)}_B\otimes\mathcal{H}^{(l)}_C\otimes\mathcal{H}_E$, where $\mathcal{H}^{(l)}_C$ is the image of $\mathcal{H}^{(l)}_K$ by $W_{C:A}$. The operation $\bar{U}_{ABCE}$ thus only connects the subspaces labeled by the same value of index l. The broadcast state $\chi^{(s)}_{BC}$, which is given by

$$\chi^{(s)}_{BC}=\mathrm{Tr}_{AE}[\bar{U}_{ABCE}(\rho_s\otimes\Sigma_B\otimes\Sigma_C\otimes\Sigma_E)\bar{U}^{\dagger}_{ABCE}], \tag{122}$$

should therefore be written as

$$\chi^{(s)}_{BC}=\bigoplus_l p^{(s,l)}\zeta^{(l)}_{BC}, \tag{123}$$

where $\zeta^{(l)}_{BC}$ is a density operator acting on $\mathcal{H}^{(l)}_B\otimes\mathcal{H}^{(l)}_C$, given by

$$\zeta^{(l)}_{BC}\equiv\mathrm{Tr}_{AE}[\bar{U}^{(l)}_{ABCE}(\rho^{(l)}_K\otimes\Sigma_B\otimes\Sigma_C\otimes\Sigma_E)\bar{U}^{(l)\dagger}_{ABCE}]. \tag{124}$$

The condition (115) for broadcasting is satisfied iff

$$\mathrm{Tr}_C(\zeta^{(l)}_{BC})=W_{B:A}\rho^{(l)}_K W^{\dagger}_{B:A}, \quad \mathrm{Tr}_B(\zeta^{(l)}_{BC})=W_{C:A}\rho^{(l)}_K W^{\dagger}_{C:A} \tag{125}$$

holds for all l. Since $\zeta^{(l)}_{BC}$ is independent of s, it can be any state by choosing $\bar{U}^{(l)}_{ABCE}$ appropriately. This means that any type of correlation is feasible in each subspace $\mathcal{H}^{(l)}_B\otimes\mathcal{H}^{(l)}_C$, ranging from quantum correlation (entanglement) to no correlation. On the other hand, Eq. (123) means that for the index l, a complete classical correlation should always be established between the broadcast systems.

One of the interesting consequences from the above general result is that the condition for the feasibility of the broadcast state with no correlation [Eq. (116)] and that of broadcast states with full quantum correlation [Eq. (118)] are the same. For both cases, the condition is that any ρ_s should be contained in one of the subspaces $\mathcal{H}^{(l)}_K$, or equivalently, any pair of states from $\{\rho_s\}$ must be identical or orthogonal.

B. Imprinting of mixed states

Another open question was the condition for the feasibility of the imprinting process [7]. The no-imprinting condition is the requirement for $\{\rho_s\}$ such that any attempt to read out the information on s should lead to some changes in the state of system A. More formally, under the notations used here, it is the condition for $\{\rho_s\}$ such that for any unitary operator U acting on $\mathcal{H}'_A\otimes\mathcal{H}_E$ satisfying $\mathrm{Tr}_E[U(\rho_s \otimes\Sigma_E)U^\dagger]=\rho_s$, the reduced state of system E, $\mathrm{Tr}_A[U(\rho_s \otimes\Sigma_E)U^\dagger]$, should be independent of s.

This condition is obvious now. According to the present result, such an operation U is insensitive to the contents of $\mathcal{H}^{(l)}_J$, and $\mathcal{H}^{(l)}_K$ holds no information on s. On the other hand, the index l can be read out freely without disturbing $\{\rho_s\}$. Hence the condition is stated as $p^{(s,l)}=p^{(s',l)}$ for all $\{s,s',l\}$, namely, the probability distribution for the index l is identical for all s. In other words, this is the requirement that if $\{\rho_s\}$ are written as matrices in the maximally simultaneously block-diagonalized form, the traces for each block are the same for all s.

