Catalytic quantum randomness as a correlational resource

Seok Hyung Lie and Hyunseok Jeong*
Department of Physics and Astronomy, Seoul National University, Seoul, 151-742, Korea

(Received 11 May 2021; accepted 10 September 2021; published 29 October 2021)

Catalysts are substances that assist transformation of other resourceful objects without being consumed in the process. However, the fact that their "catalytic power" is limited and can be depleted is often overlooked, especially in the recently developing theories on catalysis of quantum randomness utilizing building correlation with catalyst. In this work, we establish a resource theory of one-shot catalytic randomness in which uncorrelatedness is consumed in catalysis of randomness. We do so by completely characterizing bipartite unitary operators that can be used to implement catalysis of randomness using partial transpose. By doing so, we find that every catalytic channel is factorizable, and therefore there exists a unital channel that is not catalytic. We define a family of catalytic entropies that quantifies catalytically extractable Rényi entropies from a quantum state and show how much the degeneracy of a quantum state can boost the catalytic entropy beyond its ordinary entropy. Based on this, we demonstrate that a randomness source can be actually exhausted after a certain amount of randomness is extracted. We apply this theory to systems under superselection rules that forbids superposition of certain quantum states and find that nonmaximally mixed states can yield the maximal catalytic entropy. We discuss implications of this theory to various topics, including catalytic randomness absorption, the no-secret theorem, and the possibility of multiparty infinite catalysis.

DOI: 10.1103/PhysRevResearch.3.043089

I. INTRODUCTION

A catalyst is a substance that accelerates or initiates chemical reactions without being consumed or destroyed. This concept has been adopted in the context of quantum information for manipulation of entanglement, coherence, and realization of thermal operations. Recently, a generalized concept of catalytic randomness for state transitions has been explored [1–6]. In this generalized setting, a randomness source, a mixed quantum state that serves as a source of randomness for otherwise deterministic process, is catalytically used in the sense that its state remains unchanged after the interaction taking place. However, the randomness source, as a catalyst, is allowed to be correlated with other quantum systems in the course of interaction so that immediate recycle of the catalyst is sometimes impossible for the interaction with the very same quantum system it interacted with.

However, change of relationship affecting the usability of catalyst is never a new phenomenon in quantum information. Even in the original context of chemistry, a catalyst C catalyzing the reaction transforming compound A into substance B may not interact with B at all even though it is not physically damaged or altered. We can interpret it as that there is a "catalytic power" that used up in catalysis, and C has no catalytic power in relation to B.

An example in information theory of such phenomena is one-time pad. One-time pad is a table of random numbers that can be used for secure cryptographic communication. Note that the table itself remains intact and random for someone who never interacted with it, but a user cannot use the same table twice lest the communication becomes insecure, hence the name "one-time pad." These observations motivate the explicit identification and treatment of this relational resource being consumed in information processing processes.

In this work, we set to establish such a theory for catalytic randomness for implementing quantum channels. We identify uncorrelatedness is the resource being consumed in catalysis, and show that randomness produced in the process is extracted from such uncorrelatedness. As a result, we define a quantity called *catalytic entropy* for arbitrary quantum state, which equals to the maximal amount of entropy that can be extracted from the quantum state through catalysis. A significant consequence is that a randomness source correlated enough with the user can be *depleted*. Using randomness source can be compared to checking a book out of a library. If a reader checks out the same book multiple times because she cannot finish the book in one read, then whenever she returns the book, it should be made sure that the book is in its original state, undamaged and unspoiled. Nonetheless, as an information resource, a book can be "depleted" to a particular reader when the reader finishes reading. As long as the book itself is maintained perfectly, however, the book can be read again and again by different readers. Randomness sources including books are both a "catalyst" and a depletable resource in this sense. This perspective on randomness aligns with more conventional resource theories in quantum information science in which a resource has extensive quantity that can be produced or consumed.

*h.jeong37@gmail.com

We also generalize the theory of catalytic quantum randomness. First, we characterize the bipartite unitary operators that are still unitary after partial transposition as catalysis unitary operators. For this purpose, we show that every catalysis unitary operator is compatible with maximally mixed catalyst, and show that catalysis unitaries should have the controlled-unitary form with they are compatible with nonuniform catalysts. We also discuss about catalysts given in an already correlated form and randomness deposit through catalysis. Next, we introduce a few advantages of the approach that treats the correlation formed between the system and catalyst explicitly, including the infinite multiparty catalysis. In doing so, we show that the partial transpose of a catalysis unitary operator has an operational meaning as the recovery map that recovers the input state of the catalysis encoded in the correlation with environment.

II. NOTATIONS

We will denote the marginal state of a multipartite quantum state $\rho_{ABC\ldots}$ on the system A as ρ_A. However, the system subscripts will be omitted when it is obvious from context. Similarly, an operator with system indices that do not include the whole set of local systems implies that it only acts on those systems and acts trivially on the rest of the systems. For example, X_{AB} acting on the composite system ABC is a shorthand expression of $X_{AB} \otimes \mathbb{1}_C$. We will frequently use the von Neumann entropy of quantum state ρ defined as $S(\rho) := -\mathrm{Tr}[\rho \log_2 \rho]$. When the notation such as $S(A)_\rho$ is used, it represents the von Neumann entropy of the marginal state ρ_A of the multipartite state $\rho_{ABC\ldots}$, i.e., $S(A)_\rho = S(\rho_A)$. These two notations will be used interchangeably. Similarly Shannon entropy $H(p) := -\sum_i p_i \log_2 p_i$ and Rényi entropy [7], $H_\alpha(p) = \frac{1}{1-\alpha} \log_2 \sum_i p_i^\alpha$ are defined for probability distributions $\{p_i\}$. A quantum channel, or a quantum map, is a linear map on a operator space that that is completely positive and trace preserving. A unital quantum map is a quantum map that preserves the maximally mixed state. We will denote the dimension of the Hilbert space associated with system S as d_S from now on, with the exception that the dimension of the Hilbert space associated with the input state ρ being denoted as just d. A $d_A \otimes d_B$-dimensional Hilbert space stands for the tensor product of d_A-dimensional and d_B-dimensional Hilbert spaces.

III. MAIN RESULT

A. Catalytic randomness

What does using randomness mean, and how is it different from using other quantum resources? We intuitively know that a mixed quantum state has some randomness in it, but how is interacting with a quantum system prepared in a mixed state different from using only randomness of that system, not other physical properties? To precisely understand the meaning of randomness usage, we take an approach similar to that of resource theory for other quantum resources such as entanglement and coherence. To characterize a resource, we must define a situation where the resource is not present [8].

Assume that there exists a deterministic agent A who cannot generate randomness by oneself. Although the meaning of the term "randomness" may be vague at this point, at least we can say that, in quantum mechanics, having no power to generate randomness means the only actions one can take aside from appending auxiliary systems initialized in a pure state are unitary operations. An example of such an agent is the one in a closed system whose time evolution is governed by the Schrödinger equation, for which the time evolution is given as a unitary operator, which does not alter the entropy and, moreover, the spectrum of the quantum state of the system.

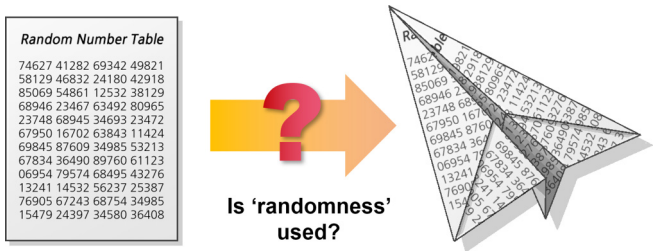

FIG. 1. What do we mean by "using randomness"? We can implement various tasks using a randomness source, but if we leave an irreversible effect on the source, then it is natural to think that some physical resources other than randomness were consumed in the process. Therefore, we accept the definition that "using randomness is extracting entropy by interacting with a mixed state without leaving detectable probabilistic effects on it."

Now, we want to provide A with a source of randomness. A typical source of randomness is a random number table. However, giving an agent a random number table and letting them do whatever they want with the table may lead to the consumption of some physical resource in the table other than randomness. For example, if we do not forbid one from leaving marks on the table or from tearing the pages of the table to make an origami (see Fig. 1), then it is hard to say that we are allowing randomness utilization only. Another key observation we can make is that a randomness source learns nothing; a one-time pad learns nothing about the message encrypted with it, and a dice rolled does not have any information about the status of the game utilizing it.

Therefore, a plausible criterion for characterizing pure randomness usage would be that, after an interaction between a user and a randomness source, the next user who is independent of the first user must be able to use the randomness source and detect no trace of the first user. It does not mean that every process involving randomness should leave the randomness source intact; it means that if the process utilized only randomness, then it must be also possible to implement the same process without altering the statistical state of the randomness source. If it is impossible to deterministically revert the effect made by the first user, then we can interpret it as that some other physical resource has been consumed in the process. As a matter of fact, sometimes it is fundamentally impossible to affect the randomness source. For example, after one person of a group of people uses some event that is unknown to all of them, say, "Whether it rained in London on November 21, 1902," as a source of randomness to implement some task, the probability of the event would stay the same for all the other people.

So far the randomness sources discussed above were all classical, but one could try to characterize randomness within

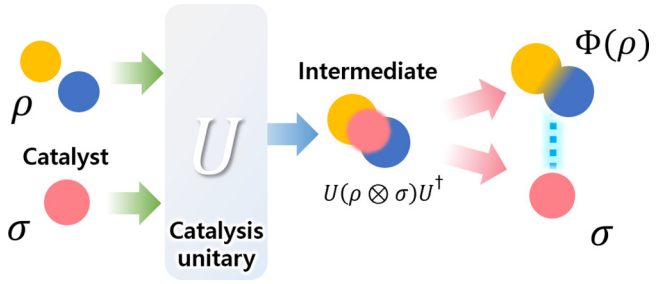

FIG. 2. Schematic depiction of catalysis process. Catalyst σ is used to implement the quantum map $\rho \mapsto \Phi(\rho)$. The catalyst stays in its original form σ as the marginal state of the global state $U(\rho \otimes \sigma)U^\dagger$ called the intermediate, after the interaction, regardless of the input state ρ. The blue dotted line depicts the correlation formed between the system and the catalyst, which indicates that the free randomness in the catalyst is used during the process.

a quantum system in a similar way. It turns out that randomness utilization of this sort fits with the framework of catalysis in quantum resource theories [1,9], the meaning of which is as follows. Suppose that A is allowed to borrow a system B called *catalyst* in the quantum state σ_B to implement a quantum map Φ. A is allowed to interact with B but should return the system B in its original state σ_B after every interaction. This can be summarized as the following two conditions (see Fig. 2). When a bipartite unitary U on systems A and B is used to implement a quantum map $\rho \mapsto \Phi(\rho)$ with a catalyst σ for arbitrary possible input state ρ, i.e.,

$$\mathrm{Tr}_B U(\rho_A \otimes \sigma_B)U^\dagger = \Phi(\rho), \quad \forall \rho. \tag{1}$$

The catalyst σ should retain its original randomness, i.e., spectrum, after the interaction regardless of the input state ρ, i.e.,

$$\mathrm{Tr}_A U(\rho_A \otimes \sigma_B)U^\dagger = V\sigma_B V^\dagger, \quad \forall \rho, \tag{2}$$

with some unitary operator V on the system B. Although the catalyst changes by some unitary operator V, any unitary operator can be reverted by a deterministic agent and it is intuitive that randomness of quantum state only depends on its spectrum, so we accept this definition. We remark that the requirement Eq. (2) is not actually requiring the state σ_B to be used indefinitely by a single user, as we will see in Sec. III E catalysts have *correlational resource* that can be depleted through randomness extraction, even though one cannot detect its effect locally.

We will call the bipartite interaction described in Eqs. (1) and (2) a *catalysis* or a *catalysis process* and a quantum map that can be implemented by catalysis a *catalytic* quantum map or channel. For example, the quantum map Φ in Eq. (1) is catalytic. We will call the bipartite unitary operator used for catalysis a *catalysis unitary* operator.

We will say that U is compatible with σ if Eq. (2) holds with $V = I$ and vice versa. Using an incompatible catalyst for a given catalysis unitary operator will lead to change of the catalyst after the interaction. For the sake of convenience, we will often use the definition of the compatibility for the cases where σ_B is an unnormalized Hermitian operator, too. Similar randomness-utilizing processes were considered in previous works, under the name noisy operations [10–12] or thermal operations. However, most studies were focused on the implementation of the transition between two fixed quantum states and the existence of a feasible catalyst for that task. Here, we are more interested in the implementation of quantum map, independently of potential input state, with a given catalyst. However, later we will see that this characterization is also relevant to state transitions, too (see Sec. IV E).

One might think that it is enough to require that no information should be leaked to the source of randomness or no change of spectrum of the state of randomness source should happen is enough. From that perspective, the condition Eq. (2) may look too strong, but actually it is equivalent to apparently weaker conditions. We refine the result of Ref. [9] to get the following equivalent conditions. All the omitted proofs of results can be found in the Appendix.

