Delocalized and dynamical catalytic randomness and information flow

Seok Hyung Lie[1,2] and Hyunseok Jeong[1]
[1]*Department of Physics and Astronomy, Seoul National University, Seoul, 151-742, Korea*
[2]*School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore, 637371*

(Received 14 July 2022; accepted 27 March 2023; published 24 April 2023)

We generalize the theory of catalytic quantum randomness to distributed and dynamical settings. First, we expand the theory of catalytic quantum randomness by calculating the amount of (Rényi) entropy catalytically extractable from a distributed or dynamical randomness source. We show that no entropy can be catalytically extracted when one cannot implement local projective measurement on randomness source without altering its state. As an application, we prove that quantum operation cannot be hidden in correlation between two parties without using randomness, which is the dynamical generalization of the no-hiding theorem. Moreover, the formalism of distributed catalysis is applied to develop a formal definition of semantic quantum information and it follows that utilizing semantic information is equivalent to catalysis using a catalyst already correlated with the transforming system. By doing so, we unify the utilization of semantic and nonsemantic quantum information and conclude that one can always extract more information from an incompletely depleted classical randomness source, but it is not possible for quantum randomness sources.

DOI: 10.1103/PhysRevA.107.042430

I. INTRODUCTION

Flow of information is a key criterion that decides which processes are allowed and which are not in physical theories. For example, there are ostensibly faster-than-light phenomena such as phase velocity (or even group velocity [1]) of electromagnetic wave, expansion velocity of far galaxies due to Hubble's law [2] and collapse of wave function shared between spacelike regions, but they are not forbidden by relativity because it is widely considered that those phenomena are not accompanied by faster-than-light propagation of information [3]. Moreover, oftentimes it is said that nothing can escape black holes, but black holes evaporate by emitting Hawking radiation. A common justification of this is that Hawking radiation does not convey information of objects fallen into the black hole. These examples suggest that information flow is not only as real as flow of matter as Landauer said "information is physical," but also has enough independency that warrants focus for its own.

However, what is information, exactly? How is it different from other materialistic entities? Can information propagate from its source to a target without visiting any other regions like a particle, or must it spread to multiple regions like wave? Although we intuitively have a vague idea about what information is, answering this question in a universally satisfactory way is highly difficult considering the sheer vastness of information science. The advent of quantum information theory burdens the already complicated field of information science with more mystery, and makes us ask the same questions for quantum information.

Quantum information is frequently identified with quantum state and displacement of a quantum state is interpreted as an information flow, but this approach is unsatisfactory since it is not quantum state *per se*, but the variance of quantum state by some information source is what carries information. This observation asks for a dynamical approach to information flow, namely, that identifies information flow with a quantum channel with nonzero capacity, which has been taken in studies on localizable and causal quantum operations [4].

While largely successful, the picture of information as a varying quantum state and the resultant measurement outcome change treats quantum systems merely as a medium for communication of classical information and overlooks the nature of "quantum information" itself. Treating pure quantum states informative is contradictory with the perspective of the Shannon information theory [5], where information is identified with randomness. Especially, considering state-dependent restrictions on causality in recent proposals for black hole information paradox such as the Hayden-Preskill protocol [6], the necessity for investigating (semi)causality in the (partially) static setting is growing lately. Interpreting randomness as information provides a picture that can satisfactorily describe information localized in a region of space-time and its propagation, as one can assign entropy to each region from their quantum state.

These two perspectives on information are complementary to each other: Randomness of quantum state represents the internal information, or information *inside* a quantum system, and the current state of a quantum system represents the external information, or information *one has* about the system. The latter is often too implicit and heavily depends on the context, hence, it is hard to locate and quantify. On the contrary, advantage of internal information is that it is easy to locate and track its presence and propagation. Therefore, to model the directional (quantum) information flow from a source to a unique target, we employ the theory of catalytic quantum randomness and generalize it further to a broader class of randomness sources such as correlated and dynamical sources.

The resource theory, a framework in which a certain physical aspect is abstracted as a resource to analyze the property in question systematically, has been immensely successful in quantum physics and quantum information science. A resource theory identifies resourceful objects (states, operations, etc.) by defining what is considered *free*, meaning that it is easy to perform or prepare, and treating everything that is not free as resourceful. There are many examples of properties for which resource theoretical approach was successful; entanglement [7], coherence [8], non-Gaussianity [9], and many more. These generic resource theories have one thing in common. They are either *convex* or admit convexification. Note that a resource theory is convex when the set of free objects is convex.

The convexity condition is considered natural in many cases; in many recent works [10–12] on unified approach to resource theory with resource-independent methods, it is assumed that the free set is convex. A common justification is that simply forgetting information, a common method of physically implementing convex sum, cannot generate useful resources. However, this assumption is by no means always justified. Indeed, there are nonconvex resource theories such as that of correlation. Statistically mixing two states without correlation can generate correlation and, especially, since the convex hull of the set of all states without correlation is the whole quantum state set, the theory does not allow convexification to form a meaningful resource theory.

More extremely, there are resource theories that are what we could say to be *concave*. In these resource theories, the set of resourceful objects, not the free objects, is convex (see Appendix, Sec. A 11, for related discussions). In this situation, forgetting information has not only a potential to create resources, but also can never eliminate resources.

The premise that destruction of information is resourceful is natural in both fundamental and practical contexts. Fundamentally, the time evolution of a closed quantum system is given by unitary operations which are invertible, thus, it is often said that no quantum information is genuinely destructible (following the usual "state = information" definition). This is the very reason behind the long-lasting controversy on what will happen eventually to quantum information fallen into black holes [13]. Practically, in some cryptographic settings where mutually distrustful participants are interacting, it is impossible for one participant to persuade other participants that some information was deleted from one's data storage without some special assumptions. (It is ridiculous to say "Hey, I just flipped a coin and I forgot the outcome. Let us bet on which side the coin was" over text message.) This is why one needs a special protocol for coin flipping by telephone [14] and more generally cryptographic primitives such as bit commitment and oblivious transfer.

Randomness represents both presence and absence of information depending on perspective. The more random an information source is, the less information one already has about the source, equivalently, the more information the source can yield. Hence, in a sense, forgetting information could create randomness. Thus, an archetype of such resource theory is the resource theory of randomness (RTR) [15–19] based on the theory of catalytic quantum randomness of Boes *et al.* [20]. In the RTR, pure states are considered free and unitary operations are free operations, but none of them have convex structure. Moreover, there is no universally resource-destroying map [21] since every locally randomness-decreasing map should increase randomness globally [19]. On the other hand, the set of mixed states and the set of unital maps, which are considered resourceful in the RTR, are both convex.

Previously, in the RTR, only static and local quantum states with nonzero entropy were considered as randomness sources, but in real life dynamical or global randomness sources are commonplace. Most symbolically, secret key randomly generated and shared by multiple agents is an example of distributed randomness source, and the simple action of rolling dice itself is a dynamical source of randomness. In this work, we extend the limit of the RTR to encompass utilization of distributed and dynamical randomness sources by employing the Choi-Jamiołkowski isomorphism [22,23] and the language of dynamical resource theory [24].

II. PRELIMINARIES

A. Notations

Without loss of generality, we sometimes identify the Hilbert space H_X corresponding to a quantum system X with the system itself and use the same symbol X to denote both. For any system X, X' is a copy of X with the same dimension, i.e., $|X| = |X'|$. When there are many systems other than a system X, then all the systems other than X are denoted by $\bar{X}$. However, the trivial Hilbert space will be identified with the field of complex numbers and will be denoted by $\mathbb{C}$. We will denote the dimension of X by $|X|$. The identity operator on system X is denoted by $\mathbb{1}_X$ and the maximally mixed state is denoted by $\pi_X = |X|^{-1}\mathbb{1}_X$. For any Hermitian matrix σ, $\lambda_i(\sigma)$ denotes its ith largest eigenvalue including degeneracy, i.e., it is possible that $\lambda_i(\sigma) = \lambda_{i+1}(\sigma)$. For any Hilbert spaces X and Y, $X \leqslant Y$ denotes that X is a subspace of Y. The space of all bounded operators acting on system X is denoted by $\mathfrak{B}(X)$, the real space of all Hermitian matrices on system X by $\mathfrak{H}(X)$. The set of all unitary operators in $\mathfrak{B}(X)$ is denoted by $\mathfrak{U}(X)$. For any matrix M, M^T is its transpose with respect to some fixed basis, and for any $M \in \mathfrak{B}(X \otimes Y)$, the partial transpose on system X is denoted by M^{T_X}. For any $M \in \mathfrak{B}(X)$, we let $\mathrm{Ad}_M \in \mathfrak{L}(X)$ be

$$\mathrm{Ad}_M(K) := MKM^\dagger.$$

The space of all linear maps from $\mathfrak{B}(X)$ to $\mathfrak{B}(Y)$ is denoted by $\mathfrak{L}(X,Y) = \mathfrak{B}(\mathfrak{B}(X), \mathfrak{B}(Y))$ and we will use the shorthand notation $\mathfrak{L}(X) := \mathfrak{L}(X,X)$. The set of all quantum states on system X by $\mathfrak{S}(X)$ and the set of all quantum channels (completely positive and trace-preserving linear maps) from system X to Y by $\mathfrak{C}(X,Y)$ with $\mathfrak{C}(X) := \mathfrak{C}(X,X)$. Similarly, we denote the set of all quantum subchannels (completely positive trace nonincreasing linear maps) by $\tilde{\mathfrak{C}}(X,Y)$ and $\tilde{\mathfrak{C}}(X) := \tilde{\mathfrak{C}}(X,X)$. We denote the identity map on system X by id_X. Let $\mathcal{T} : M \mapsto M^T$ be the transpose map, and $\dagger : M \mapsto M^\dagger$ be the adjoint map. For any $\mathcal{N} \in \mathfrak{L}(X,Y)$, we define its adjoint $\mathcal{N}^\dagger(G)$ so that $\langle \mathcal{N}^\dagger(G), H\rangle = \langle G, \mathcal{N}(H)\rangle$ for every $G \in \mathfrak{B}(Y)$ and $H \in \mathfrak{B}(X)$. We define the transpose $\mathcal{N}^T(H) := (\mathcal{N}^\dagger(H^*))^*$, where G^* is the complex conjugation of G.

$J^{\mathcal{N}}_{XX'}$ is the Choi matrix of $\mathcal{N} \in \mathfrak{L}(X)$ defined as $J^{\mathcal{N}}_{XX'} := \mathcal{N}_X(\phi^+_{XX'})$ where $\phi^+_{XX'} = |\phi^+\rangle\langle\phi^+|_{XX'}$ is a maximally entangled state with $|\phi^+\rangle_{XX'} = |X|^{-1/2}\sum_i |ii\rangle_{XX'}$. The mapping $J : \mathfrak{L}(X) \to \mathfrak{B}(X \otimes X')$ defined as $J(\mathcal{M}) := J^{\mathcal{M}}_{XX'}$ itself is called the Choi-Jamiołkowski isomorphism [22,23]. We call a linear map from $\mathfrak{L}(X)$ to $\mathfrak{L}(Y)$ a *supermap* from X to Y and denote the space of supermaps from X to Y by $\mathfrak{SL}(X, Y)$ and let $\mathfrak{SL}(X) := \mathfrak{SL}(X, X)$. Supermaps preserving quantum channels even when they only act on a part of multipartite quantum channels are called *superchannel* [24–30] and the set of all superchannels from X to Y is denoted by $\mathfrak{SC}(X, Y)$ and we let $\mathfrak{SC}(X) := \mathfrak{SC}(X, X)$. We say a superchannel $\mathcal{V} \in \mathfrak{SC}(X)$ is *superunitary* if there are U_0 and U_1 in $\mathfrak{U}(X)$ such that $\mathcal{V}(\mathcal{N}) = \mathrm{Ad}_{U_1} \circ \mathcal{N} \circ \mathrm{Ad}_{U_0}$ for all $\mathcal{N} \in \mathfrak{L}(X)$ [31].

The *supertrace* [32] is the superchannel counterpart of the trace operation modeling the loss of dynamical quantum information, denoted by $\mathfrak{Tr}$. The supertrace is defined in such a way that the following diagram is commutative:

$$\begin{array}{ccc} \mathfrak{L}(X) & \xrightarrow{\mathfrak{Tr}} & \mathbb{C} \\ \downarrow{\scriptstyle J} & & \downarrow{\scriptstyle \mathrm{id}_{\mathbb{C}}} \\ \mathfrak{B}(X \otimes X') & \xrightarrow{\mathrm{Tr}} & \mathbb{C} \end{array} . \tag{1}$$

Here, we slightly abused the notations by identifying isomorphic trivial Hilbert spaces $\mathbb{C}^* \approx \mathbb{C} \approx \mathfrak{L}(\mathbb{C}) \approx \mathfrak{B}(\mathbb{C} \otimes \mathbb{C})$ and letting $J : \mathfrak{L}(\mathbb{C}) \to \mathfrak{B}(\mathbb{C} \otimes \mathbb{C})$ be identified with $\mathrm{id}_{\mathbb{C}}$. Explicitly,

$$\mathfrak{Tr}[\mathcal{M}] := \mathrm{Tr}\big[J^{\mathcal{M}}_{XX'}\big] = \mathrm{Tr}[\mathcal{M}(\pi_X)] \tag{2}$$

for all $\mathcal{M} \in \mathfrak{L}(X)$. From (2), it is evident why the supertrace corresponds to the loss of information of quantum channels as it is operationally equivalent to the loss of input state (as the input state is assumed to be maximally mixed) and the loss of output state (as the output state is traced out). Similarly to partial trace, $\mathfrak{Tr}_X$ is a shorthand expression of $\mathfrak{Tr}_X \otimes \mathfrak{id}_{\bar{X}}$, where $\mathfrak{id}_Y := \mathrm{id}_{\mathfrak{L}(Y)}$. Note that the supertrace lacks a few tracial properties such as cyclicity, i.e., $\mathfrak{Tr}[\mathcal{A} \circ \mathcal{B}] \neq \mathfrak{Tr}[\mathcal{B} \circ \mathcal{A}]$ in general, however, it generalizes the operational aspect of trace as the discarding action. For example, for every quantum channel $\mathcal{N}$ is normalized in supertrace, i.e., $\mathfrak{Tr}[\mathcal{N}] = 1$.

In a similar way, we define the "Choi map" $\mathbb{J}[\Theta] \in \mathfrak{L}(X \otimes X', Y \otimes Y')$ of supermap $\Theta \in \mathfrak{SL}(X, Y)$ in such a way that the following diagram is commutative:

$$\begin{array}{ccc} \mathfrak{L}(X) & \xrightarrow{\Theta} & \mathfrak{L}(Y) \\ \downarrow{\scriptstyle J} & & \downarrow{\scriptstyle J} \\ \mathfrak{B}(X \otimes X') & \xrightarrow{\mathbb{J}[\Theta]} & \mathfrak{B}(Y \otimes Y') \end{array} . \tag{3}$$

Throughout the paper, the direct sum symbol $\oplus$ for operators has two meanings: If A_i are already in the same space and mutually orthogonal, then $\bigoplus_i A_i$ emphasizes such fact and it means simply $\sum_i A_i$. If B_i are not necessarily mutually orthogonal, or even repeated for different i, then $\bigoplus_i B_i$ embeds the operators into a larger Hilbert space and makes them mutually orthogonal. One possible implementation is $\bigoplus_i B_i := \sum_i |i\rangle\langle i| \otimes B_i$.

B. Superselection rule and C^* algebra

It is customary to model a quantum state of system X with a density matrix ρ in $\mathfrak{B}(X)$, but it is not necessary to assume that a quantum system has access to all of the full matrix algebra $\mathfrak{B}(X)$. In general, a quantum system can be modeled with a C^* algebra [33,34], and a finite-dimensional C^* algebra is isomorphic to a direct sum of full matrix algebras by the Artin-Wedderburn theorem [35,36]. In other words, for every finite-dimensional C^* algebra $\mathcal{C}$, there exist finite-dimensional Hilbert spaces X_i such that $\mathcal{C} \approx \bigoplus_{i=1}^n \mathfrak{B}(X_i)$ as a ring. Considering multiplicity, if $\mathcal{C}$ is a subalgebra of a matrix algebra, there is an explicit decomposition of the form $\mathcal{C} = \bigoplus_{i=1}^n \mathfrak{B}(X_i) \otimes \mathbb{1}_{d_i}$ where $\mathbb{1}_{d_i}$ is the identity operator on $\mathbb{C}^{d_i}$ with the multiplicity d_i of $\mathfrak{B}(X_i)$ [37].