A generalized version of this theorem, where the set of states $\{\sigma_{s'}\}_{s'\in S'}$ to be distinguished is different from the set of states $\{\rho_s\}$ to be preserved, can also be derived from the above results. A little care should be taken for the fact that the support of all states, defined as $\bar{\mathcal{H}}_A =[\cup_{s\in S}\mathrm{supp}(\rho_s)]\cup[\cup_{s'\in S'}\mathrm{supp}(\sigma_{s'})]$, may generally be larger than $\mathcal{H}_A=\cup_{s\in S}\mathrm{supp}(\rho_s)$. Let us write $\bar{\mathcal{H}}_A=\mathcal{H}_A \oplus\mathcal{H}_0$. Consider the set of all isometries $U:\bar{\mathcal{H}}_A\otimes|u\rangle_E\rightarrow\bar{\mathcal{H}}_A \otimes\mathcal{H}_E$ that preserve $\{\rho_s\}$, namely, $\mathrm{Tr}_E[U(\rho_s\otimes\Sigma_E)U^\dagger]=\rho_s$. What we ask here is the condition for $\{\sigma_{s'}\}_{s'\in S'}$ such that $\mathrm{Tr}_A[U(\sigma_{s'}\otimes\Sigma_E)U^\dagger]$ is independent of $s'\in S'$ under any such U. We first derive a sufficient condition. According to Theorem 3, a decomposition $\mathcal{H}_A=\oplus_l\mathcal{H}^{(l)}_J\otimes\mathcal{H}^{(l)}_K$ is determined from $\{\rho_s\}$, and U is written as

$$U=U_{0E}\oplus\left(\bigoplus_l \mathbf{1}^{(l)}_J\otimes U^{(l)}_{KE}\right), \tag{126}$$

where $U^{(l)}_{KE}$ are isometries from $\mathcal{H}^{(l)}_K\otimes|u\rangle_E$ to $\mathcal{H}^{(l)}_K\otimes\mathcal{H}_E$, and U_{0E} is an isometry from $\mathcal{H}_0\otimes|u\rangle_E$ to $\bar{\mathcal{H}}_A\otimes\mathcal{H}_E$. Note that the image of U_{0E} is not necessarily confined in $\mathcal{H}_0\otimes\mathcal{H}_E$. Then we can write

$$\begin{aligned}
&\mathrm{Tr}_A[U(\sigma_{s'}\otimes\Sigma_E)U^\dagger]\\
&\quad=\mathrm{Tr}_A[U_{0E}(\sigma_{s'}\otimes\Sigma_E)U^\dagger_{0E}]\\
&\qquad+\sum_l\,(\mathrm{Tr}_A[U_{0E}(\sigma_{s'}\otimes\Sigma_E)(\mathbf{1}^{(l)}_J\otimes U^{(l)}_{KE})^\dagger]\\
&\qquad+\mathrm{Tr}_A[(\mathbf{1}^{(l)}_J\otimes U^{(l)}_{KE})(\sigma_{s'}\otimes\Sigma_E)U^\dagger_{0E}]\\
&\qquad+\mathrm{Tr}_A[(\mathbf{1}^{(l)}_J\otimes U^{(l)}_{KE})(\sigma_{s'}\otimes\Sigma_E)(\mathbf{1}^{(l)}_J\otimes U^{(l)}_{KE})^\dagger]).
\end{aligned} \tag{127}$$

Let P_0, P_A, and $P^{(l)}_A$ be the projection operators onto $\mathcal{H}_0$, $\mathcal{H}_A$, and $\mathcal{H}^{(l)}_J\otimes\mathcal{H}^{(l)}_K$, respectively. Equation (127) means that the state left in system E depends only on the following parts of the initial state $\sigma_{s'}$, defined as

$$\sigma^{(00)}_{s'}\equiv P_0\sigma_{s'}P_0,$$

$$\sigma^{(0A)}_{s'}\equiv P_0\sigma_{s'}P_A,\quad \sigma^{(A0)}_{s'}\equiv P_A\sigma_{s'}P_0,$$

$$\sigma^{(l)}_{s'}\equiv\mathrm{Tr}^{(l)}_J(P^{(l)}_A\sigma_{s'}P^{(l)}_A), \tag{128}$$