Proposition 1. For any bipartite unitary operator U on a composite system AB, the following requirements are equivalent:

$$\text{(i)} \quad \mathrm{Tr}_A U(\rho_A \otimes \sigma_B)U^\dagger = V\sigma_B V^\dagger, \quad \forall \rho,$$

with some unitary operator V on B.

$$\text{(ii)} \quad \mathrm{Tr}_A U(\rho_A \otimes \sigma_B)U^\dagger = W_\rho \sigma_B W_\rho^\dagger, \quad \forall \rho,$$

with some unitary operator W_ρ on B depending on ρ.

$$\text{(iii)} \quad \mathrm{Tr}_A U(\rho_A \otimes \sigma_B)U^\dagger = \xi_B, \quad \forall \rho,$$

for some quantum state ξ_B on B independent of ρ_A.

$$\text{(iv)} \quad \mathrm{Tr}_A U_{AB}(\psi_{RA} \otimes \sigma_B)U_{AB}^\dagger = \psi_R \otimes \xi_B,$$

for some full-rank quantum state ψ_R on quantum system R having the same dimension with A and its purification ψ_{RA} and some quantum state ξ_B on B.

In quantum thermodynamics, interaction between a system and a thermal bath is often modeled with a energy-preserving bipartite unitary operator [13]. Although it is hard to distinguish work and heat in quantum thermodynamics, one of widely accepted definition of heat is the energy exchange accompanied by changing the spectrum of the heat bath [14]. From this point of view, condition (*ii*) states that, when considering B as a thermal bath, the process is *adiabatic* in the sense that the bath undergoes no change of entropy.

Requirement (*iii*) gives a characterization that catalytic quantum map is a quantum map that can be implemented without leaking any information of input state to the ancillary system. Forbidding information leakage is important in the context of cryptography, therefore it means that the catalysis of randomness can be applied to implement protocols that require security such as private state transfer [4]. These observations put catalysis of quantum randomness in the context of various research topics including quantum thermodynamics, private quantum decoupling [15] and quantum secret sharing [16–18].

Because of Proposition 1, for every catalysis with the catalysis unitary operator U, we have corresponding unitary operator V on B in Eq. (2). We can consider a new catalysis unitary operator $(\mathbb{1}_A \otimes V_B^\dagger)U$ that completely preserves its catalyst, e.g., $\sigma \to \sigma$ while implementing the same quantum channel. We will call such a form of a catalysis unitary operator its *canonical form*.

As it is evident from Eqs. (1) and (2), catalysis of randomness inevitably forms correlation between the system and the randomness source, thus hinders the immediate reuse of the catalyst. However, this phenomenon is neither pathological nor unprecedented in the study of catalysis for the following reasons. First, a catalyst being unable to function properly with an outcome of the catalysis is not unnatural even in the original context of chemistry. For example, if a catalyst C catalyzes the reaction that turns compound X into Y, then it is trivial that C no longer has catalytic value in the interaction with Y; yet C can still function as a catalyst with another batch of X. Second, depletability of randomness is also natural considering how randomness sources behave in everyday sense. One-time pads are valuable sources of randomness in cryptography and they act as a catalyst because their probability distribution does not change after the encryption using them, nevertheless it is impossible for a single agent to reuse the same one-time pad. Still, it is possible that the same one-time pad can be reused by agents who are completely independent of the original user and the relevant participants. Finally, catalyst functioning while forming correlation with systems has been actively studied recently in the field of quantum thermodynamics and other quantum resource theories [1–6,11,13,19–25]. All of theses observations call for the extension of the meaning of "catalysis" and motivate an analysis of consumption of "catalytic power" by forming correlation with a catalyst. In other words, a resource theory of catalytic randomness is required.

We remark that a deterministic agent cannot implement irreversible measurements on a quantum system. Thus, "quantum randomness" discussed in this work is different from the randomness generated by measuring a quantum system [26], as measurement outcomes are classical randomness, in a sense, once they are recorded on a classical medium, after all. The framework of this work is more concerned about utilizing randomness within a classical/quantum system independently of the origin of the randomness. We aim to explore the nature of pure randomness utilization in classical and quantum regime, and leave the study of true nature and origin of randomness in respective framework to be discussed elsewhere (consult Ref. [26] for more information on randomness in classical and quantum mechanics).

To develop a resource theoretical approach to catalytic randomness, we first need to identify the "standard currency" of the given resource. For example, in the resource theory of entanglement, a maximally entangled state is universal in the sense in can be used to perform almost every useful task that can be done with an entangled state. A natural candidate of such a standard unit of randomness is a maximally mixed state. Therefore, we first show that every catalysis unitary operator is compatible with the maximally mixed states. It means that for arbitrary catalysis, even when one replaces the catalyst with the maximally mixed state, it will still be a catalysis.

Proposition 2. A catalysis unitary operator U is compatible with a catalyst σ if and only if $[U, \mathbb{1} \otimes \sigma] = 0$. Thus, U is compatible with the projection onto each eigenspace of σ. Furthermore, every catalysis unitary operator is compatible with the maximally mixed catalyst.

Proposition 2 shows that any catalytic map Φ implemented with a catalysis unitary operator U on $\mathcal{H}_A \otimes \mathcal{H}_B$ with a catalyst σ_B with the spectral decomposition $\sigma = \sum_i \lambda_i \Pi_i$ ($\Pi_i \Pi_j = \delta_{ij} \Pi_i$) can be decomposed into subcatalyses. To be more precise, if $\mathcal{H}_i$ is the support of Π_i, then one can decompose the Hilbert space $\mathcal{H}_B = \bigoplus_i \mathcal{H}_i$ and the catalysis unitary operator $U = \bigoplus_i U_i$ where U_i is defined on $\mathcal{H}_A \otimes \mathcal{H}_i$. Let $r_i = \mathrm{Tr}\Pi_i$ and $\pi_i = r_i^{-1}\Pi_i$. Then, we get that Φ is a convex sum of other catalytic maps that uses a maximally mixed state as its catalyst, i.e., $\Phi = \sum_i \lambda_i r_i \Phi_i$ where $\Phi_i(\rho) = \mathrm{Tr}_{\mathcal{H}_i} U_i(\rho_A \otimes \pi_i) U_i^\dagger$.

The unital maps that can be implemented with a finite dimensional quantum system prepared in the maximally mixed state as its ancillary system are known as the *exactly factorizable maps* [27,28], which is in turn a special case of more general *factorizable maps*, whose ancillary systems can be represented with a (possibly infinite dimensional) von Neumann algebra. The catalytic maps Φ_i defined above are therefore factorizable maps, but, since the set of factorizable maps is known to be convex, we can see that arbitrary catalytic map is also factorizable. However, since there are nonfactorizable unital maps [28], we get the following results.

Theorem 3. Not every unital map is catalytic.

Theorem 3 solves an open problem introduced in Ref. [9], which asked the exact inclusion relation of the set of unital maps and the set of catalytic maps. In light of Proposition 1, it follows that there is a unital quantum map that must leak some information of the input system to *whatever* system coupled with the input system to implement the quantum map. This result is rather surprising, because even the depolarizing map, which completely deletes the information of input state, can be implemented without leaking any information to an ancillary system.

Using Proposition 2, we can also completely characterize the class of catalysis unitary operators.

Theorem 4. A bipartite unitary operator U on two systems A and B is a catalysis unitary operator if and only if its partial transpose U^{T_A} is also a unitary operator.

The class of bipartite unitary operators with unitary partial transpose was previously known as the bipartite unitary operators that induce unital maps regardless of ancillary state [29,30]. Theorem 4 adds an operational meaning to those bipartite unitary operators and we can see that only unital maps can be implemented through catalysis. We remark that, however, this characterization of catalysis unitary operator only applies to the case of implementation of quantum maps, not to the state transition between two specific quantum states.

On the Hilbert space associated a bipartite system, e.g., $\mathcal{H}_A \otimes \mathcal{H}_B$, we define the swapping operator $F := \sum_{ij} |i\rangle\langle j| \otimes |j\rangle\langle i|$. We remark that the partial transposes of $U^\dagger$ and FUF are also unitary operators. Therefore, it follows that a catalysis unitary operator U's inverse $U^\dagger$ and party-swapped version FUF are also catalysis unitary operators.

Examining if a randomness source is compatible with a given catalysis unitary operator is seemingly complicated, but we show that actually there is an easy method of examining the compatibility. One need not examine the invariance of the randomness source for every input as it is enough to check the case of the maximally mixed input.

Proposition 5. A randomness source σ is compatible with a catalysis unitary operator U if and only if its von Neumann entropy is preserved for the maximally mixed input state, i.e.,

$$S\left[\mathrm{Tr}_A U\left(\frac{\mathbb{1}_A}{d}\otimes\sigma_B\right)U^\dagger\right] = S(\sigma_B). \tag{3}$$

A special class of catalyses is *classical catalysis* [1,9]. In classical catalysis, the catalysis unitary operator is a controlled unitary operator which is conditioning on the eigenbasis of the catalyst. It is classical in the sense that the process "measures" the random variable of the catalyst classically and implements a deterministic process according to that random variable. In other words, a classical catalysis is a *random unitary operation* $\{U_X\}$, i.e., $\rho \mapsto \sum_x p_x U_x \rho U_x^\dagger$, with the corresponding probability distribution $p_x = \Pr(X = x)$.

In previous studies, advantages of quantum catalysts over classical catalysts have been discovered multiple times [1,3,9]. Now that we have an easy-to-check criterion, Theorem 4, for catalysis unitary operators, we could find another specific functionality of quantum catalyst in the maximally mixed state. A quantum catalyst in the d-dimensional maximally mixed state can be used to implement a random unitary operation $\{U_X\}$ followed by another random unitary operation $\{V_Y\}$, where $\Pr(X = x) = \Pr(Y = y) = \frac{1}{d}$ and $[U_x, V_y] = 0$ for all x and y, and the conditional probability matrix $\Pr(Y = y|X = x)$ is unistochastic. The implementation is simple; it suffices to just apply a local unitary operator to the catalyst between two controlled unitary operators implementing $\{U_x\}$ and $\{V_y\}$, respectively.

Note that a unistochastic matrix is a doubly stochastic matrix which is the Schur square (component-wise square of absolute value) of a unitary matrix. A special class of unistochastic matrices is the family of stochastic matrices with uniform components. Such matrix is the Schur square of the discrete Fourier transform unitary matrix $F = (F_{nm})$, whose components are given as $F_{nm} = \frac{1}{\sqrt{d}}\exp(i2\pi nm/d)$.

Corollary 6. A quantum catalyst in the d-dimensional maximally mixed state can be used to implement arbitrary two independent consecutive mutually commuting rank-d random unitary operations.

Corollary 6 generalizes the results of Ref. [1], where it was claimed that a maximally mixed state performs twice as efficient when it comes to catalytic implementation of dephasing maps, and Refs. [5,9], where the same efficiency doubling effect was shown for depolarizing maps. Corollary 6 says that a quantum catalyst in the maximally mixed state can implement two independent random unitary operations consisting of mutually commuting unitary operators each of which require a classical catalyst of the same size, thus it strengthens the qualitative statement "quantum randomness is twice as strong as classical randomness." It is still unclear, however, if a classical catalyst of double the size of a quantum catalyst can perform every task that the latter can. We leave it for the future research topics.

B. Mutual information as extracted randomness

Catalysis of quantum randomness [1,3,5] was made possible by explicitly treating randomness sources as a quantum system. On the other hand, we observed that randomness is consumed by building up correlation with the source of it. Therefore, we will generalize the explicit approach by explicitly treating the correlation with the randomness source as a bipartite quantum state.

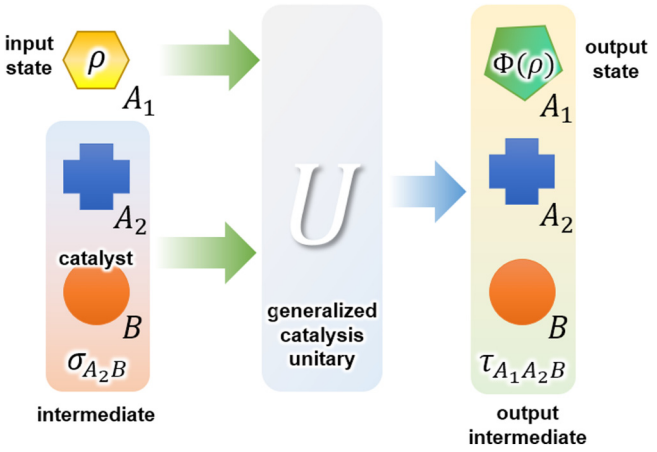

FIG. 3. Schematic depiction of generalized catalysis process. Catalyst σ_B initially correlated with system A_2 in the bipartite state σ_{A_2B} is used to implement a quantum map $\rho \mapsto \Phi(\rho)$. The catalyst stays in its original form σ_B as the marginal state of the global state $\tau_{A_1A_2B} = U(\rho_{A_1}\otimes\sigma_{A_2B})U^\dagger$ called the output intermediate, after the interaction, regardless of the input state ρ. The boxes enclosing local systems depict the correlation formed between the systems.

A resource theory should be able to describe a situation where a resourceful state that is already partially used is utilized. In Eqs. (1) and (2), only randomness sources that are not used at all were considered, i.e., only catalysts prepared in a product state were considered, but in general there could be randomness sources that have formed some correlation with the system through the previous interactions. To encompass such situations, we generalize the definition of catalysis of randomness.