In fact, it is equivalent to saying that the system X is under *superselection rules* which means that there exist subspaces $\{X_i\}$ of X called the *superselection sectors* such that $\mathfrak{S}(X) \subseteq \bigoplus_i \mathfrak{B}(X_i)$. Therefore, one can interpret that, at least for finite-dimensional cases, a C^* algebra $\mathcal{C} \approx \bigoplus_{i=1}^n \mathfrak{B}(X_i)$ represents a classical-quantum hybrid system in which a classical information i is not allowed to be in superposition.

Remember that ρ_{AB} is called a classical-quantum (C-Q) state when ρ_{AB} can be embedded into the tensor product of C^* algebras $\mathcal{C} \otimes \mathcal{D}$ where $\mathcal{C}$ is classical, i.e., there is a basis $\{|i\rangle_A\}$ of A such that ρ_{AB} has the form

$$\rho_{AB} = \sum_i p_i |i\rangle\langle i|_A \otimes \rho^i_B, \tag{4}$$

for some probability distribution $\{p_i\}$ and quantum states $\rho^i_B \in \mathfrak{S}(B)$. When the roles of A and B are switched, we call it Q-C, and if ρ_{AB} is neither C-Q nor Q-C, then it is called Q-Q. As a generalization, we will call ρ_{AB} partially classical-quantum (PC-Q) if ρ_{AB} can be embedded into the tensor product of C^* algebras $\mathcal{C} \otimes \mathcal{D}$ where $\mathcal{C}$ is partially classical, i.e., there exists a projective measurement $\{\Pi_i\}_{i=1}^n$ with $n > 1$ on A ($\Pi_i\Pi_j = \delta_{ij}\Pi_i$ and $\sum_i \Pi_i = \mathbb{1}_A$) that leaves ρ_{AB} unperturbed. In other words,

$$\rho_{AB} = \sum_i (\Pi_i \otimes \mathbb{1}_B)\rho_{AB}(\Pi_i \otimes \mathbb{1}_B). \tag{5}$$

If (5) holds, we also say that ρ_{AB} is generalized block diagonal with respect to $A = \bigoplus_i A_i$ where $A_i = \mathrm{supp}(\Pi_i)$ [38]. If the roles of A and B are reversed, we will call it Q-PC. If a bipartite state is both PC-Q and Q-PC, then it is called PC-PC. On the other hand, if a system is not partially classical, we will say that it is totally quantum (TQ), so that a bipartite system that is not PC-Q is now called TQ-Q. One can similarly define Q-TQ, PC-TQ, TQ-TQ states, etc.

III. RESOURCE THEORY OF RANDOMNESS

A. Catalytic randomness and information flow

Information can be localized and displaced, and takes an important role in physical theory, sometimes even more important than ostensible material entities. Hence, it is natural to treat information as a physical entity that a system can possess and to identify its properties.

How is information different from other physical entities? First of all, for information to be physically relevant, it should

FIG. 1. A book is a randomness (equivalently an information) source, but not every usage of it is pure randomness utilization. For example, it is hard to say that burning a book utilizes only the randomness of the book, as it leaves evidently detectable physical traces on it. Intuitively, it is clear that any usage of a book that necessitates non-negligible physical alternation of the book is not a pure information utilization. Therefore, we claim that (pure) randomness utilization must not leave any locally detectable statistical change on the randomness source.

leave detectable effects on its receiver, however, not every detectable change is made by information. If someone breaks your window by throwing a rock to notify you, is it information in the rock that broke the window? It is natural to conclude that information exchange merely accompanied the event and it is the kinetic energy of the rock that broke the window. Like this example, in general, exchange of information is mixed up with other physical effects.

What would a "pure" information source that does not yield any physical resources other than information look like? For this to be possible, no detectable change of physical resource in the source should be allowed, therefore, its state should stay unchanged. It means that no detectable change can be caused by the other system it is interacting with, equivalently, there is no information flow from it into the source. We could say that this kind of interaction has *directional information flow* in which information only flows from a distinguished information source to its user and not the other way around. This is the process we may call a purely information utilizing process and we claim that it must satisfy the following mutually related criteria (see Fig. 1).

(1) *Random*: The state of an information source must be random to be informative.

(2) *Correlating*: After use of an information source, it forms correlation with its user, altering their global state.

(3) *Directional*: Information flows from an information source to its user exclusively, not the other way around.

Information *stored* in a system, not information we *have* about the system, is the randomness of the system, just as how probability distribution of a random variable and its entropy represent the information within the variable in the Shannon information theory [5]. Moreover, information usage is entropy extraction process, not in the sense that the process reduces the entropy of a source and displaces it to the target system, but in the sense that correlation between a source and its user is built in the process and the amount of correlation formed can be interpreted as the amount of randomness extracted from the source [19].

Directionality criterion can be applied both on fundamental and various practical levels. A person may not be able to read a book leaving absolutely no traces (e.g., not perturbing molecular arrays of the book at all), but if the trace is "practically" (whatever that means in a given context) undetectable so that its statistical state is left unchanged, then we consider that the person only used the information content of the book on that practicality level. This fact allows us to circumvent the question of fundamental nature of randomness in light of deterministic time evolution of classical and quantum mechanics in closed systems, as there are events that appear random on practical level regardless of the underlying law of nature.

For example, even when one interacts with a cylinder filled with gas without altering any thermodynamic parameters such as temperature and volume, another person who memorized all the configurations of molecules of the gas is able to detect the change. However, to that person, the gas was not random from the beginning. For a person to whom only the macroscopic quantities of the gas were known, the gas can still appear intact. If a randomness source behaves the same way in every statistical aspect after an interaction, we consider it unaffected.

Hence, in a purely information, i.e., randomness, utilizing process, the information carrier simply enters the interaction and leaves it while staying in the same quantum state. Nevertheless, the information carrier could cause changes of other systems. This fits the definition of catalysis and the carrier can be considered a catalyst. This is one of the main reasons why the study on catalysis of randomness is motivated. Nonetheless, we intuitively know that information itself can be "depleted" for individual users [19]. For example, a novel is no longer interesting once a reader finishes reading it and remembers all the plot despite the fact that the book is physically unchanged. This can be explained by the correlation built between the carrier and the user, which is a purely informational quantity. On the other hand, the memory of the reader initially prepared in a pure state becomes random after forming correlation with other systems. Hence, correlation forming can be interpreted as randomness extraction. These two observations motivate the study of a theory that sounds contradictory on the surface level, the resource theory of catalytic randomness.

In this work, we will investigate the properties of quantum information flow by studying catalytic quantum randomness. One may claim that this type of "noninvasiveness" is a characteristic of classical randomness and should not be required from quantum randomness because of the inherent perturbing nature of quantum measurement. However, such a claim comes from confusing quantum information with quantum state. The latter contains every physical description of a quantum system, be it informational or not, and we are trying to characterize the former in this work. Indeed, one cannot interact nontrivially with a quantum system in a pure state without perturbing it, but a system with zero entropy has no information to provide in the first place. Therefore, a quantum information source must be in a mixed state, and we know that we can extract information, measured by entropy, without perturbing the mixed state [15,17–20].

Note that we do not concern ourselves with the mechanism of *randomness generation*. Just as resource theory of entanglement cares more about manipulation of already existing entanglement rather than studying the protocol of entanglement establishment (which is different from entanglement distillation), resource theory of randomness is more about utilization of preexisting randomness sources regardless of their generation mechanism. Hence, "quantum randomness (source)" in this work is not related to what is conventionally

referred to as quantum randomness, which usually means a classical random variable generated by measuring a quantum system, stored in classical memory. Quantum randomness in this work means the randomness of quantum systems enjoying its quantum coherence, represented by mixed quantum states. This is the reason why one need not answer the question of what is the true origin of randomness before using the resource theory of randomness, as users with different criteria for randomness can still use the same theory.

B. Catalytic randomness

In this section, we summarize and review the results of the correlational resource theory of catalytic randomness [19,20]. Suppose that A is allowed to borrow a system B called *catalyst* in the quantum state σ_B to implement a quantum channel $\mathcal{N}$. 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. When a bipartite unitary U on systems A and B is used to implement a quantum channel $\rho \mapsto \mathcal{N}(\rho)$ with a catalyst σ for arbitrary possible input state ρ, i.e.,

$$\mathrm{Tr}_B \mathrm{Ad}_U(\rho_A \otimes \sigma_B) = \mathcal{N}(\rho), \quad \forall\, \rho \in \mathfrak{S}(A). \tag{6}$$

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

$$\mathrm{Tr}_A \mathrm{Ad}_U(\rho_A \otimes \sigma_B) = \sigma_B, \quad \forall\, \rho \in \mathfrak{S}(A). \tag{7}$$

The conditions above require the catalyst to be insensitive to dynamically changing state of the target system. The dynamical definition (7) can be reexpressed in the Heisenberg picture and in the static setting; we can require the catalyst to be insensitive to the change of action on the target system.

Theorem 1. Condition (7) is equivalent to any of the following.

(i) For some state $\rho_A \in \mathfrak{S}(A)$ and for every superchannel $\Theta \in \mathfrak{SC}(A)$, the transformed bipartite quantum channel $(\Theta_A \otimes \mathfrak{id}_B)(\mathrm{Ad}_U)$ fixes the marginal state σ_B, i.e.,

$$\mathrm{Tr}_A[(\Theta_A \otimes \mathfrak{id}_B)(\mathrm{Ad}_U)(\rho_A \otimes \sigma_B)] = \sigma_B. \tag{8}$$

(ii) When $\rho_A \in \mathfrak{S}(A)$ is given, for any ancillary system R, a unitary operator $U \in \mathfrak{V}(RA)$ and the state given as $\tau_{RA} = \mathrm{Ad}_V(|0\rangle\langle 0|_R \otimes \rho_A)$, the following holds:

$$\mathrm{Tr}_A[\mathrm{id}_R \otimes \mathrm{Ad}_U(\tau_{RA} \otimes \sigma_B)] = \tau_R \otimes \sigma_B^{(V)}. \tag{9}$$

Here, the marginal state $\sigma_B^{(V)}$ may depend on V.

Especially the definition (i) aligning with the interventionist view on causation [39], the perspective according to which if a manipulation of system implies a change of another system then the former is the cause and the latter is the effect, will prove to be useful in defining one-way information flow where two correlated systems interact later. A more detailed discussion on the condition given in terms of superchannels can be found in Sec. III E.

We can see that one-way constraint on information flow is picture invariant, i.e., independent of the interpretation of randomness. Condition (i) requires that system B is indifferent to the change of dynamical process on A. Condition (ii) requires that no internal information of A, held by R, is leaked to B. Therefore, we can use whichever picture that suits the given situation to simplify expressions and, unless specified otherwise, we will consider catalysis of randomness in the form of (6) and (7).

The possible dependence of $\sigma_B^{(V)}$ on the process V hints that condition (ii) only prohibits leakage of internal information. However, there is actually no external information leakage because if there are two unitary operators V_1 and V_2 that lead to different $\sigma_B^{(V)}$, then by preparing an additional ancillary qubit prepared in $|+\rangle$ state making it control which operator among V_i is applied on RA, one can contradict condition (ii). Moreover, by Stinespring dilation, one can easily see that unitary operation Ad_V in condition (ii) can be replaced by any quantum channel. These observations combined yield condition (iii) in the next proposition, and also a completely static characterization, condition (iv). Considering the Choi-Jamiołkowski isomorphism, condition (iv) being equivalent to (i) is evident.

Proposition 1. Conditions in Theorem 1 are equivalent to the following conditions.

(iii) When $\rho_A \in \mathfrak{S}(A)$ is given, for any quantum channel $\mathcal{N} \in \mathfrak{C}(A, RA)$ with $\tau_{RA} := \mathcal{N}(\sigma_A)$, we have

$$\mathrm{Tr}_A[\mathrm{id}_R \otimes \mathrm{Ad}_U(\tau_{RA} \otimes \sigma_B)] = \tau_R \otimes \sigma_B. \tag{10}$$

(iv) For any quantum ρ_{RA} state whose marginal state ρ_A is full rank, we have

$$\mathrm{Tr}_A[\mathrm{id}_R \otimes \mathrm{Ad}_U(\rho_{RA} \otimes \sigma_B)] = \rho_R \otimes \sigma_B. \tag{11}$$

The approach of condition (iii) that treats the initial setup, the subsequent interaction and the partial trace out as a superchannel that maps interjected quantum channel into an outcome state is akin to the approach of Modi [40] for dynamics of non-Markovian open quantum systems. The requirement of full rankedness of ρ_A in condition (iv) is rather technical than physical, as the set of full-rank states is dense in the set of all states. However, precisely one prepares a quantum state, there could be an infinitesimal noise in the process that renders the prepared state full rank.

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 will call the bipartite interaction described in (6) and (7) a *catalysis* or a *catalysis process* and a quantum channel that can be implemented by catalysis a *catalytic* quantum map or channel. For example, the quantum channel $\mathcal{N}$ in (6) 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 (and vice versa) if (7) holds. If (7) holds with the right-hand side replaced with $V\sigma_B V^\dagger$ with some unitary operator V on B, then they are said to be compatible up to local unitary. 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 [41–43] 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 channel, independently of potential input state, with a given catalyst. However, later we will see that this characterization is also relevant to state transitions, too. In the following theorem, we review the characterization of catalytic unitary operators and compatibility.

Theorem 2 ([19]). A bipartite unitary operator U acting on system AB is catalytic if and only if U^{T_B} is also unitary. Also, a catalytic unitary operator U is compatible with σ_B if and only if $[U, \mathbb{1}_A \otimes \sigma_B] = 0$.

Unlike in resource theories with resource-destroying maps, in the RTR, convertibility between randomness sources is not a very interesting problem since they are either too trivial or too restrictive. Any two quantum states are freely interconvertible if and only if they share the spectrum. If we expand to conversions under catalytic maps, then the problem becomes trivial again since between any two quantum states $\rho \succ \sigma$, there exists a random unitary operation $\mathcal{F}$, which is also catalytic, such that $\mathcal{F}(\rho) = \sigma$ [44]. Therefore, focusing on how much and what kind of randomness is required to implement certain tasks is much more important than merely asking if the conversion exists.

Now we turn to the problem of quantifying the amount of resource one can extract from a source. The amount of information extracted can be quantified with the mutual information

$$I(A:B) = S(A) + S(B) - S(AB)$$

between A and B. However, under the catalysis constraints, the local state of B is invariant and the entropy of global state is invariant, i.e., $S(AB) = S(\rho_A) + S(\sigma_B)$, hence the mutual information after catalysis is equal to the entropy change of system A, i.e., $\Delta I(A:B) = S(\mathcal{N}(\rho_A)) - S(\rho_A)$. Therefore, we will count the entropy increase as the amount of extracted resource during catalysis of quantum randomness. This interpretation is consistent with the view that treats randomness as noise. Generalizing this, we interpret that randomness gained through catalytic maps is from the influx of information. Thus, although there is no simple generalization of mutual information for Rényi entropies, we will also use the Rényi entropies to measure the extracted information from a randomness source.

It was shown in Refs. [18,19] that nondegeneracy of eigenvalues of a mixed state restricts catalysis of quantum randomness. Accordingly, *the catalytic Rényi entropy* $S_\alpha^\diamond(\sigma)$ of order $\alpha \geqslant 0$ of an arbitrary quantum state $\sigma \in \mathfrak{S}(X)$ can be calculated from its spectral decomposition. By spectral decomposition, we mean $\sigma = \sum_i \lambda_i \Pi_i$ with eigenvalues λ_i of σ. Here, we require $\Pi_i \Pi_j = \delta_{ij} \Pi_i$, $\sum_i \lambda_i r_i = 1$, and the injective mapping $i \mapsto \lambda_i \geqslant 0$. If there are superselection rules imposed on X, i.e., $\mathfrak{S}(X) \subseteq \bigoplus_i \mathfrak{B}(X_i)$ for some mutually orthogonal subspaces X_i of X, then we require instead that $\mathrm{supp}(\Pi_i) \leqslant X_{f(i)}$ for some unique subspace of B, $X_{f(i)}$ and that $i \mapsto (\lambda_i, X_{f(i)})$ is injective. We denote the rank of each block by $r_i := \mathrm{Tr}[\Pi_i]$. Let the spectral decomposition satisfying these requirements be called the *catalytic decomposition* of a quantum state and we call each $\mathrm{supp}(\Pi_i)$ a catalysis sector of σ (see Fig. 2).