and Eq. (127) becomes

$$\begin{aligned}\mathrm{Tr}_A[U(\sigma_{s'}\otimes\Sigma_E)U^\dagger]&=\mathrm{Tr}_A[U_{0E}(\sigma_{s'}^{(00)}\otimes\Sigma_E)U_{0E}^\dagger]\\&\quad+\sum_l\,(\mathrm{Tr}_A[U_{0E}(\sigma_{s'}^{(0A)}\otimes\Sigma_E)(\mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)})^\dagger]\\&\quad+\mathrm{Tr}_A[(\mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)})(\sigma_{s'}^{(A0)}\otimes\Sigma_E)U_{0E}^\dagger]\\&\quad+\mathrm{Tr}_K^{(l)}[U_{KE}^{(l)}(\sigma_{s'}^{(l)}\otimes\Sigma_E)(U_{KE}^{(l)})^\dagger]).\end{aligned}\tag{129}$$

Here $\mathrm{Tr}_J^{(l)}$ and $\mathrm{Tr}_K^{(l)}$ are the partial traces over $\mathcal{H}_J^{(l)}$ and $\mathcal{H}_K^{(l)}$, respectively. Hence a sufficient condition for the state left in system E to have no dependence on s' is that the operators defined in Eq. (128) are independent of s'.

To show that this condition is also necessary, we will consider a particular measurement strategy. Let l^* be one of the possible values of the index l. The first step of the strategy is to conduct an ideal projection measurement to measure whether the state is in the subspace $\mathcal{H}_0\oplus\mathcal{H}_J^{(l^*)}\otimes\mathcal{H}_K^{(l^*)}$ or not. It is obvious that this measurement does not disturb $\{\rho_s\}$. Let $p(l^*,s')$ be the probability of obtaining the positive outcome when the initial state was $\sigma_{s'}$. Suppose that the result of the measurement was positive. Prepare auxiliary physical systems J and K with Hilbert spaces $\mathcal{H}_J$ and $\mathcal{H}_K=\mathcal{H}_{K0}\oplus\mathcal{H}_{K1}$, respectively, where $\dim\mathcal{H}_J=\dim\mathcal{H}_J^{(l^*)}$, $\dim\mathcal{H}_{K1}=\dim\mathcal{H}_K^{(l^*)}$, and $\dim\mathcal{H}_{K0}=\dim\mathcal{H}_0$. Take unitary maps $\Gamma_J:\mathcal{H}_J^{(l^*)}\to\mathcal{H}_J$, $\Gamma_K:\mathcal{H}_K^{(l^*)}\to\mathcal{H}_{K1}$, and $\Gamma_0:\mathcal{H}_0\to\mathcal{H}_{K0}$. Take an arbitrary state $|x\rangle\in\mathcal{H}_J^{(l^*)}$, and let $\Gamma_0':\mathcal{H}_0\to(\Gamma_J|x\rangle)\otimes\mathcal{H}_{K0}$ be the unitary map naturally determined from Γ_0. Then, we can construct an isometry $\Gamma:\mathcal{H}_0\oplus\mathcal{H}_J^{(l^*)}\otimes\mathcal{H}_K^{(l^*)}\to\mathcal{H}_J\otimes\mathcal{H}_K$ by $\Gamma\equiv\Gamma_0'\oplus\Gamma_J\otimes\Gamma_K$. The second step is to transfer the postmeasurement state of system A, which is projected in $\mathcal{H}_0\oplus\mathcal{H}_J^{(l^*)}\otimes\mathcal{H}_K^{(l^*)}$, to the combined system of J and K according to the isometry Γ. Note that if the initial state was ρ_s, the state of $\mathcal{H}_J\otimes\mathcal{H}_K$ after the second step is $\Gamma_J\rho_J^{(s,l^*)}\Gamma_J^\dagger\otimes\Gamma_K\rho_K^{(l^*)}\Gamma_K^\dagger$. The third step is to conduct arbitrary measurement on system K, and to leave system K in $\Gamma_K\rho_K^{(l^*)}\Gamma_K^\dagger$, which is independent of the initial state. At the final step, the state of $\mathcal{H}_J\otimes\mathcal{H}_K$, which should be contained in the image of Γ, is transferred back to $\mathcal{H}_0\oplus\mathcal{H}_J^{(l^*)}\otimes\mathcal{H}_K^{(l^*)}$. It is easy to see that the whole process does not disturb $\{\rho_s\}$. When the initial state was $\sigma_{s'}$, the marginal state of system K after the second step, multiplied by $p(l^*,s')$, is