Suppose again that an agent A is allowed to use a system B called catalyst in the quantum state σ_B. A is allowed to interact with B but the system B should stay in its original state σ_B after every interaction. However, assume that a catalyst σ_B has been transformed into a bipartite state σ_{A_2B} through the previous interaction with the system. We will call such a bipartite state σ_{A_2B} the *intermediate*, coined from the name of the molecules temporarily formed in chemical catalysis, and its marginal state σ_B the catalyst (see Fig. 3). Now, suppose that A is trying to implement a quantum map Φ for a (possibly unknown) new input state ρ with some tripartite unitary operator U on A_1A_2B in the following manner,

$$\mathrm{Tr}_B U(\rho_{A_1}\otimes\sigma_{A_2B})U^\dagger = \Phi(\rho)_{A_1}\otimes\sigma_{A_2}, \quad \forall\rho. \tag{4}$$

Note that σ_{A_2} is required to retain its form. This is equivalent to requiring that a newer randomness extraction should not affect the result of the previous randomness extraction. In addition to this, we require the catalysis constraint that σ_B should be left unchanged, i.e.,

$$\mathrm{Tr}_A U(\rho_{A_1}\otimes\sigma_{A_2B})U^\dagger = \sigma_B, \quad \forall\rho. \tag{5}$$

Here, both systems A_1 and A_2 are collectively denoted as A. We let $\tau_{A_1A_2B} := U(\rho_{A_1}\otimes\sigma_{A_2B})U^\dagger$ and we will refer to this

state as the output intermediate of the process. When this is done, we will say that Φ is implemented catalytically with the intermediate σ_{A_2B} and call U as the generalized catalysis unitary operator. The following result shows that the mutual information of intermediate quantifies the amount of randomness already extracted from a catalyst.

Theorem 7. The mutual information of the intermediate changes by the entropy production by the implemented quantum map, i.e., $I(A_1A_2 : B)_\tau - I(A_2 : B)_\sigma = S[\Phi(\rho)] - S(\rho)$.

Proof. We have

$$I(A_1A_2 : B)_\tau = S(A_1A_2)_\tau + S(B)_\tau - S(A_1A_2B)_\tau.$$

Since $S(A_1A_2)_\tau = S[\Phi(\rho)] + S(\sigma_{A_2})$, $S(B)_\tau = S(\sigma_B)$, and $S(A_1A_2B)_\tau = S(\rho) + S(\sigma_{A_2B})$ from the fact that unitary operators preserve the von Neumann entropy, we have

$$I(A_1A_2 : B)_\tau = S[\Phi(\rho)] - S(\rho) + I(A_2 : B)_\sigma, \tag{6}$$

from which the desired result follows. ■

We remark that Theorem 7 opens up an unexplored application of randomness sources, namely their usage as a randomness absorbent. If the intermediate was initially given as a highly correlated state, then the source can be used to implement entropy-decreasing maps by decreasing the mutual information of the intermediate. This aspect of quantum catalyst will be discussed in Sec. IV A. Hence, we can see that randomness can be both deposited into and withdrawn from the intermediate and the mutual information between the system and a catalyst quantifies the amount of randomness measured in the von Neumann entropy extracted from the catalyst.

However, note that the premise of the implementation of entropy-decreasing maps is rather different from that considered in Sec. III A; it requires the intermediate to be correlated in a *known* form. It can happen when the state transition between two quantum states with known forms is implemented. Such a situation does not happen if the whole process has started from an uncorrelated catalyst and only accepts unknown input states (see Sec. IV E).

We remark that consecutive implementation of quantum maps (say) $\Phi_1, \Phi_2, \ldots$ is actually equivalent to a single implementation of the tensor product of the aforementioned quantum maps, i.e., $\Phi_1 \otimes \Phi_2 \otimes \ldots$. Therefore, for that case, we can always assume that every intermediate σ_{AB} has the form $\sigma_{AB} = W(\rho_A \otimes \sigma_B)W^\dagger$ for some catalysis unitary operator W. It implies that one does not have to consider the generalized catalysis process when one implements only catalytic maps with an initially uncorrelated catalyst. Hence, unless otherwise mentioned, we will only consider catalytic processes, not generalized catalytic processes, in the following sections. It leaves the characterization of catalysis with arbitrarily correlated catalysts as an open problem.

On the other hand, since a unital quantum map never decreases the entropy of its input state, i.e., $S[\Phi(\rho)] - S(\rho) \geqslant 0$ for all ρ, implementing a unital map only increases the mutual information of the intermediate. Unital maps are important since the class of unital maps coincides with the class of quantum maps that never decreases the entropy of its input state and since every catalytic map is unital [9].

An interesting observation can be made. The "Rényi mutual information" $I_\alpha(A : B) := S_\alpha(A) + S_\alpha(B) - S_\alpha(AB)$ for $\alpha \geqslant 0$ formally generalized from the von Neumann mutual information has a defect that it can be negative when $\alpha \neq 1$ despite its property of vanishing for independent systems. However, for any intermediate generated from catalysis initially prepared in a product state, the Rényi mutual information is always positive, and they are the same with the Rényi entropy catalytically extracted from the catalyst. Especially it vanishes only when the intermediate is a product state, i.e., no randomness is extracted. Therefore, we can conclude that the Rényi mutual information is a valid measure of extracted randomness in the context of catalytic quantum randomness.

We remark that by implementing a quantum map Φ, simultaneously one also implements a multipartite quantum map $\mathcal{I} \otimes \Phi$, where $\mathcal{I}$ is the identity map on the systems that are not actively interacted with. We will call $S(\Phi) := \max_\rho\{S[\Phi(\rho)] - S(\rho)\}$ the maximal local entropy production of Φ and $S^G(\Phi) := \max_\rho\{S[(\mathcal{I} \otimes \Phi)(\rho)] - S(\rho)\}$ the maximal global entropy production of Φ. We similarly define their Rényi entropy counterparts, $S_\alpha(\Phi)$ and $S^G_\alpha(\Phi)$, in a similar way. Note that $S^G_\alpha \geqslant S_\alpha$ (see Sec. IV A).

The maximal entropy production always can be achieved with a pure state input. This can be shown from noting that for a general bipartite input state ρ_{AB}, there exists a purifying system E so that ρ_{ABE} is a pure state and the entropy production by Φ_A is given by $S(AB)_\tau - S(E)_\tau$ where $\tau_{ABE} = (\Phi_A \otimes \mathcal{I}_{BE})(\rho_{ABE})$. By using the Araki-Lieb inequality [31], we get $S(AB)_\tau - S(E)_\tau \leqslant S(ABE)_\tau$ where $S(ABE)_\tau$ can be also interpreted as the entropy production by Φ_A for the bipartite pure state input ρ_{ABE}.

For example, for the dephasing map $\mathcal{D}$ with respect to the computational basis, by choosing a pure state $\rho = |+\rangle\langle+|$ with $|+\rangle = \frac{1}{\sqrt{d}}\sum_i |i\rangle$, we have $\mathcal{D}(|+\rangle\langle+|) = \frac{1}{d}\mathbb{1}$, thus the maximal entropy production is achieved, i.e., $S(\mathcal{D}(|+\rangle\langle+|)) - S(|+\rangle\langle+|)| = \log_2 d$. For the depolarizing map $\mathcal{E}(\rho) := \frac{1}{d}\mathbb{1}$, by choosing $\Phi = \mathcal{I} \otimes \mathcal{E}$ and the input state $\rho = |\Psi\rangle\langle\Psi|$ with an arbitrary maximally entangled state $|\Psi\rangle$ (e.g., $|\Psi\rangle = \frac{1}{\sqrt{d}}\sum_i |ii\rangle$), we get $S((\mathcal{I} \otimes \mathcal{D})(|\Psi\rangle\langle\Psi|)) - S(|\Psi\rangle\langle\Psi|)| = 2\log_2 d$.

C. Catalytic entropies

In the previous section, we showed that the mutual information measures the amount of randomness catalytically extracted from a catalyst. A naturally following question is how to measure the maximum amount of randomness that can be catalytically extracted from a catalyst. In this section, we completely characterize the amount of entropy extractable from an arbitrary quantum catalyst. By the eigenspace decomposition of a quantum state σ we mean the decomposition of the form $\sigma = \sum_i \lambda_i \Pi_i$ with $\{\lambda_i\}$ being the eigenvalues of σ and Π_i being the orthogonal projector onto the eigenspace corresponding to λ_i such that $\Pi_i\Pi_j = 0$ if $\lambda_i \neq \lambda_j$. It was shown in Ref. [9] that uniformness or degeneracy of eigenvalues of a quantum state boosts its capability as a catalytic randomness source. It motivates us to define the average degeneracy $\Delta(\sigma)$ of quantum state σ counted in bits as $\Delta(\sigma) := \sum_i \lambda_i r_i \log_2 r_i$. For example, $\Delta(\sigma)$ is zero for a nondegenerate σ and $\Delta(\sigma)$ achieves its maximal value, $S(\sigma)$, when σ is completely uniform.

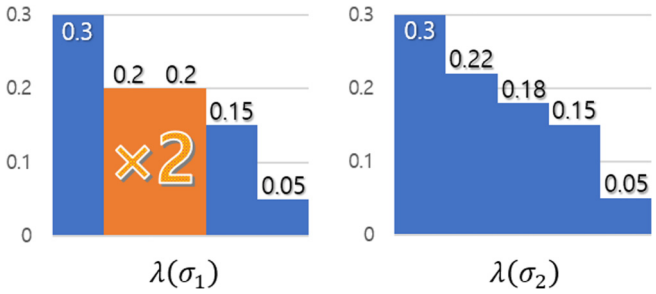

FIG. 4. Spectrums of two density matrices. Each probability p_i contributes to the catalytic entropy by $-p_i \log_2 p_i$, however, if there is degeneracy, then the same contributes by the double, i.e., $-2p_i \log_2 p_i$. Although their von Neumann entropies are very close, i.e.$|S(\sigma_1) - S(\sigma_2)| < 0.004$, their catalytic entropies differ by almost 1 bit.

In the following theorem, we show that, in addition to the von Neumann entropy of the catalyst, the average degeneracy acts as the bonus extractable entropy of the catalyst.

Theorem 8. For arbitrary randomness source σ with the eigenspace decomposition $\sigma = \sum_i \lambda_i \Pi_i$, the maximal entropy production from σ is $S(\sigma) + \Delta(\sigma)$.

Note that the maximal extractable von Neumann entropy of a quantum state σ with the eigenspace decomposition $\sigma = \sum_i \lambda_i \Pi_i$, $S(\sigma) + \Delta(\sigma)$ can be we written as

$$S^{\diamond}(\sigma) := -\sum_i \lambda_i r_i \log_2(\lambda_i / r_i), \tag{7}$$

which we will call the *catalytic (von Neumann) entropy* of the catalyst σ (see Fig. 4). This is the average of quantities $-\log_2(\lambda_i/r_i)$, which can be interpreted as the "catalytic power" of each block Π_i in the catalyst σ. This type of relation between the degeneracy and the entropy of quantum state can be extended to the min-entropy. Its natural min-entropy generalization would be

$$S^{\diamond}_{\min}(\sigma) := -\max_i \log_2(\lambda_i / r_i), \tag{8}$$

which we will call the *catalytic min-entropy* of σ. We remark that the min-entropy cannot exceed the catalytic min-entropy. Also, just as ordinary quantum Rényi entropies, we have the order relation $S^{\diamond}_{\min} \leqslant S^{\diamond}$.

In the following Theorem, we will show that this catalytic min-entropy is indeed the maximal min-entropy extractable from a given catalyst.

Theorem 9. For arbitrary randomness source σ, the maximal extractable min-entropy from σ is the catalytic min-entropy of σ, $S^{\diamond}_{\min}(\sigma)$.

In a similar way, we can define the *catalytic Rényi entropy* $S^{\diamond}_{\alpha}$ for every $\alpha \in (0,1) \cup (1,\infty)$ as

$$S^{\diamond}_{\alpha}(\sigma) := \frac{1}{1-\alpha} \log_2 \sum_i \lambda_i^{\alpha} r_i^{2-\alpha}. \tag{9}$$

Similar to the catalytic min-entropy, we can also define the catalytic max-entropy $S^{\diamond}_{\max}(\sigma) := \log_2 \sum_{i:\lambda_i>0} r_i^2$. Then,we have the order relation $S^{\diamond}_{\min} \leqslant S^{\diamond}_{\alpha} \leqslant S^{\diamond}_{\beta} \leqslant S^{\diamond}_{\max}$ for $0 < \beta < \alpha$. Like the both previously defined catalytic entropies, catalytic Rényi entropy also characterizes the maximally extractable Rényi entropy with the corresponding α.

Theorem 10. For arbitrary randomness source σ, the maximal extractable Rényi entropy from σ is the catalytic Rényi entropy of σ, $S^{\diamond}_{\alpha}(\sigma)$.

Since $\lim_{\alpha\to 1} S^{\diamond}_{\alpha} = S^{\diamond}$ and $\lim_{\alpha\to\infty} S^{\diamond}_{\alpha} = S^{\diamond}_{\min}$, Theorem 10 subsumes Theorems 8 and 9, but we gave different proofs using properties specific for each entropic quantity.

For any mixed state with the spectral decomposition $\sigma = \sum_i \lambda_i \Pi_i$ with $r_i = \mathrm{Tr}\Pi_i$, we will call the vector $(r_1, \cdots, r_n)$ the degeneracy vector of σ. Let $\|\mathbf{r}\|_2 := \sqrt{r_1^2 + \cdots + r_n^2}$ and let $t = (t_i)$ be the probability distribution formed by normalizing the squared degeneracy vector $\mathbf{r}$, i.e., $t_i := \|\mathbf{r}\|_2^{-2} r_i^2$. Then, we have the following expression with simple substitution for the catalytic Rényi entropy of σ in terms of Rényi divergence:

$$S^{\diamond}_{\alpha}(\sigma) = 2\log_2 \|\mathbf{r}\|_2 - D_{\alpha}(\lambda_i r_i \,\|\, t_i). \tag{10}$$

Here, $D_{\alpha}(p\|q) := \frac{1}{\alpha-1} \log_2 \sum_i p_i^{\alpha} q_i^{1-\alpha}$ is the Rényi divergence [32] between two probability distributions $p = (p_i)$ and $q = (q_i)$, which is nonnegative and is zero if and only if $p = q$. From this expression we get that the maximal catalytic Rényi entropy can be achieved when $\lambda_i = \|\mathbf{r}\|_2^{-2} r_i$.