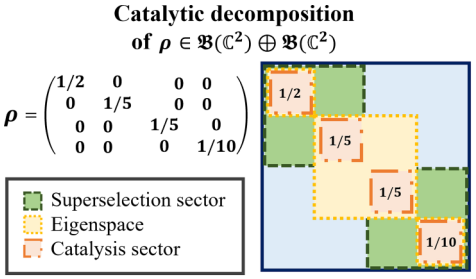


FIG. 2. Catalytic decomposition of a density matrix. A superselection rule forbids between subspaces called superselection sectors, and each density matrix has an eigenspace for each distinct eigenvalue. The intersection of a superselection sector and an eigenspace is called a catalysis sector and it plays an important role in calculating the catalytic entropies.

In this sense, a catalyst compatible with a catalytic unitary operator could be considered a partially classical quantum system only whose classical information (the weight of each catalysis sector) is known.

For any σ with the catalytic decomposition $\sigma = \sum_i \lambda_i \Pi_i$, define a density matrix $\mathfrak{c}(\sigma)$ given as

$$\mathfrak{c}(\sigma) = \bigoplus_i \frac{\lambda_i}{r_i} \mathbb{1}_{r_i^2}, \tag{12}$$

where $\mathbb{1}_{r_i^2} = \mathrm{diag}(1, \ldots, 1)$ is the identity matrix of size r_i^2. It was shown in Ref. [19] that any mixed state catalytically transformed from a pure state by using randomness source σ majorizes $\mathfrak{c}(\sigma)$ and catalytic transformation into $\mathfrak{c}(\sigma)$ from a pure state is also achievable. In other words, $\mathfrak{c}(\sigma)$ is the most random state that can be catalytically created with σ from a pure state. Let us call $\mathfrak{c}(\sigma)$ the randomness-exhausting output (REO) of σ. Since every Rényi entropy is Schur-concave, and the maximum (global) entropy production of a quantum channel is achieved with a pure state input [19], $S_\alpha(\mathfrak{c}(\sigma))$ is the the maximum Rényi entropy catalytically extractable from randomness source σ, and we call it the catalytic Rényi entropy $S_\alpha^\diamond(\sigma)$ of σ. $S_\alpha^\diamond(\sigma)$ has the following explicit expression in terms of the catalytic decomposition of σ:

$$S_\alpha^\diamond(\sigma) := \frac{1}{1-\alpha} \log_2 \left[\sum_i \lambda_i^\alpha r_i^{2-\alpha} \right]. \tag{13}$$

The important extreme cases are the catalytic von Neumann entropy $\lim_{\alpha \to 1} S_\alpha^\diamond(\sigma) = S^\diamond(\sigma) := -\sum_i \lambda_i r_i \log_2(\lambda_i / r_i)$, the min-catalytic entropy $\lim_{\alpha \to \infty} S_\alpha^\diamond(\sigma) = S_{\min}^\diamond(\sigma) := -\log_2[\max_i \lambda_i / r_i]$, and the max-catalytic entropy $\lim_{\alpha \to 0+} S_\alpha^\diamond(\sigma) = S_{\max}^\diamond(\sigma) := \log_2[\sum_i r_i^2]$. The catalytic entropies are important because of the following operational meaning.

Theorem 3 ([19]). The maximum amount of catalytically extractable Rényi entropy of order $\alpha \geqslant 0$ from a randomness source σ is its catalytic Rényi entropy defined as $S_\alpha^\diamond(\sigma)$.

Although it is known that, for a given quantum channel, more entropy is produced on a purification than on a mixed state, it could be still cumbersome to find an input state that yields the maximum entropy production for a given channel. However, if our intention is to check if the channel

produces entropy at all, then the following proposition says that inputting a maximally entangled state is enough. See Appendix for proof.

Proposition 2. A catalytic map cannot generate randomness with any input state if and only if it cannot produce randomness by acting on a part of a maximally entangled state.

C. Distributed catalytic randomness

In the last section, we only considered randomness sources that are in isolation from other systems. In this section, we generalize catalysis of randomness to correlated randomness sources. The necessity of such a generalization naturally arises when multiple parties share correlated data to implement some distributed information processing task. There are abundant examples of correlated randomness source. Multiple copies of the same book are all correlated and altering one copy can be physically detected when the copies are compared. People also share secret keys to encrypt another shared data by using it. Oftentimes, one does not only use the information of the system they are directly in contact with, but also utilize its relation with the outer world. One may also only have access to small part of large system but still want to restrict the information flow into the whole system.

Correlated information sources are also generic in the quantum setting, too. Treating systems correlated with a given information source not explicitly could cause huge confusion, as it was exemplified in the controversy around Mølmer's conjecture [45]. A way to resolve the confusion is explicitly to take account of the correlation, especially the entanglement, between laser light and the laser device. A detailed discussion can be found in the Appendix.

The detailed setting of distributed catalysis of randomness is as follows. Instead of one party, let there be two parties, Alice and Bob, separated in different laboratories. They start with an initial bipartite state $\rho_{A_SB_S}$, and they are provided with a bipartite state $\sigma_{A_CB_C}$ as a randomness source that they should return unchanged. Here, S stands for system and C stands for catalyst. Alice can only control A_SA_C and Bob can only control B_CB_S. They try to transform their initial state into some other state $\mathcal{N}(\rho_{A_SB_S})$ without altering the randomness source. We allow no communication between them in this process because communication establishes new shared randomness sources between them. Allowing classical communication and local operations without forming correlation between system and catalyst leads to catalysis of entanglement. We refer the readers to Refs. [46–48] for more information.

In the quantum setting, Alice will apply unitary operator U_A to A_SA_C, and Bob will apply U_B to B_SB_C. Just like the original catalysis scenario, they are required to preserve $\sigma_{A_CB_C}$ after the interaction, regardless of their initial state $\rho_{A_SB_S}$. This requirement can be summarized as

$$\mathrm{Tr}_{A_CB_C}[\mathrm{Ad}_{U_A\otimes U_B}(\rho_{A_SB_S}\otimes\sigma_{A_CB_C})]=\mathcal{N}(\rho_{A_SB_S}), \tag{14}$$

with some quantum channel $\mathcal{N}\in\mathfrak{C}(A_SB_S)$ and

$$\mathrm{Tr}_{A_SB_S}[\mathrm{Ad}_{U_A\otimes U_B}(\rho_{A_SB_S}\otimes\sigma_{A_CB_C})]=\sigma_{A_CB_C} \tag{15}$$

for all $\rho_{A_SB_S}\in\mathfrak{S}(A_S\otimes B_S)$ (see Fig. 3). We will call this type of catalysis a *distributed catalysis* of randomness and when

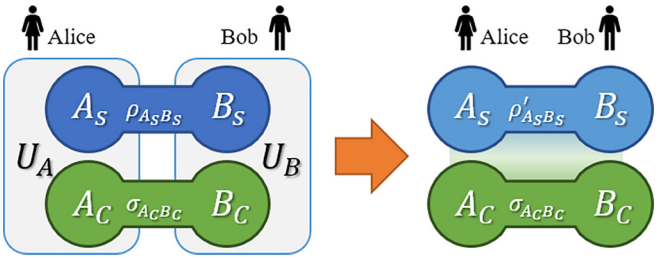


FIG. 3. Distributed catalysis of quantum randomness. Alice and Bob, separated in different laboratories, utilize the bipartite state $\sigma_{A_CB_C}$ as a catalyst to transform $\rho_{A_SB_S}$ into $\rho'_{A_SB_S}=\mathcal{N}(\rho_{A_SB_S})$. On the right side, A_SB_S and A_CB_C could be correlated (depicted as a colored box between them) but the marginal state of A_CB_C stays in the initial state $\sigma_{A_CB_C}$.

it is needed to emphasize it, we call $\sigma_{A_CB_C}$ in this situation the *distributed randomness source*. We say that the catalysis unitary operator pair (U_A, U_B) is compatible with $\sigma_{A_CB_C}$ if (15) holds, and vice versa, and we say that they are compatible up to local unitary when there exists some $V_X\in\mathfrak{U}(X_C)$ for $X=A,B$ such that (15) holds with the right-hand side substituted with $\mathrm{Ad}_{V_A\otimes V_B}(\sigma_{A_CB_C})$. If we need to emphasize, we will call the special case $V_X=\mathbb{1}_{X_S}$ for $X=A,B$ the *canonical* case. When we focus on the action of each local party, we say that $U\in\mathfrak{U}(A_SA_C)$ is compatible with $\sigma_{A_CB_C}$ on B_S when $(U,\mathbb{1}_{B_SB_C})$ is compatible with $\sigma_{A_CB_C}$.

We can observe that distributed catalysis can be considered a special case of catalysis of randomness. Thus, Theorem 2 applies here too, hence, $U_A\otimes U_B$ must be catalytic, implying that U_A and U_B must be catalytic unitary operators themselves. Also, for $\sigma_{A_CB_C}$ to be compatible with $U_A\otimes U_B$, it must be that $[U_A\otimes U_B, \mathbb{1}_{A_SB_S}\otimes\sigma_{A_CB_C}]=0$. In local catalysis of randomness, a randomness source cannot yield randomness if and only if it is a pure state. Does the same result hold in distributed catalysis too?

Now, we observe that, in distributed catalysis, each party can only interact locally with their shared randomness source without altering the global state of it. Considering that no communication between them is allowed, we could guess that each of them must leave the correlated source intact, independent of each other's action. What is the condition for this to be possible? It was recently proved that if a subsystem is not even partially classical, meaning that no nontrivial projective measurement can be implemented on its local system, then the quantum state shared with it is sensitive to changes caused by unital quantum channels [49].

Lemma 1 ([49]). For any quantum state ρ_{AB}, $(\mathcal{N}_A\otimes\mathrm{id}_B)(\rho_{AB})\neq\rho_{AB}$ for any unital channel $\mathcal{N}_A\neq\mathrm{id}_A$ if and only if ρ_{AB} is a TQ-Q state.

It is because quantum correlation can detect local randomizing disturbance and it hinders the catalytic utilization of the randomness source. From these observations, we can identify the bipartite states that cannot yield randomness and show that there are quantum states that are not pure but unable to provide any randomness catalytically.

Theorem 4. No randomness can be catalytically extracted from a bipartite quantum state if and only if it is TQ-TQ.

The reason why catalysis sectors were identified in local catalysis of randomness was that they are the maximum sub-

space within which nontrivial unital channels can be applied in an unconstrained fashion without affecting the state of randomness source (see Fig. 2). The same idea can be applied in distributed catalysis of randomness, and we should identify the maximum subspaces within which local parties can apply unital channels without any constraint and the danger of altering the state of the given randomness source.

At this point, we introduce the concept of essential decomposition, which provides the canonical decomposition of a partially classical system into classically distinguishable sectors (subspaces of the Hilbert space of each local system) for a PC-Q state. In other words, when we say a PC-Q state is "partially classical," we mean that there is a local projective measurement that does not perturb the state, and the essential decomposition identifies what is the maximally informative measurement of such kind.

Definition 1. Let $\rho_{AB} \in \mathfrak{S}(AB)$ be a bipartite quantum state. A decomposition $A = \bigoplus_i A_i^P \otimes A_i^Q$ is the *essential decomposition* of A for ρ_{AB}, if, for some quantum states $\rho_{A_i^P}$ and $\rho_{A_i^Q B}$, respectively, on A_i^P and $A_i^Q B$,

$$\rho_{AB} = \sum_i p_i \pi_{A_i^P} \otimes \rho_{A_i^Q B}, \tag{16}$$

for some probability distribution p_i and TQ-Q states $\rho_{A_i^Q B}$ such that any unital channel $\mathcal{N} \in \mathfrak{UC}(A)$ that fixes ρ_{AB} preserves every subspace A_i and each $\mathcal{N}|_i$ factorizes into $\mathcal{N}|_{A_i} = \mathcal{N}|_{A_i^P} \otimes \mathrm{id}_{A_i^Q}$ where each $\mathcal{N}|_{A_i^P}$ is unital.

We let $A_i := A_i^P \otimes A_i^Q$ and call them the *classical sectors* of A. We will also call A_i^P the local part of it and A_i^Q the (quantumly) correlated part. We will call the corresponding decomposition of $\rho_{AB} = \sum_i p_i \rho_{A_i^P} \otimes \rho_{A_i^Q B}$ the essential decomposition of ρ_{AB} on A. One could observe that the essential decomposition is related with the structure of entropy nonincreasing state under unital channels [50,51].

The essential decomposition captures the intuitive idea of "classical sectors" of PC-Q states as the following theorem shows. It says that any "randomizing transformation" acting on the local part of a PC-Q state, represented by unital maps, that preserves the whole state must respect the classical structure of the partially classical system. Additionally, it says that the unital map can act nontrivially only when there is no correlation in each classical sector.

Theorem 5. The essential decomposition exists and is unique for each quantum state.

See Appendix, Sec. A 5, for a deeper analysis of essential decomposition. Now we introduce a bipartite generalization of catalytic decomposition that we will call the *distributed catalytic decomposition* through the essential decomposition.

Definition 2. Let ρ_{AB} be a bipartite quantum state with the essential decompositions of $A = \bigoplus_i A_i^P \otimes A_i^Q$ and $B = \bigoplus_j B_j^P \otimes B_j^Q$. The distributed catalytic decomposition (DCD) of a bipartite quantum state $\rho_{AB} \in \mathfrak{S}(AB)$ is the decomposition of the following form:

$$\rho_{AB} = \bigoplus_{i,j} p_i q_j \pi_{A_i^P} \otimes \rho_{A_i^Q B_j^Q} \otimes \pi_{B_j^P}. \tag{17}$$

Since the essential decompositions are unique for A and B, respectively, the DCD is also unique for ρ_{AB}. This definition is slightly more complicated than the definition of the catalytic decomposition for single-partite systems, but it is required to identify the basic building blocks of a distributed randomness source. Most notably, each component in the DCD is still compatible with any catalysis unitary operators of the original catalysts, just as every component in the catalytic decomposition of single-partite catalysts is compatible with any catalysis unitary operator compatible with the catalyst before the decomposition. (See Appendix for more information.) This observation leads us to the following definition of the *distributed catalytic Rényi entropy*.

The DCD of a bipartite quantum state suggests that only the "classical parts" $\rho_{A_i^P B_j^P}$ of the state are available for catalysis, while the "quantum parts" $\rho_{A_i^Q B_j^Q}$ are inaccessible. However, an interesting observation one could make is that not every $\rho_{A_i^Q B_j^Q}$ has to be TQ-TQ. It is because the sensitiveness of the quantum parts does not from their individual form but from their collective behavior. Because of their sensitiveness, effectively one can ignore the quantum part of ρ_{AB} when assessing its catalytic power.

Definition 3. For the DCD of ρ_{AB} given in (17), the distributed catalytic Rényi entropy $S_\alpha^{\diamond\diamond}(\rho_{AB})$ of ρ_{AB} is defined as follows:

$$S_\alpha^{\diamond\diamond}(\rho_{AB}) := S_\alpha(\mathfrak{d}(\rho_{AB})). \tag{18}$$

Here, $\mathfrak{d}(\rho_{AB}) := \bigoplus_{i,j} p_i q_j \pi_{A_i^P}^{\otimes 2} \otimes \pi_{B_j^P}^{\otimes 2}$ is the *declocalized randomness-exhausting output* (DREO) of ρ_{AB}.

Just like the catalytic entropies, the distributed catalytic entropies also have the same kind of operational meaning. Proof of the following result can be found in the Appendix, Sec. A 6.

Proposition 3. The maximum Rényi entropy that can be catalytically extracted from a distributed randomness source $\sigma_{A_C B_C}$ is its distributed catalytic Rényi entropy.

Hence, we successfully quantified the amount of catalytically extractable randomness in the distributed setting. This analysis of static but distributed randomness sources can be directly applied to dynamical randomness sources through the Choi-Jamiołkowski isomorphism in the next section.

Note that if there is no correlation in the distributed randomness source, i.e., $\sigma_{A_C B_C} = \sigma_{A_C} \otimes \sigma_{B_C}$, then the distributed catalysis simply reduces to two independent local catalyses with $S_\alpha^{\diamond\diamond}(\sigma_{A_C} \otimes \sigma_{B_C}) = S_\alpha^{\diamond}(\sigma_{A_C}) + S_\alpha^{\diamond}(\sigma_{B_C})$.