$$\begin{aligned}\mathrm{Tr}_J[\Gamma(P_0\oplus\mathbf{1}_J^{(l^*)}\otimes\mathbf{1}_K^{(l^*)})\sigma_{s'}(P_0\oplus\mathbf{1}_J^{(l^*)}\otimes\mathbf{1}_K^{(l^*)})\Gamma^\dagger]&=\Gamma_0\sigma_{s'}^{(00)}\Gamma_0^\dagger+\Gamma_0\sigma_{s'}^{(0A)}(|x\rangle\otimes\mathbf{1}_K^{(l^*)})\Gamma_K^\dagger\\&\quad+\Gamma_K(\langle x|\otimes\mathbf{1}_K^{(l^*)})\sigma_{s'}^{(A0)}\Gamma_0^\dagger+\Gamma_K\sigma_{s'}^{(l^*)}\Gamma_K^\dagger.\end{aligned}\tag{130}$$

If we require, for this particular strategy, that the statistics of the outcomes of the measurement of the first step and the arbitrary measurement in the third step should be independent of s', then the reduced state in Eq. (130) must be independent of s'. Since the choices of l^* and $|x\rangle$ were arbitrary, we conclude that it is necessary that $\sigma_{s'}^{(00)}$, $\sigma_{s'}^{(0A)}$, $\sigma_{s'}^{(A0)}$, and $\sigma_{s'}^{(l)}$ for any l be independent of s'. It is worth emphasizing here that the above result shows that any difference in the off-diagonal part $(\sigma_{s'}^{(0A)})$ between $\mathcal{H}_0$ and $\mathcal{H}_A$ is detectable even under a stringent restriction to the operation to $\mathcal{H}_A$.

C. Cloning and imprinting of composite systems

Consider the situation in which the system holding an unknown initial state χ_s is composed of two subsystems A and B, and it is allowed to access these subsystems only in sequence, namely, subsystem A must be released before subsystem B is accessed [5,7]. In order to preserve the states $\{\chi_s\}$ in the whole system, the marginal density operator in A, $\rho_s\equiv\mathrm{Tr}_B(\chi_s)$, must not be modified when it is released. The present results can thus be applied and restrict the form of the operation when subsystem A is at hand. Let us write this operation by an isometry $U_{AE}:\mathcal{H}_A\otimes|u\rangle_E\to\mathcal{H}_A\otimes\mathcal{H}_E$, where $\mathcal{H}_A=\cup_{s\in S}\mathrm{supp}(\rho_s)$, and $\mathcal{H}_E$ describes an auxiliary system initially prepared in a standard state $\Sigma_E=|u\rangle_E\langle u|$. Let $\mathcal{H}_B$ be the Hilbert space for subsystem B. According to Theorem 3, a decomposition $\mathcal{H}_A=\oplus_l\mathcal{H}_J^{(l)}\otimes\mathcal{H}_K^{(l)}$ is determined from $\{\rho_s\}$, and U_{AE} is written as

$$U_{AE}=\bigoplus_l\mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)},\tag{131}$$

where $U_{KE}^{(l)}$ are isometries from $\mathcal{H}_K^{(l)}\otimes|u\rangle_E$ to $\mathcal{H}_K^{(l)}\otimes\mathcal{H}_E$. Then we can write the marginal state $\chi_{BE}^{(s)}$ of the combined system of E and B after the operation U_{AE} as

$$\begin{aligned}\chi_{BE}^{(s)}&\equiv\mathrm{Tr}_A[(U_{AE}\otimes\mathbf{1}_B)(\chi_s\otimes\Sigma_E)(U_{AE}^\dagger\otimes\mathbf{1}_B)]\\&=\sum_l\,\mathrm{Tr}_A[(\mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}\otimes\mathbf{1}_B)(\chi_s\otimes\Sigma_E)(\mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)\dagger}\otimes\mathbf{1}_B)]\\&=\sum_l\,\mathrm{Tr}_K^{(l)}[(U_{KE}^{(l)}\otimes\mathbf{1}_B)(\chi_s^{(l)}\otimes\Sigma_E)(U_{KE}^{(l)\dagger}\otimes\mathbf{1}_B)],\end{aligned}\tag{132}$$