Corollary 11. For a catalysis with degeneracy vector $\mathbf{r} = (r_1, \cdots, r_n)$, the maximal catalytic Rényi entropy is $2\log_2 \|\mathbf{r}\|_2$.

In previous works, it was shown that quantum maps that destroy more information require more randomness resources [5,9]. We show here that the same relation holds for the catalytic Rényi entropies.

Corollary 12. For a d-dimensional catalytic map Φ with the entanglement-assisted classical capacity $C_{EA}(\Phi)$ utilizing a catalyst σ, the following inequality holds:

$$2\log_2 d - C_{\mathrm{EA}}(\Phi) \leqslant S^{\diamond}_{\min}(\sigma). \tag{11}$$

D. Catalysis under superselection rule

From the proof structure of the previous results, the relation between the degeneracy and the entropy of catalyst follows from the relation between the decomposability of the given catalysis into subcatalyses and the entropy of catalyst. For example, every classical catalyst can be decomposed into rank-1 catalysts, therefore requires more entropy to implement the same quantum map.

To be more precise, even when we decompose a given catalyst σ more finely so that its eigenspace decomposition $\sigma = \sum_i \lambda_i \Pi_i$ need not have distinct eigenvalues for different i's, but still different $\frac{1}{r_i}\Pi_i$ are required to be orthogonal to each other and to be compatible catalysts themselves for the same catalysis unitary operator, Theorems 8–10 still hold. For instance, even when a catalyst is maximally degenerate, i.e., $\sigma = \frac{1}{d}\sum_i |i\rangle\langle i|$, if each projector $|i\rangle\langle i|$ is preserved when used instead of σ itself for the same catalysis process, then $r_i = 1$ for every i so that $S_{\alpha}(\sigma) = S^{\diamond}_{\alpha}(\sigma)$. We will still call the new $(r_1, \cdots, r_n)$ following the constraint the degeneracy vector of σ.

There are indeed situations in which there are limits on the level of degeneracy without complete specification of the form of catalysis. In a general formulation of quantum mechanics, the space spanned by the density matrices of a quantum system need not be a full matrix algebra $\mathcal{M}(\mathcal{H})$ on some Hilbert space $\mathcal{H}$, but they are in general a C^*-algebra [28,33]. A finite

dimension C^*-algebra is isomorphic to a direct sum of full matrix algebras (the Artin-Wedderburn theorem) [34,35]. It is equivalent to imposing a superselection rule that forbids superposition between a certain set of subspaces called the superselection sectors of the underlying Hilbert space [36]. It is sometimes said that an observable that has the superselection sectors as its eigenspaces is off-shell conserved [37] or superconserved [38] in the system. The tuple of the dimensions of Hilbert spaces on which the direct summands of a C^*-algebra are full matrix algebras is called the dimension vector of the C^*-algebra. For example, if a C^*-algebra $\mathcal{C}$ is isomorphic to $\bigoplus_{i=1}^{n} \mathcal{M}(\mathbb{C}^{d_i})$, then the dimension vector of $\mathcal{C}$ is $(d_1, \cdots, d_n)$.

Note that, for any catalyst σ with degeneracy vector $\mathbf{r} = (r_1, \cdots, r_m)$ in a C^*-algebra with dimension vector $\mathbf{d} = (d_1, \cdots, d_n)$, there exists a partition $f : \{1, \cdots, m\} \to \{1, \cdots, n\}$ such that $\sum_{i:f(i)=j} r_i = d_j$ for every $j \in \{1, \cdots, n\}$. Thus, if $d_i = 1$ for all i, then $r_i = 1$ is forced; hence, we say that the catalyst is classical in that case, regardless of the multiplicities of its eigenvalues.

Note that $\|\mathbf{r}\|_2 \leqslant \|\mathbf{d}\|_2$ since $\sum_{j=1}^{n} \sum_{i:f(i)=j} r_i^2 \leqslant \sum_{j=1}^{n} (\sum_{i:f(i)=j} r_i)^2$. Therefore, the catalyst achieving the maximal catalytic entropies, according to Corollary 11, has the same catalytic entropies with the maximally mixed quantum catalyst with rank $\|\mathbf{d}\|_2$. Therefore, one can interpret that $\|\mathbf{d}\|_2$ is the effective dimension of a quantum catalyst under the restriction that degeneracy vector should be $\mathbf{d}$. Moreover, it is indeed possible to implement $\|\mathbf{d}\|_2^2$-dimensional dephasing map.

Theorem 13. With a quantum catalyst σ in a C^*-algebra with dimension vector $\mathbf{d}$, the maximal dimension of a quantum system that can be catalytically dephased with σ is $\|\mathbf{d}\|_2^2$.

These observations show that the notions "the maximally mixed state" and "the state providing maximal entropy" are no longer identical under the superselection rule. For example, for an electron in atom whose azimuthal quantum number is l and magnetic quantum number m with restriction $l \leqslant l_M$, if there is a superselection rule that forbids the superposition between states with different azimuthal quantum numbers, then the state that exhibits the maximal catalytic entropy is not the maximally mixed state

$$\frac{1}{(l_M+1)^2} \sum_{l=0}^{l_M} \sum_{m=-l}^{l} |l,m\rangle\langle l,m|, \tag{12}$$

but the state with the specific mixing probability

$$\sum_{l=0}^{l_M} \frac{3(2l+1)}{(l_M+1)(2l_M+1)(2l_M+3)} \sum_{m=-l}^{l} |l,m\rangle\langle l,m|, \tag{13}$$

whose catalytic entropy is $\log_2[(l_M+1)(2l_M+1)(2l_M+3)/3]$. For the case where the catalyst is a thermal state, i.e., $\sigma = e^{-\beta H}/Z$ with some Hamiltonian H, the energy levels $\{E_i\}$ should have the form $E_i = E_\infty - 2\log_2 r_i$ with some constant energy cap E_∞.

E. Depletion of catalyst

In this section, we will show that a randomness source can be actually *depleted*. Suppose that, for a given catalyst σ, the maximal entropy production of a unital map Φ_1 is already

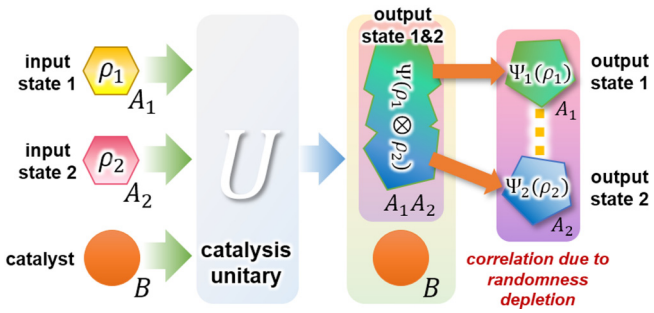

FIG. 5. Schematic depiction of depletion of randomness. When the sum of maximum entropy productions of two catalytic maps exceeds the catalytic entropy of the catalyst, their joint implementation is bound to create the correlation between the outputs of two catalytic maps, even when the input systems were prepared in a product state. As a result, two catalytic maps cannot be implemented in parallel.

$S^\diamond(\sigma)$, i.e., $S(\Psi_1) = S^\diamond(\Psi_1)$. Can we catalytically implement another unital map Ψ_2 after implementing Ψ_1, or in other words, can we implement $\Psi_1 \otimes \Psi_2$, with the catalyst σ? We answer this question negatively by proving the following result (see Fig. 5).

Theorem 14. Consider catalysis processes with the catalyst σ_B and let Ψ_1 and Ψ_2 be unital maps acting on A_1 and A_2, respectively. For arbitrary catalytical implementation of a quantum map Ψ on A_1A_2 utilizing σ_B such that $\mathrm{Tr}_{A_2} \circ \Psi = \Psi_1$ and $\mathrm{Tr}_{A_1} \circ \Psi = \Psi_2$, for every $\alpha \geqslant 0$ we have $\max_{\rho_1,\rho_2} I_\alpha(A_1 : A_2)_{\Psi(\rho_1\otimes\rho_2)} \geqslant S_\alpha(\Psi_1) + S_\alpha(\Psi_2) - S_\alpha^\diamond(\sigma)$.

Here, I_α is the Rényi mutual information discussed in Sec. III B. We remark that although there are systems with the labels A_1 and A_2 in Theorem 14, the catalysis in Theorem 14 is not the generalized catalysis introduced in Sec. III B, but the original catalysis of Eqs. (1) and (2), where the system A is simply partitioned into A_1 and A_2.

Theorem 14 implies that $\Psi_1 \otimes \Psi_2$ cannot be implemented catalytically if the sum of their maximal entropy productions exceeds the catalytic entropy of the catalysis since $\Psi_1 \otimes \Psi_2(\rho_1 \otimes \rho_2) = \Psi_1(\rho_2) \otimes \Psi_2(\rho_2)$ is a product state for arbitrary ρ_1 and ρ_2 so its Rényi mutual entropy should be zero, but Theorem 14 forbids it. By substituting $\Psi_i \mapsto \mathcal{I} \otimes \Psi_i$ for $i = 1, 2$ in Theorem 14, a useful Corollary follows.

Corollary 15. For a pair of unital maps Ψ_1 and Ψ_2 such that $S_\alpha^G(\Psi_1) + S_\alpha^G(\Psi_2) > S_\alpha^\diamond(\sigma)$ for some $\alpha \geqslant 0$, $\Psi_1 \otimes \Psi_2$ cannot be implemented catalytically with the catalyst σ.

Corollary 15 explains why it is sometimes impossible to reuse a classical catalyst even after extracting arbitrarily small von Neumann entropy from it. Consider a d-dimensional maximally mixed classical catalyst, whose catalytic Rényi entropy is $\log_2 d$ for every α. Assume that, using the catalyst, we implemented a random unitary operation $d^{-1}\sum_{i=1}^{d} U_i \cdot U_i^\dagger$ with linearly independent unitary operators $\{U_i\}_{i=1}^d$ such that every unitary operator is arbitrarily close to each other, e.g., $\|U_i - U_j\|_1 < \epsilon$ for arbitrarily small ϵ and every i and j. The Rényi entropy production for every $\alpha > 0$ by this map can be made arbitrarily close to 0 as the random unitary operation converges to the identity map with vanishing ϵ and the continuity of the Rényi entropies for $\alpha > 0$. However, as long as $\{U_i\}_{i=1}^d$ is linearly independent,

the max-entropy production by this operation is always maximal, i.e., $\log_2 d$, for maximally entangled input states, thus the catalytic max-entropy of the catalyst is depleted for every $\epsilon > 0$. Therefore, by Corollary 15, no additional catalytic map with nontrivial entropy production can be implemented with the catalyst.

IV. DISCUSSION

A. Randomness absorption of correlated catalyst

The extremal case of entropy-decreasing map is the initialization map, which maps every input state to a single pure state. An initialization map cannot be implemented with a catalyst that is uncorrelated with the system; however, it is possible with an initially correlated intermediate. The observation that the amount of randomness required to decouple a correlated state effectively measures the correlation within it was made in Ref. [39]. Catalytic utilization of correlated intermediate can be understood as a converse task. Nonetheless, surprisingly, a more correlated intermediate is not always more useful for catalytic implementation of initialization map. In fact, a highly restrictive form is required as the following Proposition shows.

Proposition 16. A d-dimensional quantum catalyst compatible for implementation of a d-dimensional initialization map should be in the maximally mixed state and be part of an intermediate with the mutual information $\log_2 d$.

One example of such an intermediate is, when d is an odd number, a d-dimensional maximally correlated classical state $\sigma_{A'B} = \frac{1}{d}\sum_{i=0}^{d-1} |i\rangle\langle i|_{A'} \otimes |i\rangle\langle i|_B$. Let the generalized catalysis unitary operator U acting on $AA'B$ be given as $U = \sum_{ijk} |j\rangle\langle i \oplus 2k|_A \otimes |i \oplus j \oplus k\rangle\langle i|_{A'} \otimes |k\rangle\langle i \oplus j|_B$. Here, $\oplus$ denotes the addition modulo d. Another extremal example is, when $d = m^2$ for some integer m, a pair of m-dimensional maximally mixed states and a m-dimensional maximally entangled pure state, i.e., $\frac{1}{m}\mathbb{1}_{A_1} \otimes |\Psi\rangle\langle\Psi|_{A_2B_2} \otimes \frac{1}{m}\mathbb{1}_{B_1}$. The generalized catalysis unitary operator consists of multiple steps. First, assign an arbitrary bipartite structure to the input system A and swap it with system A_2B_2. Next, mask the system A_2 by using B_1 as a randomness source and similarly mask the system B_2 by using A_1 as a randomness source. Examples of masking unitaries are given in Ref. [3].

Proposition 16 suggests that entropy absorption of quantum catalyst shows the dual behavior. Even if the entropy is locally decreased by catalysis, when a reference system with which the input system is correlated is introduced, the entropy of the reference-input joint system can increase. We will call this increase of entropy the global increase of entropy. Therefore, an intermediate should not only have enough free randomness but also enough room to absorb external randomness. This observation can be generalized to the following Theorem.