We remark that multipartite generalization of distributed catalysis or randomness is straightforward. Each party in distributed catalysis behaves locally and there are no collective maneuvers needed. Hence, the distributed catalytic decomposition is simply the collection of the essential decomposition of each party, so for an N-partite quantum state $\rho_{12\ldots N}$, with each party $X = 1, 2, \ldots, N$, one can partition the N parties into $X : \bar{X}$ and find the essential decomposition. The rest of the procedures, e.g., calculating the catalytic entropies and implementing the catalysis, are immediate once the distributed catalytic decomposition is found.

D. Dynamical catalytic randomness

So far, we have only considered static randomness sources, whose classical examples include random number tables and

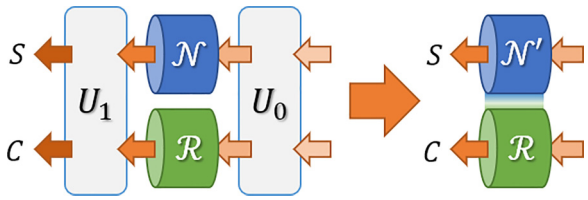


FIG. 4. Dynamical catalysis of quantum randomness. Input and output systems of the target quantum channel $\mathcal{N}$ and the catalyst channel $\mathcal{R}$ unitarily interact. The resultant bipartite channel on SC might correlate two systems, but the catalyst channel $\mathcal{R}$ stays in its original form when one ignores the system S.

secret keys. In a more realistic situation, however, *dynamical* sources of randomness are common. For example, when a group of people are playing a tabletop board game, they do not usually play the game with a random number table prepared in advance; they roll a dice to generate randomness on the spot. For example, a record of the result of a previously ($|X|$-faced) dice roll can be modeled by a static state, i.e., the maximally mixed state π_X, but the action of rolling a dice can be modeled by the depolarizing map $\mathcal{R} \in \mathfrak{C}(X)$,

$$\mathcal{R}(\rho) = \pi_X \mathrm{Tr}[\rho], \tag{19}$$

for any initial state ρ of the dice with classical system X. Even in this case, we claim that catalysis of randomness utilization is still required. In other words, if you have no idea for which game it is used and only observe the dice rolling, then the channel you used as a randomness source must retain its original form. This "information nonleaking" property is very important for characterizing pure randomness utilization [19], and we require that a randomness source must not remember for which operation it was used and must retain its probabilistic properties regardless of the result of the implemented operation. This requirement can be formulated as follows.

When one tries to catalytically transform a quantum channel $\mathcal{N}$ into $\Theta(\mathcal{N})$ by using a quantum channel $\mathcal{R}$ as a randomness source, we assume that only applying bipartite unitary operators to input and output systems of $\mathcal{N}$ and $\mathcal{R}$ is allowed as no randomness producing operation is allowed other than $\mathcal{R}$.

We will model the complete loss of information about a dynamical quantum process with the *supertrace*, denoted by $\mathfrak{Tr}$, which represents completely losing information on input and output systems of a given process, i.e., $\mathfrak{Tr}(\mathcal{N}) := \mathrm{Tr}[\mathcal{N}(\pi_X)]$ (see Sec. II A).

In this work, we will mainly focus on the case where the target channel $\mathcal{N}$ and the randomness source channel $\mathcal{R}$ act at the same time. In other words, they act on their respective systems *in parallel*. Formally, we say a superchannel $\Theta \in \mathfrak{SL}(S)$ is *catalytic* when there is a bipartite superunitary operation $\Omega \in \mathfrak{L}(SC)$ and a channel $\mathcal{R} \in \mathfrak{C}(C)$ such that

$$\mathfrak{Tr}_C \Omega(\mathcal{N} \otimes \mathcal{R}) = \Theta(\mathcal{N}) \tag{20}$$

and

$$\mathfrak{Tr}_S \Omega(\mathcal{N} \otimes \mathcal{R}) = \mathfrak{Tr}[\mathcal{N}]\mathcal{R} \tag{21}$$

for all $\mathcal{N} \in \tilde{\mathfrak{C}}(S)$ (see Fig. 4). (See Appendix, Sec. A 1, for a discussion on the set of $\mathcal{N}$.) We will call the whole process a (dynamical) *catalysis* and say that $\mathcal{R}$ is used as a *randomness source* (channel) or a *catalyst*. If a superunitary operation Ω can be used to implement a catalytic superchannel, then it is called a *catalysis superunitary operation*, or it is said to be *catalytic*. A randomness source channel $\mathcal{R}$ and a catalysis superunitary operation Ω is said to be compatible with each other when (20) and (21) hold for some superchannel Θ and every $\mathcal{N} \in \mathfrak{C}(S)$.

Since a superunitary Ω can be decomposed into the actions of preunitary U_0 and postunitary U_1 [24,25], i.e., $\Omega(\mathcal{N}) = \mathrm{Ad}_{U_1} \circ \mathcal{N} \circ \mathrm{Ad}_{U_0}$, therefore (20) and (21) can be expressed as $\mathfrak{Tr}_C[\mathrm{Ad}_{U_1} \circ \mathcal{N} \otimes \mathcal{R} \circ \mathrm{Ad}_{U_0}] = \Theta(\mathcal{N})$ and $\mathfrak{Tr}_S[\mathrm{Ad}_{U_1} \circ \mathcal{N} \otimes \mathcal{R} \circ \mathrm{Ad}_{U_0}] = \mathcal{R}$. By considering the Choi matrices, we get the following expressions:

$$\mathrm{Tr}_{CC'}\left[\mathrm{Ad}_{U_1 \otimes U_0^T}\left(J^{\mathcal{N}}_{SS'} \otimes J^{\mathcal{R}}_{CC'}\right)\right] = J^{\Theta(\mathcal{N})}_{SS'} \tag{22}$$

and

$$\mathrm{Tr}_{SS'}\left[\mathrm{Ad}_{U_1 \otimes U_0^T}\left(J^{\mathcal{N}}_{SS'} \otimes J^{\mathcal{R}}_{CC'}\right)\right] = J^{\mathcal{R}}_{CC'} \tag{23}$$

for all $\mathcal{N} \in \tilde{\mathfrak{C}}(S)$. Note that every $\rho_{XX'} \in \mathfrak{S}(X \otimes X')$, there exists a $\mathcal{M} \in \tilde{\mathfrak{C}}(X)$ such that $J^{\mathcal{M}}_{XX'} \propto \rho_{XX'}$, and vice versa. It follows that (22) and (23) are equivalent to the following requirements, in turn:

$$\mathrm{Tr}_{CC'}\left[\mathrm{Ad}_{U_1 \otimes U_0^T}\left(\rho_{SS'} \otimes J^{\mathcal{R}}_{CC'}\right)\right] = \mathbb{J}[\Theta](\rho_{SS'}) \tag{24}$$

and

$$\mathrm{Tr}_{SS'}\left[\mathrm{Ad}_{U_1 \otimes U_0^T}\left(\rho_{SS'} \otimes J^{\mathcal{R}}_{CC'}\right)\right] = J^{\mathcal{R}}_{CC'} \tag{25}$$

for every $\rho_{SS'} \in \mathfrak{S}(S \otimes S')$. Here, U_1 acts on SC and U_0^T acts on $S'C'$. Now, we can observe that (20) and (21) are only a special case of (14) and (15) after some change of notations, thus, we can conclude that Ω is catalytic if and only if $U_0^{T_S} \otimes U_1^{T_{C'}}$ is catalytic. It is equivalent to saying both U_0 and U_1 are catalytic themselves.

Theorem 6. A superunitary operation $\Omega : \mathcal{N} \mapsto \mathrm{Ad}_{U_1} \circ \mathcal{N} \circ \mathrm{Ad}_{U_0}$ is catalytic if and only if both U_0 and U_1 are catalytic. Also, Ω is compatible with $\mathcal{R}$ if and only if $U_0 \otimes U_1^T$ is compatible with $J^{\mathcal{R}}_{CC'}$, i.e.,

$$\left[U_1 \otimes U_0^T, \mathbb{1}_{SS'} \otimes J^{\mathcal{R}}_{CC'}\right] = 0. \tag{26}$$

The vanishing commutator condition (26) follows from Theorem 2. When $\mathcal{E}(\rho) = \pi_C \mathrm{Tr}[\rho]$ is the depolarizing map on C, its Choi matrix is $J^{\mathcal{E}}_{CC'} = \pi_C \otimes \pi_{C'}$, therefore, $[U_1 \otimes U_0^T, \mathbb{1}_{SS'} \otimes J^{\mathcal{E}}_{CC'}] = 0$ for any U_0 and U_1. It implies that, similarly to that every catalysis unitary operator is compatible with the maximally mixed state, every catalysis superunitary operation is compatible with the depolarizing map. In other words, a fair (quantum) dice roll can always provide randomness without leaking information.

There could be many possible measures of randomness extracted from randomness source, but from the formal similarity of static and dynamical catalysis, we will use $S_\alpha(J^{\Theta(\mathcal{N})}_{SS'}) - S_\alpha(J^{\mathcal{N}}_{SS'})$, for every $\alpha \geqslant 0$, as a measure of extracted randomness. When $\alpha = 1$, $S_\alpha(J^{\mathcal{N}}_{SS'})$ is called the map entropy $S^{\mathrm{map}}(\mathcal{N})$ of channel $\mathcal{N}$ [50,52]. Theorem 6 immediately yields an upper bound to the amount of randomness catalytically extractable from a randomness source channel $\mathcal{R} \in \mathfrak{C}(C)$, namely, $S_\alpha(J^{\Theta(\mathcal{N})}_{SS'}) - S_\alpha(J^{\mathcal{N}}_{SS'}) \leqslant S^{\diamond}_\alpha(J^{\mathcal{R}}_{CC'})$, where

$J^{\mathcal{R}}_{CC'}$ is interpreted to be an element of $\mathfrak{B}(CB \otimes C')$ without any superselection rule. However, unitary operators of the form $U_1 \otimes U_0^T$ are not of the most general form of 4-partite unitary operator that can act on $SS'CC'$, it is not evident if $S^{\diamond}_{\alpha}(J^{\mathcal{R}}_{CC'})$ is the maximally extractable Rényi entropy extractable from $\mathcal{R}$, counted with the increase of the Rényi entropy of the Choi matrix.

However, from its equivalence with distributed catalysis of randomness, we can simply use the distributed catalytic entropies to measure the maximally extractable randomness of arbitrary channel.

Definition 4. The catalytic Rényi entropy $S^{\diamond}_{\alpha}(\mathcal{C})$ of a quantum channel $\mathcal{R} \in \mathfrak{C}(C)$ is

$$S^{\diamond}_{\alpha}(\mathcal{R}) = S^{\diamond\diamond}_{\alpha}\left(J^{\mathcal{R}}_{CC'}\right). \tag{27}$$

The framework of dynamical quantum randomness encompasses the static and local quantum randomness too. Any static randomness source modeled as a quantum stat σ_C can be described as preparation channel $\mathcal{P}(\alpha) = \alpha\sigma$ in $\mathfrak{C}(\mathbb{C}, C)$, whose Choi matrix is simply $\mathcal{J}^{\mathcal{P}}_{\mathbb{C}C} = \sigma$, hence, $S^{\diamond}_{\alpha}(\mathcal{P}) = S^{\diamond\diamond}_{\alpha}(\mathcal{J}^{\mathcal{P}}_{\mathbb{C}C}) = S^{\diamond}_{\alpha}(\sigma)$.

We, now, leave a remark on a more general case of catalysis of dynamical quantum randomness. In general, a target channel and a randomness source channel need not be applied simultaneously, and one preceding another is obviously possible. For example, if we assume that the randomness source is applied after the target channel, then we should modify the catalysis conditions as follows. For all $\mathcal{N} \in \tilde{\mathfrak{C}}(S)$,

$$\mathfrak{Tr}_C \mathcal{U}_3 \circ \mathcal{R}_C \circ \mathcal{U}_2 \circ \mathcal{N}_S \circ \mathcal{U}_1 = \Theta(\mathcal{N}) \tag{28}$$

and

$$\mathfrak{Tr}_S \mathcal{U}_3 \circ \mathcal{R}_C \circ \mathcal{U}_2 \circ \mathcal{N}_S \circ \mathcal{U}_1 = \mathfrak{Tr}[\mathcal{N}]\mathcal{R}, \tag{29}$$

with some superchannel $\Theta \in \mathfrak{SC}(S)$ and some unitary operations $\mathcal{U}_i \in \mathfrak{U}(SC)$ for $i = 1, 2, 3$. One can see that the unitary operation $\mathcal{U}_2$ in the middle hinders transforming this process into a distributed catalysis process. Although we can show that $\mathcal{U}_1$ must be a catalytic unitary operation by tracing out both sides of (29), still many other parts of this process are left for further inquiry. Hence, we leave the complete characterization of dynamical catalysis of this type as an open question for the moment. Nonetheless, when there is no randomness in the randomness source $\mathcal{R}$, i.e., if $\mathcal{R}$ is a unitary process, then one can rump $\mathcal{U}_2 \circ \mathcal{R}_B \circ \mathcal{U}_1$ into a single unitary operation, hence it reduces to the dynamical catalysis discussed before, with trivial randomness source, id_B. This fact will be used when we prove the no-stealth theorem in a later section.

E. Correlated catalytic randomness and semantic information

So far, we have only considered catalysts that are initially prepared in a state independent of the target system that is going to be catalytically transformed [see (6), (14), and (20)]. From the perspective of randomness as information, it is not the most generic case of information utilization since many information sources provide useful information about the object one is going to interact with. In other words, most of the useful information is *semantic*. Therefore, it is natural to ask what happens if we lift this "Markovian" assumption and consider catalysts that are correlated with the target system from the beginning.

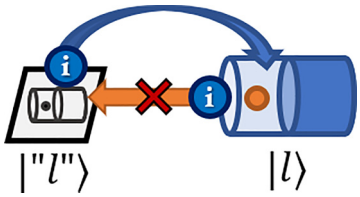


FIG. 5. Semantic information utilization demonstrated in Landauer's erasure principle. The information carrier C, depicted as a piece of paper, provides the information about the state of the gas molecule G. However, in the course of the interaction, no information flows from G to C. Here, the fact that two systems C and G start as correlated systems is important for semantic information utilization.

In previous sections, we have observed that randomness captures the probabilistic aspect of information that is independent of its semantics. However, the everyday notion of information heavily depends on the semantic properties of information, hence, one might find that the discussion of previous sections misses a large portion of discussion on information. Indeed, the semantic side and the quantitative side of information are notorious for being hard to unify. Nevertheless, in this section, we venture into the realm of semantic information and attempt to spell out the formalism of semantic information in our framework of catalytic randomness.

Floridi [53] defines semantic information as well-formed, meaningful, and truthful data. As Shannon's approach to information, which we take in the quantum setting, is probabilistic rather than propositional, we will focus on the "meaningful" part. This definition immediately assumes the existence of a reference system that is related with the carrier of semantic information, as data cannot be meaningful when it is isolated from the outer world. For example, we consider a recipe for some dish meaningful because the recipe is correlated with the properties of the ingredients, which appear random in the Bayesian sense to those who are a novice at cooking. Another example is maps: a map is meaningful compared to any other picture because it corresponds to the geography of the real world.

Therefore, we will try to be value neutral when it comes to deciding what counts as meaningful and claim that the existence of correlation between information carrier and the object you are going to interact with, the target system, is the key characteristic of semantic information in the context of our formalism. The situation is similar with distributed catalysis of randomness, but there is an important difference that interaction between information source and target system is allowed and the correlation between the two systems need not be preserved because the target system is now allowed to be altered. Recall that only the state of information source is required to be preserved in our definition of (pure) information utilization.

One of the most typical examples can be found in Landauer's erasure principle (see Fig. 5). Suppose that a gas molecule G in a piston can be either of two states of being in the left half of the piston $|l\rangle_G$ or being in the right half $|r\rangle_G$.