where

$$\chi_s^{(l)}\equiv\mathrm{Tr}_J^{(l)}[(P_A^{(l)}\otimes\mathbf{1}_B)\chi_s(P_A^{(l)}\otimes\mathbf{1}_B)].\tag{133}$$

This means that if we are to preserve $\mathrm{Tr}_B(\chi_s)$, we can obtain only the part of the correlations between A and B, namely, we can obtain classical correlations related to the index l and quantum correlations related to each $\mathcal{H}_K^{(l)}$, but cannot obtain quantum correlations related to the index l or any correlations related to each $\mathcal{H}_J^{(l)}$. Note that extracting this information to the auxiliary system E may destroy original quantum correlations between A and B.

When $\{\chi_s\}$ are all different pure states, the cloning of $\{\chi_s\}$ is possible only when $\{\chi_s\}$ are all orthogonal. Hence, if the cloning is possible, we should be able to determine s completely by conducting a measurement on $\chi_{BE}^{(s)}$, namely, $\{\chi_{BE}^{(s)}\}$ should be all orthogonal. This is possible only when $\chi_s^{(l)}$ and $\chi_{s'}^{(l)}$ are orthogonal for any l and for any $s\neq s'$. This condition is also sufficient for the cloning to be possible, since under that condition we can determine the value of s by accessing B and E without disturbing the whole state $(U_{AE}\otimes\mathbf{1}_B)(\chi_s\otimes\Sigma_E)(U_{AE}^{\dagger}\otimes\mathbf{1}_B)$. At this stage, we know exactly the current pure state of the system ABE, and the marginal state of subsystem A is $\mathrm{Tr}_B(\chi_s)$. Then we can determine a unitary operation over BE that drives the state of ABE back into $\chi_s\otimes\Sigma_E$.

When the initial states $\{\chi_s\}$ include mixed states, it is not always possible to restore the original quantum correlations between A and B by manipulating system BE only. Also in the problem of imprinting of more than two pure states, the restoration is not always possible because the identification of s by accessing system BE is not necessarily possible. The feasibility of this restoration of quantum correlation will be an interesting future problem.

D. Various schemes of quantum key distribution

An attempt was recently made by Mor [7] to give a unified explanation of why various schemes of quantum key distribution work in the ideal situations, which was based on the no-cloning principle of mixed states. Since we have obtained a general principle including the no-cloning principle, we provide a unified formalism of various schemes for quantum key distribution. The principle here places some restriction on the eavesdropper's access to the first quantum system A transmitted from the sender to the receiver, if the eavesdropper wants to preserve the state in order to conceal her presence. Then we can find three different ways to conceal the bit value from the eavesdropper, namely (i) encoding it directly on the inner degree of freedom for $\mathcal{H}_J^{(l)}$, (ii) encoding it on the correlation between A and another system B through the inner degree of freedom for $\mathcal{H}_J^{(l)}$, and (iii) encoding it on the *quantum* correlation between A and B, through the index l. The original four-state scheme of Bennett and Brassard [8] corresponds to the case (ii), since the bit value is encoded on the correlation between the quantum state of the photon and the information of the basis transmitted later [9], which corresponds to the system B. The scheme [10] using two nonorthogonal pure states corresponds to the case (i), and the schemes using three [11] or two [12] entangled states in the composite system correspond to the case (iii).