Proposition 17. Any quantum map that locally decreases entropy by ΔS should globally increase entropy by at least ΔS.

This result shows that a maximally correlated intermediate σ_{AB}, i.e., $I(A:B)_\sigma = 2S(B)_\sigma$, cannot be used for catalytical implementation of *any* quantum map which causes entropy change.

B. Secret-decoding map

The no-hiding theorem [40] can be restated as that the complementary channel of an constant channel is an isometry. In other words, if quantum information completely disappears from a system, then it can be deterministically retrieved from its purifications. However, it is possible to circumvent the no-hiding theorem and hide the quantum information from local parties if we allow the initial state of the ancillary system to be mixed. Such a hiding process is equivalent to catalytic implementation of constant channel.

Nevertheless, the following form of generalization of the no-hiding theorem applies to this situation, too [3]. If the joint system BC is in a pure state, then, when the whole quantum state of the system A is encoded solely into the correlation of the joint system AB (i.e., without altering the marginal state of B), it can be deterministically retrieved from the correlation of the joint system AC too. That is, it is impossible to hide a quantum state into the correlation of only one pair of quantum systems, since there is always another system the correlation with which stores the hidden quantum state. It implies that quantum information cannot be localized in the correlation of a unique pair of quantum systems.

A further generalization of this result named *the no-secret theorem*, which generalizes the complete information destruction to arbitrary degrading of quantum information, was proved in Ref. [9]. We introduce its proof here for completeness. Assume that a quantum map Φ on system A is implemented through a generalized randomness-utilizing process, i.e., no information about the input state of Φ is leaked to the ancillary system other than the information that the map is implemented, with a unitary M acting on AB and a randomness source σ in system B. σ_B transforms into τ_B after the implementation, regardless of the input state. Let C be a purification system σ_B, i.e., σ_{BC} is pure state such that $\mathrm{Tr}_C\sigma_{BC} = \sigma_B$. We input the part of a maximally entangled state Ψ_{RA} into Φ and similarly consider a purification τ_{BC} of τ_B. The marginal state on RB is $\frac{1}{d}\mathbb{1}_R \otimes \tau_B$, whose another purification is $\Psi_{RA} \otimes \tau_{BC}$. Since every purification of the same quantum state are unitarily similar on the purifying system, we acquire the existence of unitary operator V acting on AC such that $V_{AC}M_{AB}(\Psi_{RA} \otimes \sigma_{BC})M_{AB}^\dagger V_{AC}^\dagger = \Psi_{RA} \otimes \tau_{BC}$.

Considering the Choi-Jamiołkowski isomorphism, we can say that the information hidden between A and B by M_{AB} can be restored by the interaction between A and C, i.e., V_{AC}. It shows that not only the whole quantum state, but also *any* kind of quantum information encoded into the correlation of a pair of quantum systems must be able to be stored from an interaction between another pair of quantum systems. Note that the condition that no information should be leaked to a local system throughout the process is crucial. A localized information, of course, cannot be restored from another system unless it was copied beforehand.

Theorem 18 (the no-secret theorem [9]). There is no way to unitarily confine partial or whole quantum information into the correlation between a single pair of quantum systems without letting the local parties access the encoded information.

The no-secret theorem can be understood as a quantum generalization of the fact that any information encrypted with a random variable X as a key can be decrypted with any

random variable Y that is maximally correlated with X, i.e., $I(X:Y) = H(X)$. A remarkable point is that the encryption need not be perfect; Theorem 18 applies to any encryption with arbitrary level of concealing.

Theorem 18, however, merely implies the existence of the unitary operator that recovers the concealed quantum information. The characterization of catalysis unitary operator given by Theorem 4 shows what that unitary operator is. For a catalysis implemented with a catalysis unitary operator U_{AB}, the corresponding recovery map for the system AC is the partial transpose $U_{AC}^{T_B}$, since $U_{AB}\kappa_A \otimes \sigma_{BC} U_{AB}^\dagger = U_{AC}^{T_B}\kappa_A \otimes \sigma_{BC} U_{AC}^{T_B\dagger}$ as U_{AB} for any κ_A commutes with σ_B and $\sigma_{BC} = (\sqrt{\sigma_B}\otimes \mathbb{1}_C)|\Gamma\rangle\langle\Gamma|_{BC}(\sqrt{\sigma_B}\otimes\mathbb{1}_C)$ for an unnormalized maximally entangled state $|\Gamma\rangle_{BC} = \sum_i |i\rangle_B|i\rangle_C$.

C. Advantage of explicit model

A notable example of the advantage of adopting the explicit model of correlation being evident is the case where the intermediate σ_{A_2B} is a classical-quantum state, i.e., $\sigma_{A_2B} = \sum_{i=1}^N p_i|i\rangle\langle i|_{A_2}\otimes|\psi_i\rangle\langle\psi_i|_B$ with some probability distribution $\{p_i\}$. It is equivalent to the situation where a random pure state $|\psi_i\rangle$ is generated but the agent A has the perfect knowledge of B in the memory A_2. When the correlation with randomness source is treated implicitly, one may denote the state of the randomness source B as a randomly chosen but pure state $|\psi_i\rangle\langle\psi_i|$ with no randomness at all, i.e., $S(|\psi_i\rangle\langle\psi_i|) = 0$. It will render the randomness source useless even when it is used quantum mechanically. However, if one adopts the explicit model of correlation, then, for the case $N = d$ and $p_i = \frac{1}{d}$ with $|\psi_i\rangle = |i\rangle$, we can see that the randomness source still has $2S(B)_\sigma - I(A_2:B)_\sigma = \log_2 d$ bits of free randomness. One can even destroy $\log_2 d$ qubits of quantum information with this randomness source.

D. Multiparty infinite catalysis

We have seen that a catalyst has a limited power as a randomness source and once its randomness is depleted then it cannot be used for randomization. Does it mean that if the number of independent users of the same catalyst is finite, then the number of usages of the catalyst is limited? In the following, we introduce a counterexample to this hypothesis.

Suppose that there are two separated parties, A and B, who wish to implement dephasing maps with respect to the computational basis (i.e., $\{|i\rangle\}$) on d^2-dimensional quantum systems using a catalyst C in the state $\frac{1}{d}\mathbb{1}_C$ using the method given in [1]. For her first turn, A dephases a pure state that is unbiased to the computational basis, say, $|+\rangle = \frac{1}{d}\sum_{i=1}^{d^2}|i\rangle$. It results in the complete depletion of the randomness of the catalyst. After it, A hands over the catalyst to B and B implements the same dephasing map upon the same, but independently prepared state $|+\rangle$. Again, the catalyst becomes exhausted for B. The total state of ABC, which we will call the joint-intermediate, has the following form at this stage:

$$\tau_{ABC} = \frac{1}{d^4}\sum_{ijkl}|i\rangle\langle j|_A\otimes|k\rangle\langle l|_B\otimes(U_kU_iU_j^\dagger U_l^\dagger)_C, \tag{14}$$

where $\{U_i\}$ is a set of orthonormal unitary operators, i.e., $\mathrm{Tr}U_iU_j^\dagger = d\delta_{ij}$. However, when B returns the catalyst back to A, from the perspective of A, the catalyst looks "refuelled." It is because the marginal state on the system AC decoupled, i.e.,

$$\tau_{AC} = \frac{1}{d^3}\mathbb{1}_A\otimes\mathbb{1}_C. \tag{15}$$

The same logic applies to A, too. Therefore, if they repeat this process, then they can implement dephasing maps indefinitely many times.

This initialization of randomness happens because the complete depletion of randomness by B, i.e., $I(B:C)_\tau = 2\log_2 d$ leads to the complete decoupling of AC, because of the information conservation law [5]. To be concrete, the following conservation law holds for any four-partite pure state ξ_{WXYZ},

$$2S(Y)_\xi = I(X:Y)_\xi + I(Y:WZ)_\xi. \tag{16}$$

From the data-processing inequality [41] $I(Y:WZ)_\xi \geqslant I(Y:Z)_\xi$, by ignoring W. It follows the inequality $2S(Y)_\xi \geqslant I(X:Y)_\xi + I(Y:Z)_\xi$. We apply this inequality to the joint-intermediate τ_{ABC} with C being the catalyst. If B nearly depletes the randomness, i.e., $I(B:C)_\tau \geqslant 2S(C)_\tau - \epsilon$, then the randomness for A is nearly perfectly restored, i.e., $I(A:C)_\tau \leqslant \epsilon$. Note that obviously multiple users become more and more correlated as the usage of catalyst by them repeats.

The possibility of infinite catalysis with a finite number of users is a stark difference between quantum and classical catalyst. If C is a classical catalyst, then the upper bound $I(B:C)_\tau \leqslant S(C)$ forbids the monogamous argument that upper bounds the mutual information of $I(A:C)_\tau$. Indeed, as any catalysis with a classical catalyst completely preserves the each eigenstate of the catalyst, the usage of the catalyst by other agents does not alter the intermediate of an agent at all. An agent cannot use the same catalyst twice.

E. Catalytic implementation of state transition vs. quantum map

Previous studies on catalytic quantum randomness mainly focused on the transition between two specific quantum states with a correspondingly prepared catalyst. On the contrary, our main interest in this work is the implementation of quantum maps with unspecified input states, not transitions between two specific quantum states. The former approach is highly effective for characterizing fundamental properties or the conditions for state transition. For example, it was newly discovered that the von Neumann entropy emerges among the family of Rényi entropies as the only deciding factor if the catalytic transition between two specific states is possible, as the catalytic entropy conjecture, which was conjectured in Ref. [2], was recently proved by Wilming [19] using the technique introduced by Shiraishi and Sagawa [23].

The aforementioned technique is preparing a fine-tuned catalyst that is highly dependent on the initial and final states of the state transition in question. This setting, although it saturates the ultimate limit, is rather contrived from the operational perspective. It is because, since one needs different catalyst for each input and output state pair, one requires an enormous size of arsenal of catalysts for variable input and output state pair, which can easily be infinite. One should not need a different type of stove for cooking each dish; a tool

must have a certain degree of versatility. If one assumes that a catalyst is built whenever it is required, then one encounters a circular argument. How could one make a catalyst if randomness is not free? Therefore, it is more natural to treat a catalyst as a tool that takes resources to build and that one needs to return in its original form after every use.

In this setting, one starts with a given catalyst and the target map. Input states can be decided afterwards with the capability of the catalyst in mind. This is the motivation of studying the catalytic implementation of quantum maps, instead of state transitions between specific states. In that case, it is logical to assess the power of a given catalyst, which was done in this work by finding the catalytic entropy of a given catalyst.

Nevertheless, the characterization of randomness utilization of this work can be applied to state transitions, too. Following the argument of Sec. III A, we claim that a state transition $\rho \to \rho'$ can be implemented by using randomness only when it is possible to implement it without leaking information to the ancillary system. What does it mean that there is no information leakage when the initial state ρ is fixed? For any mixed state, we can consider a reference system that purifies the mixed state, and we say there is no information leakage to the ancillary system if the reference system and the ancillary system are independent after the state transition, i.e., the mutual information between them remains vanished. Consider how the channel capacity of a channel is quantified by maximizing the mutual information between a reference system that was initially maximally correlated with the input system and the output system [42]. We will call this type of state transition a *randomness utilizing state transition*.

Now, we make a technical assumption similar to that made in Ref. [2], that ρ is full-rank. A justification is that, for any quantum state, one can always find a full-rank quantum state that is arbitrarily close to the quantum state, therefore its physical relevance is not significant. After making the assumption, we can see that (iv) of Proposition 1 exactly describes this randomness utilizing state transition, thus it implies the following result.

Theorem 19. A randomness utilizing state transition $\rho \to \rho'$ with a full-rank quantum state ρ must be mediated by a catalytic map.

One of the most symbolic examples of catalytic map that is relevant to state transition is dephasing map. Dephasing map was shown to be catalytically implementable [1] and can be used for implementing state transition between two arbitrary quantum state, e.g., $\rho \to \rho'$ with majorization relation $\rho \succ \rho'$ by (quantum) Schur-Horn lemma [11,19,43,44]. However, it is till unknown if dephasing map is the most randomness-efficient method of implementing state transition. This type of usage of catalyst is not input-dependent, therefore subject to the resource theory of this work, even when the initial state is not full-rank. For example, even if one tries to dephase almost-dephased input state $0.001|+\rangle\langle+|+0.999\frac{1}{d}\mathbb{1}$ (here, $|+\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|i\rangle$) to transform it into the maximally mixed state $\frac{1}{d}\mathbb{1}$ with catalyst $\frac{1}{d}\mathbb{1}$, one cannot implement more than two times of the state transition of this type by naively implementing the tensor product of multiple dephasing maps, as the maximal entropy production exceeds the catalytic entropy of the catalyst, even if that entropy production does not actually take place. In this sense, the resource theory of randomness for quantum maps developed in this work encompasses state transitions, too.