Let the molecule be in the maximally mixed state,

$$\sigma_G = \tfrac{1}{2}|l\rangle\langle l|_G + \tfrac{1}{2}|r\rangle\langle r|_G. \tag{30}$$

A common precondition of Landauer's erasure principle is the acquisition of information about the position of the molecule. Acquisition of information requires the existence of an information carrier that gets correlated with its reference, hence, we spell it out as C, i.e., σ_G is the marginal state of

$$\sigma_{CG} = \tfrac{1}{2}|\text{“}l\text{”}\rangle\langle\text{“}l\text{”}|_C \otimes |l\rangle\langle l|_G + \tfrac{1}{2}|\text{“}r\text{”}\rangle\langle\text{“}r\text{”}|_C \otimes |r\rangle\langle r|_G. \tag{31}$$

The states $|\text{“}l\text{”}\rangle_C$ and $|\text{“}r\text{”}\rangle_C$ are orthogonal to each other and contain the classical information about the state of G. By conditioning on the state of C, we can initialize the molecule G by applying a reversible process, so that the final state of CG is

$$\left(\tfrac{1}{2}|\text{“}l\text{”}\rangle\langle\text{“}l\text{”}|_C + \tfrac{1}{2}|\text{“}r\text{”}\rangle\langle\text{“}r\text{”}|_C\right) \otimes |r\rangle\langle r|_G. \tag{32}$$

As one can see, we only used the system C as an information source so the state of C is left unaltered but that of G is changed. Observe that the end result is all the entropy being concentrated in C, which corresponds to the entropy production according to Landauer's erasure principle.

Our way of modeling semantic information requires two systems: the information source that only provides information and the target system that can be physically affected. If we admit this asymmetry between them, then we need a mathematical characterization of their difference. This distinction is important as Korzybski said "A map is not the territory" [54]. In the case of (31), information carrier C is not the gas molecule G itself.

As we have seen in Theorem 1, we could expect that there exist different characterizations of semantic information in each picture, dynamical (Heisenberg) and static (Schrödinger). To construct the dynamical characterization, let us go back to the example of Landauer's erasure principle. When we used the information source, our initial intention was initializing the position of the gas molecule. However, we could always change our mind and do whatever we want with the information we acquired from the source other than initializing the gas molecule into the right half of the cylinder. We claim that this alternation of plan, strictly happening to the action on the target system, must not affect the information source. This requirement, which is a generalization of the interventionist definition of information utilization, condition (i) of Theorem 1, can be expressed concretely as follows. (S:A∼C in what follows stand for 'Semantic information: A∼C'.).

Definition 5 (S:A). We say that a bipartite unitary operation $\mathcal{U} = \mathrm{Ad}_U$ with $U \in \mathfrak{U}(AB)$ utilizes *(semantic) information* of B in a bipartite state σ_{AB} when for any superchannel $\Theta \in \mathfrak{SC}(A)$, $\mathcal{U}_\Theta := (\Theta_A \otimes \mathfrak{id}_B)(\mathcal{U})$ does not affect B, i.e., there exists $\eta_B \in \mathfrak{S}(B)$ such that for all $\Theta \in \mathfrak{SC}(A)$,

$$\mathrm{Tr}_A[\mathcal{U}_\Theta(\sigma_{AB})] = \eta_B. \tag{33}$$

We remark that such η_B in (33) must be unitarily similar to σ_B (see Appendix). For the static characterization, imagine that we redistribute the information of system A to a larger joint system RA by applying some channel $\mathcal{N}_{A\to RA}$. Because of the correlation formed between R and A, when static information of A is leaked to B by the interaction between A and B, there will be a change in the correlation between R and B. Based on this speculation, we can formulate the following definition in the same spirit with condition (iii) of Proposition 1.

Definition 6 (S:B). We say that a bipartite unitary operation $\mathcal{U} = \mathrm{Ad}_U$ with $U \in \mathfrak{U}(AB)$ utilizes *(semantic) information* of B in a bipartite state σ_{AB} when for any state $\tau_{RAB} = (\mathcal{N}_{A\to RA} \otimes \mathrm{id}_B)(\sigma_{AB})$ with a quantum channel $\mathcal{N}_{A\to RA}$, we have

$$\mathrm{Tr}_A[(\mathrm{id}_R \otimes \mathcal{U})(\tau_{RAB})] = (\mathrm{id}_R \otimes \mathrm{Ad}_V)(\tau_{RB}), \tag{34}$$

with some $V \in \mathfrak{U}(B)$.

Alternatively, since we have already developed the definition of using only information of a local system in a multipartite quantum state, one may rather import the definition of distributed catalysis of randomness and claim the following.

Definition 7 (S:C). We say that a bipartite unitary operation $\mathcal{U} = \mathrm{Ad}_U$ with $U \in \mathfrak{U}(AB)$ utilizes *(semantic) information* of B in a bipartite state σ_{AB} when U is compatible with σ_{AB} on B up to local unitary as a distributed catalyst.

The main result of this section is that these seemingly different definitions of semantic information are equivalent. In other words, utilization of semantic information is fundamentally not different from distributed catalysis of randomness. Hence, "using only information of system B in correlated systems $ABC\ldots$" can be universally discussed without paying attention to which is allowed to be altered and which system is used as an information source other than B. This can be concretely expressed as follows.

Theorem 7. Definitions (S:A), (S:B), and (S:C) are equivalent.

The proof is in the Appendix. This result unifies many notions of information usage introduced so far as it will be demonstrated afterwards. So, we will simply drop "semantic" when we refer to this type of information usage. First of all, we can observe that nonsemantic (quantum) information is a special case of semantic information by considering uncorrelated $\sigma_{AB} = \sigma_A \otimes \sigma_B$.

Without loss of generality, unless we explicitly state "up to local unitary," we will only consider the "canonical" cases; we assume that no nontrivial unitary operation is applied on B after the interaction for the sake of simplicity.

One can observe that this characterization of semantic information utilization is actually equivalent to catalysis of *partially depleted* randomness source, the characterization of which was an open problem raised in Ref. [19]. It is because now we consider randomness sources that are initially correlated with the target system, and we concluded that randomness sources are consumed by forming correlation with its user. It is in contrast with the previous sections where randomness sources were assumed to be initially in a product state with the target system. Therefore, we can consider utilization of semantic information is also in the formalism of catalytic quantum randomness.

We already know that a bipartite state σ_{AB} that is Q-TQ cannot yield catalytic randomness on B. Hence, we get the following corollary which shows that utilization of semantic quantum information is impossible when you cannot use nonsemantic quantum information when you are required not

to disturb the information source, just as it is in the classical setting.

Corollary 1. If σ_{AB} is Q-TQ, then no nonproduct bipartite unitary operation can utilize only semantic information of B in σ_{AB}.

An important example of quantum state that is Q-TQ is pure states with full Schmidt rank. Hence, as pure states were not useful for distributed catalysis of randomness, they also do not allow utilization of pure semantic information. Note that the requirement of full Schmidt rank can be circumvented by limiting the local Hilbert spaces to the support of each marginal state, as they are the only physically relevant Hilbert spaces.

One may wonder, since utilization of information of B in σ_{AB} allows for information flow from A to AB and from AB to B, if it is possible to circumvent the restriction of one-way information flow by breaking the process in two steps so that one has net flow of information from A to B. Indeed, even if M and N are catalytic unitary operators compatible with σ_B, the same need not hold for their composition NM.

However, such circumvention is impossible after all; one lesson we learned from the observations of previous sections is that one should be explicit about reference systems when one treats information from the internal information perspective. First of all, if system A starts from the maximally mixed state uncorrelated with any other systems, then the action of arbitrary catalytic unitary compatible with the state of B does not change the state of joint system AB. This is mainly because, without a method to track information that was originally stored in A, the ostensible information exchange between A and B yields no detectable difference.

Especially, if we start from an initial state $\rho_{RA} \otimes \sigma_B$ where R is a reference system of A and apply a catalytic unitary M_{AB}, then the information source B gets correlated with RA in the tripartite state $\sigma_{RAB} := (\mathrm{id}_R \otimes \mathrm{Ad}_M)(\rho_{RA} \otimes \sigma_B)$. Any unitary that utilizes the information of B in σ_{RAB} must be compatible with it on B, so, due to the following corollary of Theorem 7, the marginal state on RB does not change after the second step; it stays in the product state $\sigma_{RB} = \sigma_R \otimes \sigma_B$, which means that no information in A has been transferred to B.

Corollary 2. If $\mathbb{1}_R \otimes U_{AB}$ with $U \in \mathfrak{U}(AB)$ utilizes only semantic information of B in σ_{RAB}, then we have

$$\mathrm{Tr}_A[\mathrm{Ad}_{U_{AB}} \circ \mathcal{L}_A(\sigma_{RAB})] = \mathrm{Tr}_A[\mathcal{L}_A(\sigma_{RAB})] \tag{35}$$

for any $\mathcal{L} \in \mathfrak{L}(A)$. Especially, when $\mathcal{L} = \mathrm{id}_A$, we get

$$\mathrm{Tr}_A[\mathrm{Ad}_{U_{AB}}(\sigma_{RAB})] = \sigma_{RB}. \tag{36}$$

Even after this observation, we should remark that Definitions (S:A–C) do not guarantee that there is no influx of information into the randomness source at all. Information that was encoded in the correlation between the source and the target system can be concentrated into the source.

For example, in Landauer's erasure principle example we discussed [(30)-(32)], if we call the purifying system of (31) R, then $I(R:C)$ increases from 1 bit to 2 bits in the course of interaction between C and G, although we interpreted that no physical property other than information of C was used in the interaction. This is not because information flowed from G to C, but because the quantum entanglement of CG with R was concentrated into C after the interaction, albeit it was not accompanied by information flow from G to C.

We can interpret Definition (S:B) as that we characterize usage of (pure) semantic information of B in σ_{AB} as an interaction in which no information in AB that is *also present in A* flows to B. Corollary 3 easily follows from Definition (S:B). The proof is given in the Appendix.

Corollary 3. If a bipartite unitary operation $\mathcal{U} = \mathrm{Ad}_U$ with $U \in \mathfrak{U}(AB)$ utilizes *(semantic) information* of B in a bipartite state σ_{AB}, then, for any extension σ_{RAB} of σ_{AB} such that $I(R:A) = I(R:AB)$, we have

$$\mathrm{Tr}_A[(\mathrm{id}_R \otimes \mathcal{U})(\sigma_{RAB})] = \sigma_{RB}. \tag{37}$$

As it was briefly discussed in Ref. [19], a randomness source correlated with a target system can absorb randomness as demonstrated in the example of Landauer's erasure principle initializing a gas molecule. This is impossible with uncorrelated randomness sources since they can only increase the amount of randomness in the target system. Now, with the complete characterization of information usage in correlated quantum system, we can quantify the amount of randomness that a given source can absorb or yield.

Theorem 8. The least disordered state on A that can be made from σ_{AB} using B as an information source is $\sum_j (\sum_i p_i \lambda_j(\sigma_A^i))|j\rangle\langle j|_A$ where $\sigma_{AB} = \sum_i p_i \sigma_{AB}^i$ is the essential decomposition of σ_{AB} on B.

The proof can be found in the Appendix. Theorem 8 shows that quantum correlation hinders catalytic randomness absorption. Only classical correlation between A and B, which provides deterministic protocol to align eigenbases of conditional states of A, can reduce the amount of randomness in A without leaking any information of it to B. Why is it so? Classical information can be copied and deleted, unlike quantum information, so reduction of randomness in A can happen without any change in B when it is conditioned on classical data in B.

It is important that the results of this section do not imply that pure entangled states allow no utilization of semantic information of any form whatsoever. We expect that there is a multitude of information flow in generic quantum interactions, but they are often too complicated and complex in both directions or, sometimes, in ambiguous directions. Therefore, to understand the nature of (quantum) information flow, we only focused on directional information flow, which also has characterization as pure information usage. It is only that utilization of semantic information in pure multipartite states necessitates physical manipulation of information carrier.

We remark that our usage of the term *semantic information* may not completely match with others': we used the term to refer to information contained in a system that is correlated with another system the agent is going to interact with. This correlation differs from correlation among subsystems of an information source considered in distributed catalysis of randomness. Our definition of semantic information is not propositional, hence cannot be true or false on its own. Hence, our semantic information does not satisfy the criteria of Floridi [53]. One might think that our semantic information is closer to what Floridi calls *environmental* information.

Nevertheless, well-formedness can be expressed in terms of syntax, i.e., correlation between subsystems of information

source like that between a sentence and the language, and semantic information given as multipartite state is meaningful as it is informative about the world outside of information source and as truthful as the given state describes the physical reality. This type of probabilistic and correlational definition was necessary for the generalization to quantum semantic information. In summary, our "semantic information" does not refer to the essence of information that is exclusively semantic but refers to information that *could* contain semantic content.

F. Superselection rules in distributed and dynamical catalyses

The essential decomposition for bipartite states already identifies the partition of the Hilbert spaces that should be essentially classically distinguishable, but there could be additional classical structure imposed by the superselection rule of each system. This consideration was made in identifying catalysis sector for static and local catalysis of randomness in Sec. III B.

Note that the superselection sectors cannot intersect nontrivially with the correlated parts of essential decompositions as the quantum state in each subspace cannot be a PC-Q state, hence no superselection rule can be nontrivially imposed on it. Physically, superselection rules only limit the quantum advantage that can be taken from the local parts by partitioning a large uniform quantum state into the tensor product of smaller ones and forbidding nonclassical interaction between them. Since the catalytic entropies of quantum channels are defined through the distributed catalytic entropies of their corresponding Choi matrices, this new definition equally affects the definition of the dynamical catalytic entropies.

Definition of superselection rule provides a rather complicated way of treating randomness sources under superselection rules, but we show that actually it can be unified within the formalism of distributed catalysis of randomness. When $\{Q_i\}$ are projectors onto superselection sectors of A, then any given catalysis ρ_{AB} can be replaced with an extension ρ_{E_AAB} given as

$$\rho_{E_AAB} = \sum_i |i\rangle\langle i|_{E_A} \otimes (\mathrm{Ad}_{Q_i} \otimes \mathrm{id}_B)(\rho_{AB}), \tag{38}$$

when it is treated as a distributed randomness source. It can be interpreted that the classical observable i of A which is forbidden to be in superposition should be treated as a piece of classical data correlated with the quantum state being used as a catalyst. Thus, introduction of distributed catalysis of randomness nullifies the necessity of introducing C^* algebra formalism to discuss catalysts under superselection rules.

G. The no-stealth theorem

We consider the following dynamical generalization of the no-hiding theorem [55] or, equivalently, the no-masking theorem [56]. Consider that we want to hide a dynamical process $\mathcal{N} \in \tilde{\mathfrak{C}}(A)$ from two parties A and B by applying a global superunitary operation $\Omega \in \mathfrak{SC}(AB)$. (Alternatively one could consider an arbitrary multipartite channel $\mathcal{N}$. See Appendix, Sec. A 1.) By hiding, we mean that both of the marginal processes are constant regardless of the process $\mathcal{N}$

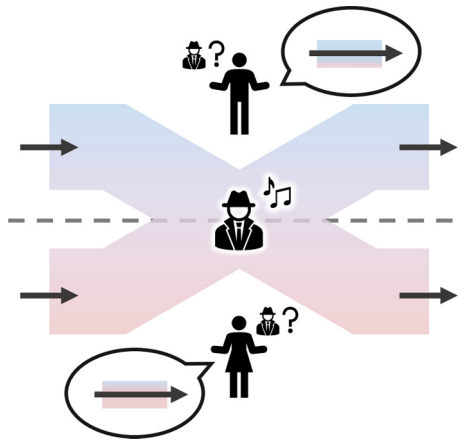


FIG. 6. Suppose that input and output systems of a given quantum operation are reversibly distributed to two systems. Is it possible to hide the identity of the operation from the respective systems? In other words, is it possible to implement quantum operations stealthily? The no-stealth theorem says that it is impossible.