E. Optimal compression rate of quantum-state signals

Consider a source that produces the ensemble $\mathcal{E}=\{p_s,\rho_s\}$, namely, it emits a system in a quantum state ρ_s with probability $p_s>0$. One of the fundamental questions in quantum information theory is to identify the optimal compression rate of $\mathcal{E}$, namely, to determine how much qubits are needed to compress a sequence of systems independently prepared from this source so that it can be decompressed back with negligible errors in the asymptotic limit of the infinitely long sequence. Noting that the original states ρ_s are reproduced after the decompression, the present results can be applied to the whole operation of compression and decompression, and reveal the optimal compression rate in the blind scenario. Using the decomposition $\rho_s=\oplus_l p^{(s,l)}\rho_J^{(s,l)}\otimes\rho_K^{(l)}$, the average density operator $\rho\equiv\Sigma_s p_s\rho_s$ is also decomposed as

$$\rho=\bigoplus_l p^{(l)}\rho_J^{(l)}\otimes\rho_K^{(l)}, \tag{134}$$

where $p^{(l)}\equiv\Sigma_s p_s p^{(s,l)}$ and $\rho_J^{(l)}\equiv(\Sigma_s p_s p^{(s,l)}\rho_J^{(s,l)})/p^{(l)}$. This naturally gives a decomposition of the von Neumann entropy of ρ, defined as $S(\rho)\equiv-\mathrm{Tr}\rho\log_2\rho$, into the sum of three parts as follows:

$$\begin{aligned} S(\rho)&=\sum_l p^{(l)}[-\log_2 p^{(l)}+S(\rho_J^{(l)})+S(\rho_K^{(l)})]\\ &\equiv I_C+I_{NC}+I_R. \end{aligned} \tag{135}$$

Then, the form $\rho_s=\oplus_l p^{(s,l)}\rho_J^{(s,l)}\otimes\rho_K^{(l)}$ tells us that $\mathcal{E}$ can be compressed into I_C+I_{NC} qubits, and its optimality can be shown from the fact that any compression-decompression scheme must be written in the form of $U_{AE}=\oplus_l\mathbf{1}_J^{(l)}\otimes U_{KE}^{(l)}$ [13]. It was also shown that among I_C+I_{NC} qubits, I_C qubits can be replaced by the same number of classical bits [14,15]. A similar argument can also be made to the teleportation of the ensemble $\mathcal{E}$, and the optimally required amount of entanglement was shown to be I_{NC} ebits. These results again suggest that the decomposition $\rho_s=\oplus_l p^{(s,l)}\rho_J^{(s,l)}\otimes\rho_K^{(l)}$ gives a way to classify the degrees of freedom into the three parts, namely, classical, nonclassical, and redundant parts.

Using Theorem 4 derived in Sec. VI, we immediately see that the above information-theoretic functions $I_C(\mathcal{E})$, $I_{NC}(\mathcal{E})$, $I_R(\mathcal{E})$, and hence the various optimal rates, are additive for independent sources. That is to say, if we consider another source $\mathcal{E}'=\{q_{s'},\sigma_{s'}\}$ and the combined source $\tilde{\mathcal{E}}=\{p_s q_{s'},\rho_s\otimes\sigma_{s'}\}$, we have $I_X(\tilde{\mathcal{E}})=I_X(\mathcal{E})+I_X(\mathcal{E}')$ $(X=C,NC,R)$.

IX. CONCLUSION

In this paper, we have considered a situation that we frequently encounter in dealing with problems in quantum information, namely, given a system secretly prepared in one of the possible states $\{\rho_s\}$, conducting a general operation to the system, then leaving the state of the system exactly in the same state as the initially given state. In order to derive a general property of such operations, we noted two basic principles. One is a natural extension of a property of classical signals, which states that in order not to disturb a signal that may be produced by two different probability distributions, we are not allowed to operate on the entire signal space freely, but are forced to operate on two or more signal subspaces independently. The other principle stems genuinely from quantum origin, and it states that if we are to operate on two subspaces independently while preserving a state having a nonzero off-diagonal part with respect to the two subspaces, the operations to the two subspaces must satisfy a similarity defined through the off-diagonal part of the state. The two types of constraints alternately invoke each other, and finally reveal a stringent condition for the operations to preserve $\{\rho_s\}$, together with a decomposition of the support space of $\{\rho_s\}$, which takes a form $\mathcal{H}_A = \oplus_l \mathcal{H}_J^{(l)} \otimes \mathcal{H}_K^{(l)}$. Under this decomposition, the states $\{\rho_s\}$ are written as $\rho_s = \oplus_l p^{(s,l)} \rho_J^{(s,l)} \otimes \rho_K^{(l)}$. If we consider how the information of the state index s is encoded on three parts, namely, on index l, on Hilbert space $\mathcal{H}_J^{(l)}$, and on Hilbert space $\mathcal{H}_K^{(l)}$, we may regard them as classical, nonclassical (quantum), and redundant parts, respectively, since ρ_s has no off-diagonal part with respect to index l, and no information on s is stored on $\mathcal{H}_K^{(l)}$. Under this decomposition, the main result describing the property of the operations to preserve $\{\rho_s\}$ is written as $U_{AE} = \oplus_l \mathbf{1}_J^{(l)} \otimes U_{KE}^{(l)}$ that informally implies that the nonclassical part is untouchable, the classical part is read only, and the redundant part is open.