V. CONCLUSION AND OPEN PROBLEMS

The correlational resource theory of randomness developed in this paper is distinctly different from conventional resource theories with convex free state sets and free operations that preserve the free state set. It is because of the concavity of the set of states without randomness, namely, pure states and the dynamic property of the results of randomness utilization, namely, catalytic maps. Unlike many other quantum resources, in general, randomness increases when one probabilistically mixes two quantum states. It renders the resource theory of randomness out of the scope of recently developed general resource theory, in which it is often assumed that the free state set is convex [45–47]. In many resource theories, the outcome of manipulation of a resourceful quantum state is still a quantum state, for example, a partially entangled state can be made from a maximally entangled state through LOCC (local operation and classical communication), however, in the correlational resource theory of randomness, the outcome is a dynamic process, a quantum map, that does not have a static quantum state expression unless an input state is specified. Nevertheless, we introduced a measure of maximally extractable randomness, the catalytic entropies, and a measure of extracted randomness, the mutual information to establish a correlation resource theory of quantum randomness. This correlational aspects of quantum resources are getting more attention in recent years [20,48], and we anticipate that exploring this direction further will enrich the resource theory of quantum resources.

In this paper, we have seen that the maximally extractable randomness from an arbitrary mixed quantum state depends on the degeneracy of the state and can be quantified by the measure we defined in this work, the catalytic entropy. We highlighted an often overlooked fact that forming correlation with a catalyst depletes the useful randomness within it, by explicitly treating the correlation as a bipartite quantum state. We also gave an operational meaning associated with the partial transpose of bipartite unitary operators and showed that it works as the recovery operator of a catalysis unitary operator whose existence is guaranteed by the no-secret theorem.

This work opens up a broad field of research. We obtained a characterization of catalysis unitary operator for initially decoupled catalyst, however, the characterization for initially correlated catalyst is still an open problem. A second open problem is to find the "catalytic entropy of formation" of quantum maps, i.e., for a quantum map $\mathcal{N}$, find $S_\alpha^F(\mathcal{N}) := \min_\sigma S_\alpha^\diamond(\sigma)$ where the minimization is over the catalysts that can be used for catalytic implementation of $\mathcal{N}$. As the maximal entropy production of channel can be understood as the counterpart of one-shot distillable entanglement of entanglement theory because they correspond to the maximum extractable amount of resource from a given resource, it is not surprising that $S_\alpha^G(\mathcal{N}) \leqslant S_\alpha^F(\mathcal{N})$ holds. A natural conjecture is that there is no "bound randomness," randomness that is used to implement a catalytic map that cannot be extracted,

just as there is no bound coherence in coherence theory [49]. It can be formulated as $S_\alpha^G(\mathcal{N}) = S_\alpha^F(\mathcal{N})$, but it is known that there are finite-dimensional catalytic maps whose maximum entropy production is naturally finite, that require infinite dimensional ancillary systems [50], therefore it implies that there is bound randomness. This surprising asymmetry calls for deeper exploration of the nature of quantum randomness.

Another interesting problem worth attention is solving the problem of discontinuity of the catalytic entropies. Since the catalytic entropies defined in this paper depend on the degeneracy of a quantum state, they are sensitive to infinitesimal change of the quantum state. It is understandable considering the requirement of exact preservation of catalyst, which is often assumed in research on catalysis of quantum resources because of the issue of embezzlement [13]; nevertheless, it is worthwhile to explore the theory of approximate catalysis of randomness and formulate a continuous version of the catalytic entropies so that the theory is robust to noises.

ACKNOWLEDGMENTS

This work was supported by National Research Foundation of Korea grants funded by the Korea government (Grants No. 2019M3E4A1080074, No. 2020R1A2C1008609, and No. 2020K2A9A1A06102946) via the Institute of Applied Physics at Seoul National University and by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (Grants No. IITP-2021-2020-0-01606 and No. IITP-2021-0-01059).

APPENDIX: PROOFS OF RESULTS

1. Proof of Proposition 1

Proof. $(i) \Rightarrow (ii)$ is trivial. $(ii) \Rightarrow (i)$ can be proved as follows. Consider a convex combination of two arbitrary inputs ρ_1 and ρ_2, i.e., $\tau = \frac{1}{2}(\rho_1 + \rho_2)$. Then, from the invariance of the von Neumann entropy under unitary transformation, $S(\sigma) = S(W_\tau \sigma W_\tau^\dagger) = S(W_{\rho_1} \sigma W_{\rho_1}^\dagger) = S(W_{\rho_2} \sigma W_{\rho_2}^\dagger)$. Therefore, we have $S(W_\tau \sigma W_\tau^\dagger) = \frac{1}{2}[S(W_{\rho_1} \sigma W_{\rho_1}^\dagger) + S(W_{\rho_2} \sigma W_{\rho_2}^\dagger)]$. Note that, from the linearity of (ii) of Proposition 1 in the input state ρ, it follows that $W_\tau \sigma W_\tau^\dagger = \frac{1}{2}(W_{\rho_1} \sigma W_{\rho_1}^\dagger + W_{\rho_2} \sigma W_{\rho_2}^\dagger)$. Therefore, from the saturation condition of the concavity of the von Neumann entropy [51], it follows that $W_{\rho_1} \sigma W_{\rho_1}^\dagger = W_{\rho_2} \sigma W_{\rho_2}^\dagger$. The equivalence of (i) and (iii) was shown in Ref. [9]. The equivalence between (iii) and (iv) follows from the fact that $\psi_R^{-1/2} \psi_{RA} \psi_R^{-1/2}$ is an unnormalized maximally entangled state and the Choi-Jamiołkowski isomorphism [52,53]. By multiplying (iv) by $\psi_R^{-1/2}$ from both sides, one can check that (iv) is the Choi matrix expression of (iii). ∎

2. Proof of Proposition 2

Proof. The following lemma was first proved as a special case more general result for von Neumann algebra theory [9,54]. Here we give a more elementary proof.

Lemma 20. Let Φ be a unital channel on a finite dimensional Hilbert space $\mathcal{H}$ given as $\Phi(\rho) := \sum_i K_i \rho K_i^\dagger$. If Φ fixes a positive Hermitian operator $\sigma > 0$ on $\mathcal{H}$, i.e., $\Phi(\sigma) = \sigma$, then Φ also fixes the projector onto each eigenspace of σ. Furthermore, each projector commutes with each Kraus operator K_i of Φ regardless of the choice of Kraus operators.

Proof. Without loss of generality, we can assume that σ has at least two different eigenvalues. Let λ_i be the ith largest eigenvalue of σ with Π_i being the projector onto the corresponding eigenspace. We first prove that Φ fixes the projector Π_m onto the eigenspace corresponding to the smallest eigenvalue λ_m of σ. It will prove the desired lemma since, then, Φ also fixes $\sigma + \|\sigma\| \Pi_m$ whose smallest eigenvalue is the second smallest eigenvalue of σ and the same conclusion can be drawn about $\sigma + \|\sigma\| \Pi_m$. First, let $|\psi\rangle$ be an arbitrary eigenvector of σ corresponding to λ_m. We conjugate $\Phi(\sigma) = \sigma$ with $|\psi\rangle$ to get the following equation:

$$\lambda_m = \sum_i \langle\psi|\Phi(\Pi_i)|\psi\rangle \lambda_i. \tag{A1}$$

Here, $\{\langle\psi|\Phi(\Pi_i)|\psi\rangle\}_{i=1}^m$ forms a probability distribution since $\sum_i \Pi_i = \mathbb{1}$ and Φ is unital. Therefore, the right-hand side of Eq. (A1) is an average of $\{\lambda_i\}$, which is strictly larger than λ_m whenever $\langle\psi|\Phi(\Pi_m)|\psi\rangle < 1$. Therefore, we have $\langle\psi|\Phi(\Pi_m)|\psi\rangle = 1$. Since this result holds for arbitrary eigenvector $|\psi\rangle$ corresponding λ_m, we have $\Phi(\Pi_m) = \Pi_m \oplus P$ for some $P \geqslant 0$, but since $\mathrm{Tr}\Phi(\Pi_m) = \mathrm{Tr}(\Pi_m)$, we have $\Phi(\Pi_m) = \Pi_m$.

Let $|\psi\rangle$ and $|\phi\rangle$ be eigenvectors corresponding to distinct eigenvalues λ_r and λ_s of σ. Then we have

$$\langle\psi|\Phi(|\phi\rangle\langle\phi|)|\psi\rangle \leqslant \langle\psi|\Pi_s|\psi\rangle = 0, \tag{A2}$$

so we have $\langle\psi|\Phi(|\phi\rangle\langle\phi|)|\psi\rangle = 0$ but $\langle\psi|\Phi(|\phi\rangle\langle\phi|)|\psi\rangle = \sum_i \langle\psi|K_i|\phi\rangle\langle\phi|K_i^\dagger|\psi\rangle = \sum_i |\langle\psi|K_i|\phi\rangle|^2$. It implies that $\langle\psi|K_i|\phi\rangle = 0$ for every i, which implies that $[\Pi_i, K_j] = 0$ for every i and j. ∎

Lemma 20 yields the following result. Without loss of generality, we assume that the catalysis unitary operator U is in its canonical form. Consider the quantum channel T defined as $T(\tau) := \mathrm{Tr}_A U(\frac{1}{d}\mathbb{1} \otimes \tau)U^\dagger$. Note that T is a unital channel that also fixes σ. Therefore, if $\{|s\rangle\}$ is a basis on A, then $\frac{1}{\sqrt{d}}(\langle s| \otimes \mathbb{1})U(|r\rangle \otimes \mathbb{1})$, Kraus operators of T, commute with Π_i, arbitrary projector onto one of eigenspaces of σ. Therefore, the catalysis unitary operator U itself also commutes with every $\mathbb{1} \otimes \Pi_i$. It is equivalent to $[U, \mathbb{1} \otimes \sigma] = 0$. It implies that Π_i are also compatible with U since

$$\lambda_i \mathrm{Tr}_A U(\rho \otimes \Pi_i)U^\dagger = \mathrm{Tr}_A U(\rho \otimes \Pi_i \sigma \Pi_i)U^\dagger \tag{A3}$$

$$= \Pi_i \mathrm{Tr}_A U(\rho \otimes \sigma)U^\dagger \Pi_i \tag{A4}$$

$$= \Pi_i \sigma \Pi_i = \lambda_i \Pi_i, \tag{A5}$$

for arbitrary ρ. By the linearity, it follows that $\sum_i \Pi_i = \mathbb{1}_B$ is also compatible with U. ∎

3. Proof of Theorem 4

Proof. First, assume that $U : \mathcal{H}_{AB} \to \mathcal{H}_{AB}$ a unitary operator whose partial transpose U^{T_A} is also unitary. We define a unnormalized maximally entangled state on system A and its copy A' as $|\Gamma\rangle := \sum_i |ii\rangle_{AA'}$. Then, for any quantum state ρ_A

on system A,

$$\mathrm{Tr}_A U\left(\rho_A \otimes \frac{1}{d_B}\mathbb{1}_B\right)U^\dagger \tag{A6}$$

$$= \langle\Gamma|_{AA'} U_{AB}\left(\rho_A \otimes \frac{1}{d_B}\mathbb{1}_B\right)U_{AB}^\dagger|\Gamma\rangle_{AA'} \tag{A7}$$

$$= \langle\Gamma|_{AA'} U_{A'B}^{T_A}\left(\rho_A \otimes \frac{1}{d_B}\mathbb{1}_B\right)U_{A'B}^{T_A\dagger}|\Gamma\rangle_{AA'} \tag{A8}$$

$$= \mathrm{Tr}_A\left(\rho_A \otimes \frac{1}{d_B}\mathbb{1}_B\right) = \frac{1}{d}\mathbb{1}_B. \tag{A9}$$

In the first equality, the fact that $\langle\Gamma|_{AA'}X_A|\Gamma\rangle_{AA'} = \sum_i \langle i|_A X_A|i\rangle_A = \mathrm{Tr}X$ for any operator on A is used. In the second equality, we used the property of $|\Gamma\rangle$ that $(\mathbb{1}_{A'}\otimes O_A)|\Gamma\rangle = (O_{A'}^T \otimes \mathbb{1}_A)|\Gamma\rangle$ for any operator O. In the third equality, $U_{A'B}^{T_A}$ and $U_{A'B}^{T_A\dagger}$ canceled each other as $U_{A'B}^{T_A}$ is unitary by the assumption. Therefore, U is the catalysis unitary operator for a catalysis that uses $\frac{1}{d_B}\mathbb{1}_B$ as the catalyst.