(see Fig. 6), i.e.,

$$\mathfrak{Tr}_B[\Omega(\mathcal{N}_A \otimes \mathrm{id}_B)] = \mathfrak{Tr}[\mathcal{N}]\mathcal{E} \tag{39}$$

and

$$\mathfrak{Tr}_A[\Omega(\mathcal{N}_A \otimes \mathrm{id}_B)] = \mathfrak{Tr}[\mathcal{N}]\mathcal{F} \tag{40}$$

for some channels $\mathcal{E} \in \mathfrak{C}(A)$ and $\mathcal{F} \in \mathfrak{C}(B)$ and for all $\mathcal{N} \in \tilde{\mathfrak{C}}(A)$. As discussed in Sec. III D, the duality between distributed and dynamical settings immediately yields that it is equivalent to the problem of hiding a bipartite state $\rho_{AA'}$, i.e., with some unitary operators $U_0 \in \mathfrak{U}(AB)$ and $U_1 \in \mathfrak{U}(A'B')$, we want

$$\mathrm{Tr}_{BB'}[\mathrm{Ad}_{U_0\otimes U_1}(\rho_{AA'} \otimes \phi^+_{BB'})] = \eta_{AA'} \tag{41}$$

and

$$\mathrm{Tr}_{AA'}[\mathrm{Ad}_{U_0\otimes U_1}(\rho_{AA'} \otimes \phi^+_{BB'})] = \zeta_{BB'} \tag{42}$$

for some quantum states $\eta_{AA'}$ and $\zeta_{BB'}$. These types of processes were called randomness-utilizing processes in Ref. [18], and it was shown there that every dimension preserving randomness utilizing process must be a catalysis. Hence, we can set $\zeta_{BB'} = \phi^+_{BB'}$, which is a pure state. Also, because the distributed catalytic entropy of $\phi^+_{BB'}$ is zero, $\eta_{AA'}$ cannot have larger entropy than the input state $\rho_{AA'}$, which can be chosen as a pure state, hence $\eta_{AA'}$ must be pure as well. This immediately yields a contradiction since whenever $\rho_{AA'}$ is mixed, then the transformation $\rho_{AA'} \mapsto \eta_{AA'}$ decreases the entropy, which is impossible with a catalytic map. Remember that every catalytic map is unital, so it cannot decrease the entropy of the input state.

It follows that the original task of hiding arbitrary quantum process $\mathcal{N} \in \tilde{\mathfrak{C}}(A)$ by unitarily distributing it to two parties is also impossible. In short, a quantum process cannot be stealthy on a system with reversible time evolution. Nevertheless, by using the resource theory of randomness for quantum processes developed in Sec. III D, it is indeed possible to hide quantum processes when there is a randomness source with enough randomness.

H. Randomness amplification

Suppose that there is a sequence of (classical or quantum) systems $(A_n)_{n=0}^{\infty}$, and the initial system is prepared in some state ρ_0. At step n, similarly with a Markov chain, only two adjacent systems A_n and A_{n+1} can unitarily interact with the constraint that information must not flow from A_{n+1} to A_n. This means that catalysis of randomness should happen with system A_n being the catalyst. Let ρ_n be the state of A_n after the interaction with A_{n-1}. We will call this type of sequence a *randomness chain*.

Assume that A_0 is the only initial randomness source, i.e., every A_n with $n \geqslant 1$ is prepared in a pure state. One observation we can make is that, when every system A_n is classical, the amount of randomness never increases with increasing n. This is because $S_\alpha^\diamond(\rho_n) = S_\alpha(\rho_n)$ for classical systems but $S_\alpha(\rho_{n+1}) \leqslant S_\alpha^\diamond(\rho_n)$ by Theorem 3. On the other hand, if every system A_n is quantum, then the amount of randomness can increase *exponentially* over n. This is because $S_\alpha^\diamond(\rho_n) \geqslant S_\alpha(\rho_n)$ and even $S_\alpha^\diamond(\rho_n) = 2S_\alpha(\rho_n)$ is achievable. In other words, *randomness amplification* is possible only in the chain of quantum systems.

Interpretations of this observation could vary. One could conclude that in classical chain, when information backflow is not allowed, then the total amount of information measured by its randomness can only decay over successive transmission between systems. It is fundamentally because classical systems cannot generate new randomness without shifting information to other systems. However, in quantum systems, correlation can be formed within a single system without requiring any randomness, in contrast to classical systems. Therefore, by using preexisting randomness, one can destroy the correlation and create even larger randomness. As a result, quantum randomness that was initially minuscule can be amplified to the macroscopic randomness after the long chain of quantum systems, but no information has flowed backward through the chain.

Because of the generalization developed in this work, we can see that the same phenomenon could also happen to a chain of quantum processes. Analogously, we can consider a sequence of quantum channels $(\mathcal{N}_n)_{n=0}^{\infty}$ where $\mathcal{N}_n \in \mathfrak{C}(A_n)$ and there exists a catalytic superchannel Θ_n such that $\Theta_n(\mathcal{M}) = \mathfrak{Tr}[\Omega_n(\mathcal{M} \otimes \mathcal{N}_n)]$ with some catalysis superunitary operation $\Omega_n \in \mathfrak{SU}(A_{n+1}A_n)$ compatible with the catalyst $\mathcal{N}_n$ for every $n \geqslant 0$ so that $\Theta_n(\Upsilon_n) = \mathcal{N}_{n+1}$ for some superunitary operation $\Upsilon_n \in \mathfrak{U}(A_n)$. It means that all the randomness of $\mathcal{N}_{n+1}$ is catalytically extracted from $\mathcal{N}_n$, hence there is no detectable effect left on the action of $\mathcal{N}_n$ alone by the randomness extraction. We will call this a randomness chain of quantum channels. For example, a depolarizing noise on a 1000-qubit quantum system can be realized from a depolarizing noise on a qubit system after about 10 steps along a randomness chain because of the exponential growth of randomness. Along with chaos, this type of quantum randomness amplification might be one of the mechanisms realizing macroscopic disorder with microscopic initial disorder. An interesting observation is that a chain of completely dephasing channels cannot see this kind of randomness amplification because there are no local parts in the DCD that could yield quantum advantage of randomness extraction (see Sec. III I).

I. Examples

First, any pure state shared between two parties is useless as a randomness source. Especially, the maximally entangled state, corresponding to the identity channel through the Choi-Jamiołkowski isomorphism, cannot yield any information without being perturbed. One can see that the mixture of TQ-Q with the maximally mixed state is still a TQ-Q state as the maximally mixed state does not affect the commutator in Definition 1. It immediately follows that every Werner state is a TQ-Q state.

On the contrary, every classical-classical (C-C) state can yield all of its entropy through catalysis. Suppose that a quantum state σ_{AB}^{cc} is a C-C state:

$$\sigma_{AB}^{cc} = \sum_{i,j} p(i,j)|i\rangle\langle i| \otimes |j\rangle\langle j|, \tag{43}$$

with the superselection rules that forbid any superposition between basis elements (i.e., $\{|i\rangle\}$) for both systems. For σ_{AB}^{cc}, there is no quantumly correlated part in its DCD, therefore, the distributed catalytic entropies and the ordinary entropies are the same, i.e., $S_\alpha^{\diamond\diamond}(\sigma_{AB}^{cc}) = S_\alpha(\sigma_{AB}^{cc}) = S_\alpha(\{p(i,j)\}_{i,j})$ for all $\alpha \geqslant 0$.

This fact could be directly translated to classical-to-classical channels. Suppose that $\mathfrak{B}(B)$ is the C^* algebra of $|B|$-dimensional diagonal matrices and $\mathcal{R}_c \in \mathfrak{C}(B)$ is a classical channel:

$$\mathcal{R}_c(\rho) = \sum_{i,j=1}^{|B|} p(j|i)\langle i|\rho|i\rangle |j\rangle\langle j| \tag{44}$$

for some conditional probability distribution $p(j|i)$. Then its Choi matrix is a C-C state, i.e., $J_{CC'}^{\mathcal{R}_c} = |B|^{-1}\sum_{i,j} p(j|i)|j\rangle\langle j|_B \otimes |i\rangle\langle i|_{B'}$ and $J_{CC'}^{\mathcal{R}_c}$, thus $S_\alpha^\diamond(\mathcal{R}_c) = S_\alpha(J_{CC'}^{\mathcal{R}_c}) = S_\alpha(\{|B|^{-1}p(j|i)\}_{i,j})$ for all $\alpha \geqslant 0$.

The procedure of finding the essential decomposition of an arbitrary bipartite state σ_{AB} is simple. First, find the spectral decomposition of σ_{AB}, and group them into classes that are mutually orthogonal on A. If one finds the classes that resist further grouping, then the decomposition is unique.

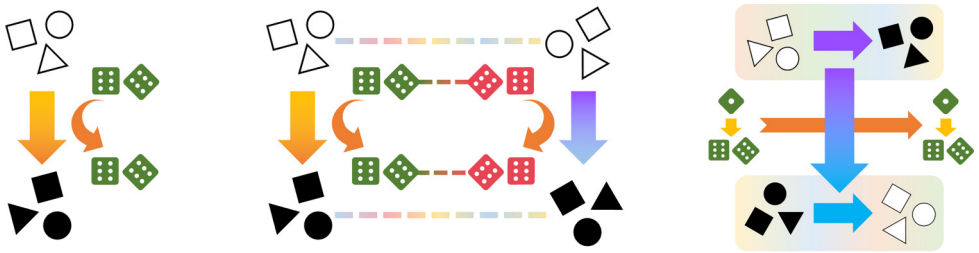
Next, suppose that systems have coarser superselection rules compared to completely classical systems. Let $A = \bigoplus_i A_i$ and $B = \bigoplus_j B_j$ be the superselection sectors of two systems with $\Pi_i^A := \mathbb{1}_{A_i}$ and $\Pi_j^B = \mathbb{1}_{B_j}$. Consider any classically correlated state of the form

$$\sigma_{AB}^{pc} = \sum_{i,j} p(i,j)\pi_{A_i} \otimes \pi_{B_j}. \tag{45}$$

Hence, we have $S_\alpha^{\diamond\diamond}(\sigma_{AB}^{pc}) = S_\alpha^\diamond(\sigma_{AB}^{pc})$ and $S^{\diamond\diamond}(\sigma_{AB}^{pc}) = S(\sigma_{AB}^{pc}) + \sum_{i,j} p(i,j)\log_2(|A_i||B_j|)$ when $\alpha = 1$. This means that there are no constraints imposed by the distributed setting when there is no correlated part in the DCD.

The channel counterpart is the following type of measure-and-prepare channel from A to B with the superselection rules $A = \bigoplus_i A_i$ and $B = \bigoplus_j B_j$,

$$\mathcal{R}_{mp}(\rho) = \sum_{i,j} p(j|i)\mathrm{Tr}\left[\Pi_i^A \rho\right] \pi_{B_j}, \tag{46}$$



(a) Static and local randomness (b) Delocalized randomness (c) Dynamical randomness

FIG. 7. Comparison of three types of catalysis of quantum randomness. Randomness represented by dice enters the interaction and leaves it locally unchanged but correlated with the system. On the other hand, distributed catalysis and dynamical catalysis of randomness are intimately related; rotating one diagram by 90° makes it very similar to the other one.

for any conditional probability distribution $p(j|i)$. The Choi matrix of this channel has the following spectral decomposition:

$$J_{BA}^{\mathcal{R}_{mp}} = \sum_{i,j} p(j|i) a_i \pi_{B_j} \otimes \pi_{A_i}, \tag{47}$$

where $a_i := |A_i|/|A|$. A special case is the completely depolarizing channel with no superselection rules and trivial measurement, i.e.,

$$\mathcal{R}_{cp}(\rho) = \pi_B \mathrm{Tr}[\rho]. \tag{48}$$

The catalytic entropy of this channel, which functions as the completely randomizing quantum channel, is $S_\alpha^\diamond(\mathcal{R}_{cp}) = 2\log_2|A| + 2\log_2|B|$. However, if both systems A and B are classical, then the same channel $\mathcal{R}_{cp}$ now models "dice rolling" and the catalytic entropy becomes the half; $S_\alpha^\diamond(\mathcal{R}_{cp}) = \log_2|A| + \log_2|B|$.

Conversely, let us consider the pinching channel $\mathcal{R}_d$ with respect to a complete set of orthonormal projectors $\{\Pi_i\}$ on B such that $\sum_i \Pi_i = \mathrm{id}_B$, i.e.,

$$\mathcal{R}_d(\rho) = \sum_i \Pi_i \rho \Pi_i. \tag{49}$$

In this case, the Choi matrix of the randomness source is

$$J_{CC'}^{\mathcal{R}_d} = \sum_i b_i |\Gamma_i\rangle\langle\Gamma_i|, \tag{50}$$

where $b_i := |B_i|/|B|$, $|\Gamma_i\rangle = |B_i|^{-1/2}(B_i \otimes \mathbb{1}_{B_i'}) \sum_j |jj\rangle_{CC'}$ with $B_i = \mathrm{supp}(\Pi_i)$. Every subspace B_i has no local part in a product form, so no nontrivial action can be applied on them. Hence, $S_\alpha^\diamond(\mathcal{R}_d) = S_\alpha^{\diamond\diamond}(J_{CC'}^{\mathcal{R}_d}) = S_\alpha(\{b_i\}) \leqslant S_\alpha^\diamond(J_{CC'}^{\mathcal{R}_d})$ for all $\alpha \geqslant 0$. It means that even if there are multiple b_i with the same value, i.e., even if $J_{CC'}^{\mathcal{R}_d}$ has degeneracy, the quantum correlation between two systems hinders the utilization of that correlation without leaving traces.

IV. CONCLUSIONS

Why is it important to understand what it means to use information and information only? With the success of quantum information theory, there has been a trend of calling the advantage of using quantum systems compared to using classical systems for implementing the same task the advantage of "quantum information," even when it is accompanied by destruction or deterioration of quantum systems. But after a moment's thought, not every quantum property is purely informational, and there is a necessity of distinguishing the power of information and that of other physical properties. In this work, following the gist of Shannon [5], we analyzed randomness as information in the quantum setting.

We generalized the resource theory of catalytic quantum randomness to distributed and dynamical randomness sources (see Fig. 7). The distributed and dynamical catalytic entropies were introduced to measure the catalytically extractable randomness within multipartite quantum states. In contrast to static catalysis of randomness, not every mixed state can yield catalytic randomness in the distributed setting for nonclassically correlated quantum states are sensitive to the effect of catalytic maps. As an application, we proved a no-go theorem that is a generalization of the no-hiding theorem [55], the no-stealth theorem, that forbids unitarily hiding quantum processes by distributing it to two distributed parties.

We also attempted to analyze semantic information in the context of catalytic quantum randomness, by focusing on the correspondence between information's meaning and correlation with other systems. By doing so, we showed that nonsemantic information, randomness, is a special case of semantic information and revealed that the usability of semantic information is exactly same with that of nonsemantic information.

As we have completed the characterization of maximum entropy extractable with exact catalysis, natural next steps include generalization to approximate catalysis and the converse problem. By converse problem, we mean characterizing randomness sources that can realize a given catalytic map.

Characterizing tasks that can be done without altering randomness sources is important for understanding the nature of randomness in physics in comparison to other concepts, but in practice, one can always use randomness in combination with other physical properties, hence, it would be interesting to study the relation of the randomness cost and other costs of implementing quantum processes.

ACKNOWLEDGMENTS

S.H.L. thanks Seongwook Shin for helpful discussions. 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 Ministry of Science and ICT, Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-0-01606) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation). This work is also supported by the quantum computing technology development program of the National Research Foundation of Korea (NRF) funded by the Korean government (Ministry of Science and ICT(MSIT)) (Grant No. 2021M3H3A103657312).

APPENDIX: MATHEMATICAL RESULTS

1. Issues of CP map input

In contrast to static catalysis, which requires the invariance of the state of randomness source for every normalized input state, we required dynamical catalysis the invariance of the randomness source channel for every CP trace nonincreasing map in (21). However, in contrast to that, every subnormalized quantum state can be made into a normalized one by simply multiplying by some positive number, but not every CP map can be made into a quantum channel (CPTP map) in the same way. Hence, one might suspect that requiring condition (21) for every $\mathcal{N} \in \tilde{\mathfrak{C}}(A)$ is too severe. In this section, we justify this condition. Alternatively, we could require the following condition:

$$\mathfrak{Tr}_A[(\mathfrak{id}_{E_0\to E_1} \otimes \Omega)(\mathcal{N} \otimes \mathcal{R})] = \mathfrak{Tr}_A[\mathcal{N}] \otimes \mathcal{R} \tag{A1}$$

for every $\mathcal{N} \in \mathfrak{C}(AE_0, AE_1)$, where $\mathfrak{id}_{E_0\to E_1}(\mathcal{L}) = \mathrm{id}_{E_1} \circ \mathcal{L} \circ \mathrm{id}_{E_0}$ for every $\mathcal{L} \in \mathfrak{L}(E_0, E_1)$. The differences are that now $\mathcal{N}$ is a multipartite channel, and that output channels $\mathfrak{Tr}_A[\mathcal{N}] \in \mathfrak{C}(E_0, E_1)$ and $\mathcal{R} \in \mathfrak{C}(B)$ are required to be uncorrelated.