The result may be viewed as an unexpectedly straightforward extension of the simplest case of binary string $s=0$, 1 encoded on two pure states $|\Psi_0\rangle$ and $|\Psi_1\rangle$. We can distinguish three cases according to the inner product of the two pure states. The encoding will be regarded as ‘‘classical’’ when the two states are orthogonal, ‘‘nonclassical’’ when they are nonorthogonal and nonidentical, and ‘‘redundant’’ when identical. When this situation is extended to allow mixed states and a larger number of states, it has turned out that the three types of the encoding may coexist, but they are still distinct. The inner product for two vectors must be replaced by mathematical concepts describing rather complicated relations among many density operators. In this paper, we have attempted to do this by regarding the Hilbert space as a module over an algebra generate by $\{\rho_s\}$ with a proper normalization. Then, the notion of ‘‘nonorthogonal’’ corresponds to irreducibility (being simple) of a submodule, the notion of ‘‘orthogonal’’ corresponds to reducibility into inequivalent simple submodules, and the notion of ‘‘identical’’ corresponds to reducibility into equivalent simple submodules.

The main result was shown to be applicable to various problems of quantum information. The tasks of cloning, broadcasting, imprinting, and eavesdropping in quantum cryptography belong to a class of problems in which extraction of information on the initial state of the system is required without introducing disturbance. The present result can naturally be applied to this class of problems, and helps to derive various conditions on the set of possible initial states for various tasks to be feasible. In addition, the result was also successfully applied to tasks such as quantum data compression and quantum teleportation, in which the extraction of the information on the initial state is not directly required. It was shown (see also Refs. [13,15]) that the optimal rates of bits and qubits for asymptotically faithful blind compression is simply equal to the Shannon or von Neumann entropy of the classical and nonclassical parts, respectively. This result also justifies the terminology of classical, nonclassical, and redundant parts in operational sense, namely, the classical part can be encoded on bits and sent through a classical channel, but the nonclassical part can be encoded only on qubits and requires shared entanglement to be sent over a classical channel.

ACKNOWLEDGMENTS

This work was supported by a Grant-in-Aid for Encouragement of Young Scientists (Grant No. 12740243) and a Grant-in-Aid for Scientific Research (B) (Grant No. 12440111) by the Japan Society for the Promotion of Science.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982); D. Dieks, Phys. Lett. **92A**, 271 (1982).
[2] H. P. Yuen, Phys. Lett. A **113**, 405 (1986).
[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[5] M. Koashi and N. Imoto, Phys. Rev. Lett. **81**, 4264 (1998).
[6] G. Lindblad, Lett. Math. Phys. **47**, 189 (1999).
[7] T. Mor, Phys. Rev. Lett. **80**, 3137 (1998).
[8] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[9] A. Peres, Phys. Rev. Lett. **77**, 3264 (1996); L. Goldenberg and L. Vaidman, *ibid.* **77**, 3265 (1996).
[10] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[11] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[12] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
[13] M. Koashi and N. Imoto, Phys. Rev. Lett. **87**, 017902 (2001).
[14] H. Barnum, P. Hayden, R. Jozsa, and A. Winter, Proc. R. Soc. London, Ser. A **457**, 2019 (2001).
[15] M. Koashi and N. Imoto, e-print quant-ph/0104001.