Conversely, assume that U is the catalysis unitary operator of a catalysis that uses an arbitrary quantum state σ as its catalyst. From Proposition 2, we can assume that $\sigma = \frac{1}{d_B}\mathbb{1}$. We input $|\Gamma\rangle_{AA'}$ into the catalysis. If we trace out the system A after applying U to A and B, then we get $U^{T_A}(\mathbb{1}_{A'}\otimes \frac{1}{d_B}\mathbb{1}_B)U^{T_A\dagger} = \frac{1}{d_B}U^{T_A}U^{T_A\dagger}$ for a similar reason with that of the previous case. However, this state should be $\mathrm{Tr}_A[(\mathbb{1}_{A'}\otimes U)|\Gamma\rangle\langle\Gamma|_{AA'}\otimes\frac{1}{d_B}\mathbb{1}_B(\mathbb{1}_{A'}\otimes U^\dagger)] = \mathbb{1}_{A'}\otimes\frac{1}{d_B}\mathbb{1}_B$ since the catalyst should remain unchanged regardless of the input state [3]. This proves that U^{T_A} is unitary. ■

4. Proof of Proposition 5

Proof. Consider the system A is initially a part of a maximally entangled state $|\Phi\rangle_{RA} = \frac{1}{\sqrt{d}}\sum_{i=1}^d |ii\rangle_{RA}$ whose marginal state on A is $\frac{1}{d}\mathbb{1}_A$. The catalysis condition Eq. (2) is satisfied if and only if RB is in a product state after applying U to AB. Note that the mutual information $I(R:B) = S(R)+S(B)-S(RB)$ is zero if and only if the composite system RB is in a product state. Since the system R does not participate in the interaction, R stays in the maximally mixed state, i.e., $S(R) = \log_2 d$. The composite system RB is in $U^{T_A}(\frac{\mathbb{1}_R}{d}\otimes\sigma_B)U^{T_A\dagger}$ and $U_{RB}^{T_A}$ is also a unitary operator, hence $S(RB) = \log_2 d + S(\sigma)$. Therefore, $I(R:B) = S(B)-S(\sigma)$ and $S(B) = S(\mathrm{Tr}_A U(\frac{\mathbb{1}}{d}\otimes\sigma_B)U^\dagger)$, we get the wanted result. ■

5. Proof of Theorem 8

Proof. Consider a catalytic map Φ using σ as a catalyst given as

$$\Phi(\rho) = \mathrm{Tr}_B U(\rho_A\otimes\sigma_B)U^\dagger. \tag{A10}$$

It follows that $[U, \mathbb{1}_A\otimes\sigma_B] = 0$, which was first proved in Ref. [9], from Proposition 2. Therefore, by letting $U_i := (\mathbb{1}_A\otimes\Pi_i)U(\mathbb{1}_A\otimes\Pi_i)$, we can see that each U_i is a unitary operator on $\mathrm{supp}(\mathbb{1}_A\otimes\Pi_i)$. It allows us to decompose Φ into the following form:

$$\Phi(\rho) = \sum_i \lambda_i r_i \mathrm{Tr}_B U_i(\rho_A\otimes\pi_i)U_i^\dagger, \tag{A11}$$

where $\pi_i := \frac{1}{r_i}\Pi_i$. Thus, Φ can be considered a probabilistic mixture of subchannels, i.e., $\Phi = \sum_i \lambda_i r_i \Phi_i$, where $\Phi_i(\rho) := \mathrm{Tr}_B U_i(\rho_A\otimes\pi_i)U_i^\dagger$. Note that $\sum_i \lambda_i r_i = 1$. Since each Φ_i is a catalysis using a uniform catalyst, each of them can produce entropy up to $2\log_2 r_i$. Now, for arbitrary pure state input ϕ, the entropy production by Φ is given by $S[(\mathcal{I}\otimes\Phi)(\phi)]$, which is upper bounded by $H(\lambda_i r_i) + \sum_i \lambda_i r_i S[(\mathcal{I}\otimes\Phi_i)(\phi)]$. The latter terms is, in turn, upper bounded by $2\sum_i \lambda_i r_i \log_2 r_i$. Therefore, we get the upper bound $H(\lambda_i r_i) + 2\sum_i \lambda_i r_i \log_2 r_i = S(\sigma) + \sum_i \lambda_i r_i \log_2 r_i$.

We will show that this upper bound is indeed achievable. First we let n be the number of different eigenvalues of σ and R be the least common multiple of all r_i^2. Suppose that the system A is composed of two systems, n-dimensional A_1 and R-dimensional A_2. Similarly, we consider their reference systems E_1 and E_2 with the same dimensions. We define the following entangled state:

$$|\Psi\rangle_{AE} = \frac{1}{\sqrt{nR}}\sum_{i=1}^n\sum_{j=1}^R |ij\rangle_{A_1A_2}\otimes|ij\rangle_{E_1E_2}.$$

Next, consider the following unitary operator U acting on A and B:

$$U = \sum_{i=1}^n\sum_{j=1}^{r_i^2} V_{A_1 i}\otimes P_{A_2 j}^{(i)}\otimes W_{Bj}^{(i)}. \tag{A12}$$

Here, $P_j^{(i)}$ are mutually orthogonal projectors satisfying $\mathrm{Tr}P_j^{(i)} = R/r_i^2$ on A_2 satisfying $\sum_j P_j^{(i)} = \mathbb{1}_{A_2}$ for all i. Also, $\{V_m\}$ and $\{W_m^{(i)}\}$ are the sets of orthogonal unitary operators on, respectively, A_1 and $\mathrm{supp}\Pi_i$ satisfying $\Pi_i W_m^{(i)}\Pi_i = W_m^{(i)}$. One can check that $U^\dagger U = UU^\dagger = \mathbb{1}_{AB}$. The catalytic map Φ defined in such a way increases the entropy of the pure input state Ψ_{AE} by $H(\lambda_i r_i) + 2\sum_i \lambda_i r_i \log_2 r_i = S(\sigma) + \sum_i \lambda_i r_i \log_2 r_i$. ■

6. Proof of Theorem 9

Proof. Consider an arbitrary catalysis Φ whose catalyst is σ. We employ the same decomposition of $\Phi = \sum_i \lambda_i r_i \Phi_i$ in the proof of Theorem 8. The following Lemma will be helpful for the proof.

Lemma 21. Let a quantum state ρ be a convex sum of other quantum states, i.e., $\rho = \sum_i p_i\rho_i$. Then we have

$$S_{\min}(\rho) - S_{\min}(\rho_i) \leqslant -\log_2 p_i$$

for every i.

It follows from the facts that $2^{-S_{\min}(\rho)} = \max_{|\psi\rangle}\langle\psi|\rho|\psi\rangle$ and that, for $|\phi\rangle$ such that $2^{-S_{\min}(\rho_i)} = \langle\phi|\rho_i|\phi\rangle$, $p_i 2^{-S_{\min}(\rho_i)} \leqslant \sum_i p_i\langle\phi|\rho_i|\phi\rangle = \langle\phi|\rho|\phi\rangle \leqslant \max_{|\psi\rangle}\langle\psi|\rho|\psi\rangle = 2^{-S_{\min}(\rho)}$.

For arbitrary bipartite state ϕ, we apply this Lemma by substituting $\rho = (\mathcal{I}\otimes\Phi)(\phi)$, $\rho_i = (\mathcal{I}\otimes\Phi_i)(\phi)$ and $p_i = \lambda_i r_i$. Now, as each Φ_i is a catalysis with the corresponding catalyst π_i, from the weak subadditivity of Rényi entropy [55], we have

$$S_{\min}[(\mathcal{I}\otimes\Phi_i)(\phi)] - S_{\max}(\pi_i) \leqslant S_{\min}(\pi_i).$$

However, since the catalyst π_i is uniform, we have $S_{\min}(\pi_i) = S_{\max}(\pi_i) = \log_2 r_i$, thus an upper bound $S_{\min}[(\mathcal{I}\otimes\Phi_i)(\phi)] \leqslant$

$2\log_2 r_i$ follows. Combining all the results, we have

$$S_{\min}[(\mathcal{I}\otimes\Phi)(\phi)] \leqslant -\log_2(\lambda_i/r_i).$$

This result holds for every i and pure state ϕ, so we get

$$\max_{\phi} S_{\min}[(\mathcal{I}\otimes\Phi)(\phi)] \leqslant -\max_i \log_2(\lambda_i/r_i), \tag{A13}$$

where the left-hand side can be interpreted as the maximal min-entropy production on pure states by Φ. We claim that, from Lemma 21, it follows that actually the maximal min-entropy production can be achieved with a pure state input. It can be shown by substituting $\rho = (\mathcal{I}\otimes\Phi)(\tau)$, where τ is an arbitrary (possibly mixed) input state, and $\rho_i = (\mathcal{I}\otimes\Phi)(\tau_i)$, where $\tau = \sum_i t_i\tau_i$ is the spectral decomposition of τ so that each τ_i is a pure eigenstate of τ corresponding to the eigenvalue t_i and $p_i = t_i$. By picking the index k such that $t_k = 2^{-S_{\min}(\tau)}$ and using the fact that $S_{\min}[(\mathcal{I}\otimes\Phi)(\tau_k)] \leqslant \max_\phi S_{\min}[(\mathcal{I}\otimes\Phi)(\phi)]$ where the maximization is over every pure state ϕ so that the right-hand side is the maximal min-entropy production of Φ on pure state inputs, we get the wanted result.

Conversely, the same $|\Psi\rangle$ and U of the proof of Theorem 8 achieves the maximal min-entropy extraction of $-\max_i \log_2(\lambda_i/r_i)$ as the spectrum of the output state of the process is $\{\lambda_i/r_i\}$. ■

7. Proof of Theorem 10

Proof. The proof is basically identical with that of Theorem 8, except that we use the facts [56] that

$$(\mathcal{I}\otimes\Phi)(\phi) = \sum_i \lambda_i r_i (\mathcal{I}\otimes\Phi_i)(\phi) \tag{A14}$$

$$\succ \bigoplus_i \lambda_i r_i (\mathcal{I}\otimes\Phi_i)(\phi), \tag{A15}$$

and that for each i, $(\mathcal{I}\otimes\Phi_i)(\phi) \succ \frac{1}{r_i^2}\mathbb{1}_{r_i^2}$, where $\mathbb{1}_{r_i^2}$ is a projector with rank r_i^2. Here, $\oplus$ operation is the direct sum operation which can be interpreted in terms of tensor product as $\bigoplus_i O_i = \sum_i |i\rangle\langle i|\otimes O_i$ for a set of operators $\{O_i\}$ with an orthonormal basis $\{|i\rangle\}$. The latter majorization relation follows from the fact that the rank of each $(\mathcal{I}\otimes\Phi_i)(\phi)$ is upper bounded by r_i^2 from the triangular inequality of the max-entropy. From the Schur concavity of Rényi entropy, we have $S_\alpha[(\mathcal{I}\otimes\Phi)(\phi)] \leqslant S_\alpha(\bigoplus_i \lambda_i r_i^{-1}\mathbb{1}_{r_i^2}) = \frac{1}{1-\alpha}\log_2\sum_i \lambda_i^\alpha r_i^{2-\alpha}$. Again, the maximal entropy extraction is achievable with pure states since for any mixed state input ρ with the spectral decomposition $\rho = \sum_i a_i\phi_i$, we have

$$(\mathcal{I}\otimes\Phi)(\rho) = \sum_i a_i(\mathcal{I}\otimes\Phi)(\phi_i) \tag{A16}$$

$$\succ \bigoplus_i a_i(\mathcal{I}\otimes\Phi)(\phi_i) \succ \bigoplus_i a_i\left(\bigoplus_j \lambda_j r_j^{-1}\mathbb{1}_{r_j^2}\right) \tag{A17}$$

$$= \sum_i a_i|i\rangle\langle i|\otimes\left(\bigoplus_j \lambda_j r_j^{-1}\mathbb{1}_{r_j^2}\right). \tag{A18}$$

Note that $S_\alpha(\sum_i a_i|i\rangle\langle i|) = S_\alpha(\rho)$. Repeatedly, from the Schur concavity of S_α, it follows that $S_\alpha[(\mathcal{I}\otimes\Phi)(\rho)] \leqslant S_\alpha[(\sum_i a_i|i\rangle\langle i|)\otimes(\bigoplus_j \lambda_j r_j^{-1}\mathbb{1}_{r_j^2})] = S_\alpha(\rho) + S_\alpha^\diamond(\sigma)$, i.e., the Rényi entropy production by Φ on ρ, $S_\alpha[(\mathcal{I}\otimes\Phi)(\rho)] - S_\alpha(\rho)$ is upper bounded by $S_\alpha^\diamond(\sigma)$.

Conversely, this bound can be achieved with the same example in the proof of Theorem 8. ■

8. Proof of Corollary 12

Proof. Consider the decomposition of Φ of the from of Eq. (A11), which we re-express as $\Phi = \sum_i \lambda_i r_i \Phi_i$. By denoting the entanglement-assisted classical capacity of Φ_i by C_i, we have the following inequality [5]:

$$C_i - C_{\mathrm{EA}}(\Phi) \leqslant -\log_2\lambda_i r_i. \tag{A19}$$

However, from the proof of Theorem 8, it follows that each C_i is d-dimensional catalysis utilizing the catalyst π_i, we have the following inequality [9]:

$$2(\log_2 d - \log_2 r_i) \leqslant C_i. \tag{A20}$$

From these two inequalities we get the following relation:

$$2\log_2 d - C_{\mathrm{EA}}(\Phi) \leqslant -\log_2(\lambda_i/r_i). \tag{A21}$$

By maximizing $\log_2 r_i$ over i we get $2\log_2 d - C_{\mathrm{EA}}(\Phi) \leqslant \Delta_{\max}(\sigma) - \log_2\lambda_i$. As it holds for every i, we get the wanted result. ■

9. Proof of Theorem 13

Proof. We assume that the catalyst σ has the eigenspace decomposition $\sigma = \|\mathbf{d}\|_2^{-1}\sum_m d_m\Pi_m$ with $\mathrm{Tr}\Pi_m = d_m$. Let $S_m := \sum_{k=1}^{m-1} d_k^2$ with $S_1 := 0$ and $\|\mathbf{d}\|_2^2\otimes d_m$-dimensional unitary operator W_m be defined as $W_m := d_m^{-1/2}\sum_{i,j=0}^{d_m-1}\omega_m^{ij}Z^{S_m+id_m+j}\otimes|m_i\rangle\langle m_j|$, where ω_m is the d_mth root of unity and $\{|m_i\rangle\}$ is an orthonormal basis of the support of Π_m. Note that each W_m is a catalysis unitary operator for the catalyst $d_m^{-1}\Pi_m$ that implements the random unitary map $\Phi_m(\rho) := d_m^{-2}\sum_{k=0}^{d_m^2-1} Z^{S_m+k}\rho Z^{-S_m-k}$. Then $\sum_m W_m$ is a catalysis unitary operator on $\|\mathbf{d}\|_2^2\otimes\|\mathbf{d}\|_1$-dimensional space that implements a convex sum of Φ_m, i.e., $\Phi(\rho) = \|\mathbf{d}\|_2^{-2}\sum_m d_m^2\Phi_m(\rho) = \|\mathbf{d}\|_2^{-2}\sum_{k=1}^{\|\mathbf{d}\|_2^2} Z^k\rho Z^{-k}$, which is the $\|\mathbf{d}\|_2^2$-dimensional dephasing map with respect to the eigenbasis of Z. ■