This is a well-motivated requirement since superchannels can be applied to a part of multipartite channels, and the requirement of information nonleakage through Ω can be reinterpreted as the requirement of no formation of correlation between the systems that did not interact directly through $\Omega \in \mathfrak{SC}(AB)$. We remark that any CP trace nonincreasing map can be a subchannel of another channel. It means that for any $\mathcal{N}_0 \in \tilde{\mathfrak{C}}(A)$, there exists some $\mathcal{N}_1 \in \tilde{\mathfrak{C}}(A)$ such that $\mathcal{N}_0 + \mathcal{N}_1 \in \mathfrak{C}(A)$. Also, for some $U \in \mathfrak{U}(AE_0)$ and a positive operator-valued measure (POVM) $\{M_0, M_1\}$ with $M_0 + M_1 = \mathbb{1}_{E_0}$ on E_0 and

$$\mathcal{N}_i(\rho) = \mathrm{Tr}_{E_0}[(\mathbb{1}_A \otimes M_i)\mathrm{Ad}_U(\rho \otimes |0\rangle\langle 0|_{E_0})] \tag{A2}$$

for every $\rho \in \mathfrak{B}(A)$ and $i = 0, 1$. Naturally, we can define the corresponding channel $\mathcal{N} \in \mathfrak{C}(A, AE_1)$ given as

$$\mathcal{N}(\rho) := \mathcal{N}_0 \otimes |0\rangle\langle 0|_{E_1} + \mathcal{N}_1 \otimes |1\rangle\langle 1|_{E_1}. \tag{A3}$$

With this expression, (A1) requires that

$$\mathfrak{Tr}_A[(\mathfrak{id}_{E_0\to E_1} \otimes \Omega)(\mathcal{N} \otimes \mathcal{R})] = \sigma_{E_1} \otimes \mathcal{R}, \tag{A4}$$

with $\sigma_{E_1} = \mathfrak{Tr}[\mathcal{N}_0]|0\rangle\langle 0|_{E_1} + \mathfrak{Tr}[\mathcal{N}_1]|1\rangle\langle 1|_{E_1}$. However, we can observe that

$$\langle i|_{E_1}\mathcal{N}|i\rangle_{E_1} = \mathcal{N}_i \tag{A5}$$

for $i = 0, 1$; therefore, by contracting $|i\rangle\langle i|_{E_1}$ with both sides of (A4), using $\langle i|_{E_1}\sigma_{E_1}|i\rangle_{E_1} = \mathfrak{Tr}[\mathcal{N}_i]$, we get

$$\mathfrak{Tr}_A\Omega(\mathcal{N}_i \otimes \mathcal{R}) = \mathfrak{Tr}[\mathcal{N}_i]\mathcal{R}. \tag{A6}$$

Since $\mathcal{N}_0$ was chosen arbitrarily in $\tilde{\mathfrak{C}}(A)$, we can see that (A1) implies condition (21).

Conversely, let $\mathcal{L}^\ddagger := \dagger \circ \mathcal{L} \circ \dagger$ for any linear map $\mathcal{L}$. We can see that any linear map $\mathcal{L}$ can be decomposed into the Hermitian-preserving part $\mathcal{L}_R := (\mathcal{L} + \mathcal{L}^\ddagger)/2$ and the anti-Hermitian-preserving part $\mathcal{L}_I := -i(\mathcal{L} - \mathcal{L}^\ddagger)/2$ so that $\mathcal{L} = \mathcal{L}_R + i\mathcal{L}_I$. Again, any Hermitian-preserving linear map $\mathcal{H}$ can be expressed as the difference of two CP maps $\mathcal{P}$ and $\mathcal{L}$ so that $\mathcal{H} = \mathcal{P} - \mathcal{N}$. (It follows from the spectral decomposition of its Choi matrix.) Hence, if (21) holds for every $\mathcal{N} \in \tilde{\mathfrak{C}}(A)$, by the linearity, it also holds for every $\mathcal{L} \in \mathfrak{L}(A)$, so (A1) follows. Therefore, (21) and (A1) are equivalent.

2. Proof of Proposition 2

Proof. Let $\mathcal{C} \in \mathfrak{C}(X)$ be a catalytic map. The entropy increase of a quantum state σ_X by $\mathcal{N}$ cannot be larger than that of its purification $|\Sigma\rangle_{XX'}$ $(\mathrm{Tr}_{X'}|\Sigma\rangle\langle\Sigma|_{XX'} = \sigma_X)$ [19]. Therefore, the largest entropy production happens on a pure bipartite state, and let $|\Psi\rangle_{XX'}$ be a pure state that achieves the maximum entropy production by $\mathcal{N}$. Note that every pure bipartite state s related with a maximally entangled state $|\Phi\rangle_{XX'}$ by the action of a local matrix, i.e., there exists $M \in \mathfrak{B}(X)$ such that $|\Psi\rangle_{XX'} = (\mathbb{1}_X \otimes M_{X'})|\Phi\rangle_{XX'}$. Note that $\mathcal{N}$ cannot generate any randomness if $\mathcal{N}_X(|\Psi\rangle\langle\Psi|)_{XX'}$ is pure, i.e., rank 1. Since $\mathcal{N}_X(|\Psi\rangle\langle\Psi|_{XX'}) = (\mathrm{id}_X \otimes \mathrm{Ad}_M)(\mathcal{N}_X(|\Phi\rangle\langle\Phi|_{XX'}))$, if $\mathcal{N}_X(|\Phi\rangle\langle\Phi|_{XX'})$ is pure, then it follows that $\mathcal{N}$ cannot generate randomness. Conversely, if $\mathcal{N}$ cannot generate randomness, then by definition $\mathcal{N}(|\Phi\rangle\langle\Phi|_{XX'})$ is pure. ∎

3. Discussion on Mølmer's conjecture

Mølmer's conjecture [45] insists that the quantum state of laser light should not be represented by a pure coherent state

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{A7}$$

but the mixed state

$$\frac{1}{2\pi}\int_0^{2\pi} ||\alpha|e^{i\theta}\rangle\langle|\alpha|e^{i\theta}|d\theta = e^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{|\alpha|^{2n}}{n!}|n\rangle\langle n|, \tag{A8}$$

because of the loss of phase information caused by inaccessibility of laser device. Choosing to use the pure coherent state representation without considering correlated systems amounts to committing the *preferred ensemble fallacy* [57,58]. When it is stated that "a random pure state $|\phi\rangle_A$ is prepared," oftentimes it is assumed, very implicitly, that there exists a fixed preparation protocol that produces $|\phi\rangle_A$. This protocol can be classically identified with a careful inspection, and be represented by an orthonormal basis $\{|\text{“}\phi\text{”}\rangle_P\}$ that is orthogonal between each different state, even when $|\phi\rangle_A$ itself is not orthogonal to each other, i.e., $\langle\text{“}\phi\text{”}||\text{“}\psi\text{”}\rangle = 0$ whenever $\phi \neq \psi$. In this case, the global quantum state of system AC is

$$\sum_\phi p(\phi)|\phi\rangle\langle\phi|_A \otimes |\text{“}\phi\text{”}\rangle\langle\text{“}\phi\text{”}|_C, \tag{A9}$$

with some probability distribution $p(\phi)$. (One can replace the sum with an integral when the probability distribution is not discrete.) If one runs the same preparation protocol n times, then it becomes

$$\sum_{\phi} p(\phi)|\phi\rangle\langle\phi|_A^{\otimes n} \otimes |\text{“}\phi\text{”}\rangle\langle\text{“}\phi\text{”}|_C. \tag{A10}$$

Or, systems AC can even be entangled:

$$\sum_{\phi} \sqrt{p(\phi)}|\phi\rangle_A \otimes |\text{“}\phi\text{”}\rangle_C. \tag{A11}$$

Whether to treat the whole system AC or system A alone as the information source depends on one's choice and on a given situation. For example, if it is implicitly assumed that there exists a referee who remembers the identity of the random state $|\phi\rangle_A$ and if you treat the relation between the state and the referee as a part of information you utilize, then the whole system AC should be considered an information source. However, if system A is in isolation from any context other than the distribution $p(\phi)$, then it is natural to treat only system A as an information source.

4. Proof of Theorem 4

Proof. The assumption that no randomness can be catalytically extracted from $\sigma_{A_CB_C}$ means that any catalytic unitary operators compatible with $\sigma_{A_CB_C}$ are a product unitary operator. Therefore, any action applied to $\sigma_{A_CB_C}$ after catalysis is also of the form of product unitary operations, i.e., $\sigma_{A_CB_C} \mapsto \mathrm{Ad}_{V_A\otimes V_B}(\sigma_{A_CB_C})$ with some $V_A \in \mathfrak{U}(A_C)$ and $V_B \in \mathfrak{U}(B_C)$. As a special case, assume that $U_A = \mathbb{1}_{A_SA_C}$. It implies that $V_A = \mathbb{1}_{A_C}$. Note that, in this case, V_B should be also proportional to the identity operator. It is because, if $V_B \not\propto \mathbb{1}_{B_C}$, then the random unitary operation given as $\frac{1}{2}(\mathrm{id}_{B_C} + \mathrm{Ad}_{V_B})$ on B_C that is not a unitary operation also fixes $\sigma_{A_CB_C}$. This contradicts the previous result that any action on $\sigma_{A_CB_C}$ should be a unitary operation. It is equivalent to saying that whatever catalytic map is applied to system B_C, if it fixes $\sigma_{A_CB_C}$, then it should the identity operation. This property is called sensitivity to catalytic maps according to the definition given in Ref. [49]. As the set of catalytic map is contained in the set of unital maps, and contains the set of random unitary operations, by the results of Ref. [49], it follows that it is equivalent to that $\sigma_{A_CB_C}$ is not a Q-PC state. The same argument can be applied when the roles of A_C and B_C are switched, thus $\sigma_{A_CB_C}$ is neither a PC-Q state.

Conversely, assume that $\sigma_{A_CB_C}$ is TQ-TQ. Let $U_A \in \mathfrak{U}(A_SA_C)$ and $U_B \in \mathfrak{U}(B_SB_C)$ be arbitrary catalytic unitary operators and $\mathcal{N}_A := \mathfrak{Tr}_{A_S} \circ \mathrm{Ad}_{U_A} \in \mathfrak{UC}(A_C)$ and $\mathcal{N}_B := \mathfrak{Tr}_{B_S} \circ \mathrm{Ad}_{U_B} \in \mathfrak{UC}(B_C)$ be induced catalytic maps on A_C and B_C, respectively. For $\sigma_{A_CB_C}$ to be compatible with U_A and U_B, $\mathcal{N}_A \otimes \mathcal{N}_B$ must fix $\sigma_{A_CB_C}$. However, since catalytic maps can never decrease the von Neumann entropy, it means that both $\mathcal{N}_A$ and $\mathcal{N}_B$ fix the von Neumann entropy of $\sigma_{A_CB_C}$. By Theorem 2.1 of Ref. [50], it is equivalent to that both $\mathcal{N}_A^\dagger \circ \mathcal{N}_A$ and $\mathcal{N}_B^\dagger \circ \mathcal{N}_B$ fix $\sigma_{A_CB_C}$. Since $\sigma_{A_CB_C}$ is TQ-TQ, it is sensitive to unital channels on both sides [49], hence, it follows that $\mathcal{N}_A^\dagger \circ \mathcal{N}_A = \mathrm{id}_{A_C}$ and $\mathcal{N}_B^\dagger \circ \mathcal{N}_B = \mathrm{id}_{B_C}$. It is equivalent to that both $\mathcal{N}_A$ and $\mathcal{N}_B$ are unitary operations, therefore, U_A and U_B are product unitary operators. It follows that no randomness can be extracted from $\sigma_{A_CB_C}$. ■

5. Other results on essential decomposition

Here, we provide a proof of Theorem 5. The structure result formally resembles Theorem 6 of Ref. [59], but the methodology is slightly simpler as we only use the structure theorem of C^* algebra and no other functional analytic results.

Proof. Let $\mathcal{C}_A(\rho_{AB})$ be the centralizer of ρ_{AB} on A, i.e.,

$$\mathcal{C}_A(\rho_{AB}) := \{M \in \mathfrak{B}(A) : [M_A \otimes \mathbb{1}_B, \rho_{AB}] = 0\}. \tag{A12}$$

It is easy to check that $\mathcal{C}_A(\rho_{AB})$ is closed under addition, scalar multiplication, and matrix multiplication and adjoint operation. Therefore, $\mathcal{C}_A(\rho_{AB})$ is a finite-dimensional C^* algebra, hence, A has the decomposition $A = \bigoplus_i A_i^P \otimes A_i^Q$ (we let $A_i := A_i^P \otimes A_i^Q$) so that ρ_{AB} has the decomposition of the following form [35,36]:

$$\mathcal{C}_A(\rho_{AB}) = \bigoplus_i \mathfrak{B}\big(A_i^P\big) \otimes \mathbb{1}_{A_i^Q}. \tag{A13}$$

It implies that, for all i, $\mathbb{1}_{A_i^P} \otimes \mathbb{1}_{A_i^Q}$, which is a projector, is in $\mathcal{C}_A(\rho_{AB})$, hence, ρ_{AB} is block diagonal with respect to the direct sum $A = \bigoplus_i A_i$, i.e.,

$$\rho_{AB} = \sum_i p_i \rho_{A_iB}. \tag{A14}$$

Now, we focus on each summand ρ_{A_iB}. Since it commutes with every element in $\mathfrak{B}(A_i^P) \otimes \mathbb{1}_{A_i^Q}$, it has the form of $\rho_{A_iB} = \pi_{A_i^P} \otimes \rho_{A_i^QB}$, where $\pi_{A_i^P}$ is the maximally mixed state on A_i^P. To show it explicitly, one can average over the action of every unitary operator (“twirl”) on ρ_{A_iB}. Now, $\rho_{A_i^QB}$ must be TQ-Q because no projector on A_i^Q other than $\mathbb{1}_{A_i^Q}$ commutes with it. A unital channel fixes a quantum state if and only if all of its Kraus operators commute with the quantum state. Therefore, for any unital channel $\mathcal{N}$ on A fixes ρ_{AB} if and only if its Kraus operators are in $\mathcal{C}_A(\rho_{AB})$. It implies that $\mathcal{N}$ preserves all the subspaces A_i, and its limitation on A_i $\mathcal{N}|_{A_i}$ has Kraus operators in $\mathfrak{B}(A_i^P) \otimes \mathbb{1}_{A_i^Q}$. Again, it means that $\mathcal{N}|_{A_i}$ factorizes into $\mathcal{N}_{A_i^P} \otimes \mathrm{id}_{A_i^Q}$.

The uniqueness of the decomposition is immediate from the uniqueness of the decomposition (A13), which determines and is determined by the essential decomposition of ρ_{AB}. By summing up the terms with a common $\rho_{A_i^QB}$ factor, we get the essential decomposition of ρ_{AB}. ■

Lemma 2. A unital channel $\mathcal{N} \in \mathfrak{UC}(A)$ does not increase the entropy of a quantum state ρ_{AB} with the essential decomposition $\rho_{AB} = \sum_i p_i \rho_{A_i^P} \otimes \rho_{A_i^QB}$ if and only if $\mathcal{N}$ can be decomposed into $\mathcal{N} = \mathrm{Ad}_V \circ \mathcal{M}$ with some unitary operator $V \in \mathfrak{U}(A)$ and a unital channel $\mathcal{M}$ that preserves every subspace A_i and $\mathcal{M}|_{A_i^P\otimes A_i^Q}$ factorizes into $\mathcal{M}|_{A_i^P\otimes A_i^Q} = \mathcal{M}|_{A_i^P} \otimes \mathrm{id}_{A_i^Q}$ while $\mathcal{M}|_{A_i^P}$ is unital on A_i^P.