10. Proof of Theorem 14

Proof. We first let ρ_i be a quantum state that achieves $S_\alpha(\Psi_i) = S_\alpha[\Psi_i(\rho_i)] - S_\alpha(\rho_i)$ for $i = 1, 2$ and let $\Delta\mathcal{S}_\alpha = S_\alpha(\Psi_1) + S_\alpha(\Psi_2) - S_\alpha^\diamond(\sigma)$. Then, we get, omitting the subscript, i.e., $I_\alpha(A_1:A_2) = I_\alpha(A_1:A_2)_{\Psi(\rho_1\otimes\rho_2)}$,

$$\begin{aligned} &I_\alpha(A_1:A_2)\\ &= S_\alpha[\Psi_1(\rho_1)] + S_\alpha[\Psi_2(\rho_2)] - S_\alpha[\Psi(\rho_1\otimes\rho_2)]\\ &= S_\alpha(\Psi_1) + S_\alpha(\Psi_2) + S_\alpha(\rho_1\otimes\rho_2) - S_\alpha[\Psi(\rho_1\otimes\rho_2)]\\ &= \Delta\mathcal{S}_\alpha + S_\alpha^\diamond(\sigma) + S_\alpha(\rho_1\otimes\rho_2) - S_\alpha[\Psi(\rho_1\otimes\rho_2)]\\ &\geqslant \Delta\mathcal{S}_\alpha, \end{aligned}$$

where the second equality holds since $S_\alpha(\Psi_i) = S_\alpha[\Psi_i(\rho_i)] - S_\alpha(\rho_i)$ for $i = 1, 2$ and $S_\alpha(\rho_1 \otimes \rho_2) = S_\alpha(\rho_1) + S_\alpha(\rho_2)$, and the third inequality holds since $\Delta\mathcal{S}_\alpha = S_\alpha(\Psi_1) + S_\alpha(\Psi_2) - S^\diamond(\sigma)$. The inequality holds since $S^\diamond_\alpha(\sigma)$ is the maximally extractable entropy from σ through catalysis and Ψ itself is also being implemented catalytically, therefore $S^\diamond_\alpha(\sigma) \geqslant S_\alpha[\Psi(\rho_1 \otimes \rho_2)] - S_\alpha(\rho_1 \otimes \rho_2)$. ■

11. Proof of Proposition 16

Proof. We can assume that the target map Φ is given as $\Phi(\rho) = |0\rangle\langle 0|$ without loss of generality. The maximal entropy decrease by Φ is $\log_2 d$ which can be achieved only with the maximally mixed input state $\frac{1}{d}\mathbb{1}$, and the maximal entropy increase by $\mathcal{I} \otimes \Phi$ is also $\log_2 d$, achieved with a maximally entangled pure input state, e.g., $\frac{1}{d}|\Gamma\rangle\langle\Gamma|$.

Therefore, the mutual information of the intermediate should be able to change by $\log_2 d$ in both directions. However, the mutual information of an intermediate for a d-dimensional catalyst is upper bounded by $2\log_2 d$, which can only be achieved with the maximally mixed catalyst. It leaves $\log_2 d$ as the only possible value for the mutual information of the initial intermediate. ■

12. Proof of Proposition 17

Proof. Let Φ be the quantum map in question and let A be the system Φ acts on. Let γ be the quantum state that achieves the entropy decrease of ΔS, i.e., $S(\gamma) - S[\Phi(\gamma)] = \Delta S$. Consider a purification $|G\rangle_{AB}$ of γ, i.e., $\mathrm{Tr}_B|G\rangle\langle G|_{AB} = \gamma_A$. Next, we let $\zeta_{AB} := (\Phi_A \otimes \mathcal{I}_B)(|G\rangle\langle G|_{AB})$ and use the inequality $S(B)_\zeta - S(A)_\zeta \leqslant S(AB)_\zeta$ from the Araki-Lieb inequality of the von Neumann entropy [31]. Note that $S(A)_\zeta = S[\Phi(\gamma)]$ and $S(B)_\zeta = S(\gamma)$. Therefore, $S(B)_\zeta - S(A)_\zeta$ equals to the local decrease of entropy by Φ. Similarly, $S(AB)_\zeta$ can be interpreted as the global entropy increase of the pure input state $|G\rangle_{AB}$ as a pure state has zero von Neumann entropy. This proves the desired result. ■

[1] P. Boes, H. Wilming, R. Gallego, and J. Eisert, Catalytic Quantum Randomness, Phys. Rev. X **8**, 041016 (2018).

[2] P. Boes, J. Eisert, R. Gallego, M. P. Müller, and H. Wilming, Von Neumann Entropy from Unitarity, Phys. Rev. Lett. **122**, 210402 (2019).

[3] S. H. Lie, H. Kwon, M. Kim, and H. Jeong, Quantum one-time tables for unconditionally secure qubit-commitment, Quantum **5**, 405 (2021).

[4] S. H. Lie, S. Choi, and H. Jeong, Min-entropy as a resource for one-shot private state transfer, quantum masking, and state transition, Phys. Rev. A **103**, 042421 (2021).

[5] S. H. Lie and H. Jeong, Randomness cost of masking quantum information and the information conservation law, Phys. Rev. A **101**, 052322 (2020).

[6] M. P. Müller, Correlating Thermal Machines and the Second Law at the Nanoscale, Phys. Rev. X **8**, 041051 (2018).

[7] A. Rényi *et al.*, On measures of entropy and information, in *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability*, Volume 1: Contributions to the Theory of Statistics (The Regents of the University of California, Berkeley, CA, 1961).

[8] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).

[9] S. H. Lie and H. Jeong, Randomness for quantum channels: Genericity of catalysis and quantum advantage of uniformness, Phys. Rev. Research **3**, 013218 (2021).

[10] M. Horodecki, P. Horodecki, and J. Oppenheim, Reversible transformations from pure to mixed states and the unique measure of information, Phys. Rev. A **67**, 062104 (2003).

[11] J. Scharlau and M. P. Mueller, Quantum Horn's lemma, finite heat baths, and the third law of thermodynamics, Quantum **2**, 54 (2018).

[12] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Y. Halpern, The resource theory of informational nonequilibrium in thermodynamics, Phys. Rep. **583**, 1 (2015).

[13] N. H. Y. Ng and M. P. Woods, Resource theory of quantum thermodynamics: Thermal operations and second laws, Thermodynam. Quantum Regime: Fund. Aspects New Direct. **195**, 625 (2018).

[14] F. Binder, S. Vinjanampathy, K. Modi, and J. Goold, Quantum thermodynamics of general quantum processes, Phys. Rev. E **91**, 032119 (2015).

[15] F. Buscemi, Private quantum decoupling and secure disposal of information, New J. Phys. **11**, 123002 (2009).

[16] D. Gottesman, Theory of quantum secret sharing, Phys. Rev. A **61**, 042311 (2000).

[17] R. Cleve, D. Gottesman, and H.-K. Lo, How to Share a Quantum Secret, Phys. Rev. Lett. **83**, 648 (1999).

[18] H. Imai, J. Müller-Quade, A. C. A. Nascimento, P. Tuyls, and A. Winter, An information theoretical model for quantum secret sharing schemes, Quantum Inf. Comput. **5**, 69 (2005).

[19] H. Wilming, Entropy and reversible catalysis, arXiv:2012.05573.

[20] R. Takagi and N. Shiraishi, Correlation in catalysts enables arbitrary manipulation of quantum coherence, arXiv:2106.12592.

[21] M. P. Müller and M. Pastena, A generalization of majorization that characterizes Shannon entropy, IEEE Trans. Inf. Theory **62**, 1711 (2016).

[22] H. Wilming, R. Gallego, and J. Eisert, Axiomatic characterization of the quantum relative entropy and free energy, Entropy **19**, 241 (2017).

[23] N. Shiraishi and T. Sagawa, Quantum Thermodynamics of Correlated-Catalytic State Conversion at Small Scale, Phys. Rev. Lett. **126**, 150502 (2021).

[24] T. V. Kondra, C. Datta, and A. Streltsov, Catalytic Entanglement, Phys. Rev. Lett. **127**, 150503 (2021).

[25] P. Lipka-Bartosik and P. Skrzypczyk, Catalytic Quantum Teleportation, Phys. Rev. Lett. **127**, 080502 (2021).

[26] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, Randomness in quantum mechanics: Philosophy, physics, and technology, Rep. Prog. Phys. **80**, 124001 (2017).

[27] P. Shor, Structure of Unital Maps and the Asymptotic Quantum Birkhoff Conjecture, Steklov Mathematical Institute of RAS, Conference Hall, Moscow (2010).

[28] U. Haagerup and M. Musat, Factorization and dilation problems for completely positive maps on von Neumann algebras, Commun. Math. Phys. **303**, 555 (2011).

[29] J. Deschamps, I. Nechita, and C. Pellegrini, On some classes of bipartite unitary operators, J. Phys. A: Math. Theor. **49**, 335301 (2016).

[30] T. Benoist and I. Nechita, On bipartite unitary matrices generating subalgebra-preserving quantum operations, Linear Algebra Appl. **521**, 70 (2017).

[31] H. Araki and E. H. Lieb, Entropy inequalities, Commun. Math. Phys. **18**, 160 (1970).

[32] T. Van Erven and P. Harremos, Rényi divergence and Kullback-Leibler divergence, IEEE Trans. Inf. Theory **60**, 3797 (2014).

[33] N. P. Landsman, Lecture notes on c*-algebras, Hilbert c*-modules, and quantum mechanics, arXiv:math-ph/9807030.

[34] E. Artin, Zur theorie der hyperkomplexen zahlen, in *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, Vol. 5 (Springer, Berlin, 1927), pp. 251–260.

[35] J. Wedderburn, On hypercomplex numbers, Proc. London Math. Soc. **s2-6**, 77 (1908).

[36] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Reference frames, superselection rules, and quantum information, Rev. Mod. Phys. **79**, 555 (2007).

[37] M. Peskin, *An Introduction to Quantum Field Theory* (CRC Press, Boca Raton, FL, 2018).

[38] S. Sołtan, M. Fraczak, W. Belzig, and A. Bednorz, Conservation laws in quantum noninvasive measurements, Phys. Rev. Research **3**, 013247 (2021).

[39] B. Groisman, S. Popescu, and A. Winter, Quantum, classical, and total amount of correlations in a quantum state, Phys. Rev. A **72**, 032317 (2005).

[40] S. L. Braunstein and A. K. Pati, Quantum Information Cannot be Completely Hidden in Correlations: Implications For the Black-Hole Information Paradox, Phys. Rev. Lett. **98**, 080502 (2007).

[41] E. H. Lieb and M. B. Ruskai, Proof of the strong subadditivity of quantum-mechanical entropy, J. Math. Phys. **14**, 1938 (1973).

[42] T. M. Cover, *Elements of Information Theory* (John Wiley & Sons, New York, NY, 1999).

[43] A. Horn, Doubly stochastic matrices and the diagonal of a rotation matrix, Am. J. Math. **76**, 620 (1954).

[44] I. Schur, Uber eine klasse von mittelbildungen mit anwendungen auf die determinantentheorie, Sitzungsberichte der Berliner Mathematischen Gesellschaft **22**, 51 (1923).

[45] B. Regula, K. Bu, R. Takagi, and Z.-W. Liu, Characterizing one-shot distillation in general resource theories, Phys. Rev. A **101**, 062315 (2020).

[46] Z.-W. Liu, K. Bu, and R. Takagi, One-Shot Operational Quantum Resource Theory, Phys. Rev. Lett. **123**, 020401 (2019).

[47] K. C. Tan, V. Narasimhachar, and B. Regula, Fisher information universally identifies quantum resources, arXiv:2104.01763.

[48] M. Lostaglio, M. P. Müller, and M. Pastena, Stochastic Independence As a Resource in Small-Scale Thermodynamics, Phys. Rev. Lett. **115**, 150402 (2015).

[49] A. Winter and D. Yang, Operational Resource Theory of Coherence, Phys. Rev. Lett. **116**, 120404 (2016).

[50] M. Musat and M. Rørdam, Nonclosure of quantum correlation matrices and factorizable channels that require infinite dimensional ancilla (with an Appendix by Narutaka Ozawa), Commun. Math. Phys. **375**, 1761 (2020).

[51] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2002).

[52] M.-D. Choi, Completely positive linear maps on complex matrices, Linear Algebra Appl. **10**, 285 (1975).

[53] A. Jamiołkowski, Linear transformations which preserve trace and positive semidefiniteness of operators, Rep. Math. Phys. **3**, 275 (1972).

[54] A. Arias, A. Gheondea, and S. Gudder, Fixed points of quantum operations, J. Math. Phys. **43**, 5872 (2002).

[55] W. van Dam and P. Hayden, Renyi-entropic bounds on quantum communication, arXiv:quant-ph/0204093.

[56] M. A. Nielsen, Probability distributions consistent with a mixed state, Phys. Rev. A **62**, 052308 (2000).