Proof. The existence of the decomposition $\mathcal{N} = \mathrm{Ad}_V \otimes \mathcal{M}$ with $\mathcal{M}$ being a unital channel that fixes ρ_{AB} is shown in Ref. [50] [Theorem 2.1 (iii)]. By Theorem 5, the decomposition is unique, thus, $\mathcal{M}$ is decomposed into the form above. ■

Corollary 4. Let a distributed catalysis unitary operator pair (U_A, U_B) be compatible with a distributed randomness

source $\sigma_{A_C B_C}$ with the DCD

$$\sigma_{A_C B_C} = \bigoplus_{ij} p_i q_j \rho_{A^P_{Ci}} \otimes \rho_{A^Q_{Ci} B^Q_{Cj}} \otimes \rho_{B^P_{Cj}}, \tag{A15}$$

and the essential decompositions $A_C = \bigoplus_i A^P_{Ci} \otimes A^Q_{Ci}$ and $B_C = \bigoplus_j B^P_{Cj} \otimes B^Q_{Cj}$. It follows that there exist $W_X \in \mathfrak{U}(X_C)$ for $X = A, B$ such that $U_X = (\mathbb{1}_{X_S} \otimes W_X)(\bigoplus_k U_{Xk} \otimes \mathbb{1}_{X^Q_{Ck}})$ where $U_{Xk} \in \mathfrak{U}(X_S X^P_{Ck})$.

Proof. Consider the maximally mixed initial state $\pi_{A_S} \otimes \pi_{B_S}$ for the catalysis and let $\mathcal{N}_X \in \mathfrak{UC}(X_C)$ given as $\mathcal{N}_X := \mathfrak{Tr}_{X_S}[\mathrm{Ad}_{U_X}]$ be the induced catalytic map on X_C acting on the distributed catalyst $\sigma_{A_C B_C}$ for $X = A, B$. Since (U_A, U_B) and $\sigma_{A_C B_C}$ are compatible with each other, we have $(\mathcal{N}_A \otimes \mathcal{N}_B)(\sigma_{A_C B_C}) = \sigma_{A_C B_C}$. It follows that both of $\mathcal{N}_X$ do not increase the entropy of $\sigma_{A_C B_C}$. By Corollary 2, $\mathcal{N}_X$ can be decomposed into $\mathrm{Ad}_{WX} \circ \mathcal{M}_X$ where $\mathcal{M}_X$ preserves each subspace $X^P_k \otimes X^Q_k$ and the limitation onto each subspace is further decomposed into $\mathcal{M}|_{X^P_i \otimes X^Q_i} = \mathcal{M}|_{X^P_i} \otimes \mathrm{id}_{X^Q_i}$. It implies the dilation of $\mathcal{M}_X$, the action of U_X on $X_S X_C$ with the maximally mixed state on X_S has the same form of decomposition, which is the wanted result. ■

6. Proof of Proposition 3

Proof. By Corollary 4, every component in the DCD of a distributed catalyst is compatible up to a local unitary with the given pair of catalysis unitary operators by itself. Let $\mathcal{C}$ be the catalytic map implemented by the catalysis unitary operators U_A and U_B by using $\sigma_{A_C B_C}$ as the catalyst. In other words, $\mathcal{C}(\rho) := \mathrm{Tr}_{A_C B_C}[(\mathrm{Ad}_{U_A} \otimes \mathrm{Ad}_{U_B})(\rho_{A_S B_S} \otimes \sigma_{A_C B_C})]$. Now we let $\mathcal{C}_{ij}$ be given as $\mathcal{C}_{ij}(\rho) := \mathrm{Tr}_{A_C B_C}[(\mathrm{Ad}_{U_{A_i}} \otimes \mathrm{Ad}_{U_{B_j}})(\rho_{A_S B_S} \otimes \pi_{A^P_i} \otimes \pi_{B^P_j})$, which is a catalytic map by itself, then we have $\mathcal{C} = \sum_{ij} p_i q_j \mathcal{C}_{ij}$. For arbitrary pure initial state $\rho_{A_S B_S}$ (recall that the maximum entropy production is made with a pure state input), we have the following:

$$\begin{aligned} \mathcal{C}(\rho) = \sum_{ij} p_i q_j \mathcal{C}_{ij}(\rho) &\succ \bigoplus_{ij} p_i q_j \mathcal{C}_{ij}(\rho) \\ &\succ \bigoplus_{ij} p_i q_j \pi^{\otimes 2}_{A^P_i} \otimes \pi^{\otimes 2}_{B^P_j}. \end{aligned} \tag{A16}$$

The first majorization relation follows from the fact that a convex sum of quantum states always majorizes the direct sum of the same summands [60]. The last majorization relation follows from the fact that a direct sum of quantum states majorizes another when its individual summand majorizes that of the other and that each $\mathcal{C}_{ij}(\rho)$ majorizes $\pi^{\otimes 2}_{A^P_i} \otimes \pi^{\otimes 2}_{B^P_j}$. It is because for each pair (i, j), $\pi_{A^P_i} \otimes \pi_{B^P_j}$ functions as two separated catalytic randomness sources, hence, any output for a pure input state should majorize its REO, $\pi^{\otimes 2}_{A^P_i} \otimes \pi^{\otimes 2}_{B^P_j}$ [19]. Since every Rényi entropy of order $\alpha \geqslant 0$ is Schur-concave, the desired upper bound of extractable Rényi entropy follows.

Now we show that one can actually attain this bound. First of all, with the maximally mixed catalyst $\pi_{X^P_i}$, one can catalytically transform a pure state into a mixed state unitarily similar to $\pi^{\otimes 2}_{X^P_i}$ [19,20]. Let each catalysis unitary operator U_{X_i} implement such transformation. Therefore, by preparing a "counter" system E_X initialized in $|0\rangle_{E_X}$ for each party X and letting U_{X_i} to map $|0\rangle_{E_X}$ to $|i\rangle_{E_X}$ (for example, applying the generalized Pauli operator $X = \sum_n |n \oplus 1\rangle\langle n \oplus 1|n \ i$ times), we can transform a product pure state into the output state unitarily similar to $\bigoplus_{ij} p_i q_j \pi^{\otimes 2}_{A^P_i} \otimes \pi^{\otimes 2}_{B^P_j}$. ■

7. Proof of Theorem 7

Let us first show that utilization of semantic information is a special case of randomness utilization.

Lemma 3. If $U \in \mathfrak{U}(AB)$ and $\sigma_{AB} \in \mathfrak{S}(AB)$ are given as in Definition 5, then U is a catalysis unitary operator compatible with σ_B as a catalyst up to local unitary.

Proof. As any superchannel can be decomposed into preprocessing and postprocessing channels, (33) is equivalent to

$$\mathrm{Tr}_A[\mathcal{U} \circ (\mathcal{N}_A \otimes \mathrm{id}_B)(\sigma_{AB})] = \eta_B \tag{A17}$$

for any channel $\mathcal{N} \in \mathfrak{C}(A)$. Here, $\mathcal{N}$ is the partial trace of the arbitrarily chosen preprocessing channel of $\Theta_{A \to B}$ in (33). By letting $\mathcal{N}$ be a state preparation channel, i.e., $\mathcal{N}(\rho) = \tau_A \mathrm{Tr}\rho$ for every $\tau \in \mathfrak{S}(A)$, we get that

$$\mathrm{Tr}_A[\mathcal{U}(\tau_A \otimes \sigma_B)] = \eta_B \tag{A18}$$

for any $\tau \in \mathfrak{S}(A)$. By the result of Ref. [18], there exists a unitary operator V such that $\eta_B = \mathrm{Ad}_V(\sigma_B)$, thus by the definition given in (7), U is a catalysis unitary operator and it is compatible with σ_B up to local unitary. ■

As a side note, this lemma provides a proof of the first part of Theorem 1. That is, if σ_{AB} is uncorrelated, i.e., $\sigma_{AB} = \sigma_A \otimes \sigma_B$, then every catalytic unitary operation compatible with σ_B as a catalyst utilizes only information of B in σ_{AB}. It is because if $\sigma_{AB} = \sigma_A \otimes \sigma_B$, then (A17) becomes equivalent to

$$\mathrm{Tr}_A[\mathcal{U}(\rho_A \otimes \sigma_B)] = \sigma_B \tag{A19}$$

for every $\rho \in \mathfrak{S}(A)$ as the set $\{\mathcal{N}(\sigma_A) \,|\, \mathcal{N} \in \mathfrak{C}(A)\}$ is same with $\mathfrak{S}(A)$. Since it is equivalent to (7), we get the desired result.

[(S:B) $\Rightarrow$ (S:A)] It immediately follows from the fact that any superchannel can be decomposed into preprocesses and postprocesses. Note that the output of the transformed channel on A is immediately discarded, and the postprocess is irrelevant. The process $\mathcal{N}_{A \to RA}$ can be considered the preprocess of the superchannel Θ in (S:A).

[(S:C) $\Leftrightarrow$ (S:B)] Without loss of generality, we consider the canonical case (without local unitary transformation on catalysts), if $U \in \mathfrak{U}(AB)$ is compatible with σ_{AB} on B, we have

$$\mathrm{Tr}_{A'} \circ \mathrm{Ad}_{U_{A'B}}(\sigma_{AB}) = \mathrm{Tr}_{A'} \otimes \sigma_{AB}. \tag{A20}$$

A simple change of system labels yields that for every $\mathcal{L} \in \mathfrak{L}(A)$ (by considering it as linear map that maps from A to A'), we have

$$\mathrm{Tr}_A \circ \mathrm{Ad}_{U_{AB}} \circ \mathcal{L}_A(\sigma_{AB}) = \mathrm{Tr}_A \circ \mathcal{L}_A(\sigma_{AB}). \tag{A21}$$

By inserting arbitrary quantum map $\mathcal{N} \in \mathfrak{C}(A, RA)$ into the position of $\mathcal{L}_A$, we have the desired result

$$\mathrm{Tr}_A \circ \mathrm{Ad}_{U_{AB}} \circ \mathcal{N}_{A \to RA}(\sigma_{AB}) = \mathrm{Tr}_A \circ \mathcal{N}_{A \to RA}(\sigma_{AB}). \tag{A22}$$

By choosing $\mathcal{N}_{A \to RA} = |\psi\rangle\langle\psi|_A \otimes \mathrm{id}_{A \to R}$ for each state $|\psi\rangle$ on A, one can also show the converse.

[(S:A) $\Rightarrow$ (S:C)] We will use the following lemma.

Lemma 4. For any constant superchannel Θ that maps channels in $\mathfrak{C}(A,B)$ to channels in $\mathfrak{C}(C,D)$, meaning that $\Theta(\mathcal{N})$ is the same for every $\mathcal{N}\in\mathfrak{C}(A,B)$, there exists a quantum channel $\mathcal{P}\in\mathfrak{C}(C,AD)$ such that

$$\Theta(\mathcal{L}) = (\mathrm{Tr}_B\circ\mathcal{L}_{A\to B}\otimes \mathrm{id}_D)\circ\mathcal{P}_{C\to AD} \tag{A23}$$

for any $\mathcal{L}\in\mathfrak{L}(A,B)$.

Proof. A basis of $\mathfrak{L}(A,B)$ is $\{\mathcal{E}_{ij} := Y_j\mathrm{Tr}[X_i^\dagger\cdot\,]\}$, where $\{X_i\}$ and $\{Y_j\}$ are orthonormal bases of $\mathfrak{B}(A)$ and $\mathfrak{B}(B)$, respectively, that consist of traceless Hermitian operators except for $X_0 = |A|^{-1/2}\mathbb{1}_A$ and $Y_0 = |B|^{-1/2}\mathbb{1}_B$. Hence, every $\mathcal{L}\in\mathfrak{L}(A,B)$ has the expression of the form

$$\mathcal{L} = \sum_{ij}\mathcal{E}_{ij}\mathrm{Tr}[Y_j^\dagger\mathcal{L}(X_i)]. \tag{A24}$$

Note that the span of $\mathfrak{C}(A,B)$ coincides with the span of $\{\mathcal{E}_{ij}\}$ excluding $\mathcal{E}_{i0}$ with $i>0$. If we let $\mathcal{F}_{ij} := \Theta(\mathcal{E}_{ij})\in\mathfrak{L}(C,D)$, we get the expression

$$\Theta(\mathcal{L}) = \sum_{ij}\mathcal{F}_{ij}\mathrm{Tr}[Y_j^\dagger\mathcal{L}(X_i)]. \tag{A25}$$

By the condition that Θ is constant for quantum channels in $\mathfrak{C}(A,B)$, there exists some channel $\mathcal{C}\in\mathfrak{C}(C,D)$ such that $\Theta(\mathcal{N}) = \mathcal{C}$ for all $\mathcal{N}\in\mathfrak{C}(A,B)$ and

$$\Theta(\mathcal{L}) = \mathcal{C}\mathrm{Tr}[\mathcal{L}(\pi_A)] + \sum_{i>0}\mathcal{F}_{i0}\mathrm{Tr}[\mathcal{L}(X_i)]. \tag{A26}$$

Now, we let $\mathcal{P}\in\mathfrak{L}(C,AD)$ defined as

$$\mathcal{P} := \pi_A\otimes\mathcal{C} + \sum_{i>0}X_i\otimes\mathcal{F}_{i0}. \tag{A27}$$

From (A26), we can see that if $\mathcal{Q}\in\mathfrak{C}(C,AE)$ and $\mathcal{R}\in\mathfrak{C}(BE,D)$ are preprocessing and postprocessing channels of Θ so that $\Theta(\mathcal{L}) = \mathcal{R}\circ(\mathcal{L}\otimes\mathrm{id}_E)\circ\mathcal{Q}$ for every $\mathcal{L}\in\mathfrak{L}(A)$, then $\mathcal{P}_{C\to AD} = (\mathcal{R}_{A'E\to D}\otimes\mathrm{id}_A)(\tau_{A'}\otimes\mathcal{Q}_{C\to AE})$ for some $\tau\in\mathfrak{S}(A')$. Therefore, as a composition of quantum channels, $\mathcal{P}$ is obviously a quantum channel. Moreover, by comparing (A26) and (A27), we get the desired result

$$\Theta(\mathcal{L}) = (\mathrm{Tr}_B\circ\mathcal{L}_{A\to B}\otimes\mathrm{id}_D)\circ\mathcal{P}_{C\to AD}. \tag{A28}$$

■

Indeed, as we can observe that the left-hand side of (A17) is a constant superchannel when $\mathcal{N}$ is considered an input, we can apply Lemma 4. Therefore, there exists a quantum state (which is a special type of quantum channel) τ_{AB} such that

$$\mathrm{Tr}_A[\mathcal{U}\circ(\mathcal{L}_A\otimes\mathrm{id}_B)(\sigma_{AB})] = \mathrm{Tr}_A[(\mathcal{L}_A\otimes\mathrm{id}_B)(\tau_{AB})] \tag{A29}$$

for every $\mathcal{L}\in\mathfrak{L}(A)$. Equivalently, inputting a part of the swapping gate on AA', we get

$$\mathrm{Tr}_{A'}[\,(\mathcal{U}_{A'B}\otimes\mathrm{id}_A)(\rho_{A'}\otimes\sigma_{AB})] = \tau_{AB} \tag{A30}$$

for all $\rho_{A'}\in\mathfrak{S}(A')$. In other words, the mapping $\rho_{A'}\mapsto\tau_{AB}$ is constant. If one interprets (A30) as that $U_{A'B}\otimes\mathbb{1}_A$ utilizes σ_{AB} as a randomness source, by the result of Ref. [18], τ_{AB} must have the same spectrum, thus also the same entropy, with σ_{AB}. Then, by Corollary 2, there exists a unitary operator $V\in\mathfrak{U}(B)$ such that $\tau_{AB} = \mathrm{id}_A\otimes\mathrm{Ad}_V(\sigma_{AB})$. This proves the desired result.

8. Proof of Corollary 3

Let $\mathcal{U} := \mathrm{Ad}_U$. We will use the following lemma.

Lemma 5 ([59]). If a tripartite state ρ_{RAB} satisfies $I(R:A) = I(R:AB)$, then the Hilbert space of A has a direct sum structure of the form of $A = \bigoplus_i A_{i,K}\otimes A_{i,L}$ and ρ_{RAB} can be decomposed into

$$\rho_{RAB} = \bigoplus_i p_i\rho_{RA_{i,K}}\otimes\rho_{A_{i,L}B}, \tag{A31}$$

where for each i, $\rho_{RA_{i,K}}\in R\otimes A_{i,K}$ and $\rho_{RA_{i,L}B}\in A_{i,L}\otimes B$. Additionally, it is equivalent to that $I(A:B) = I(RA:B)$.

By Lemma 5, ρ_{RAB} has the form of (A31). Therefore, its marginal state on AB must have a form of

$$\rho_{AB} = \bigoplus_i p_i\rho_{A_{i,K}}\otimes\rho_{A_{i,L}B}. \tag{A32}$$

Since each subspace $A_{i,K}\otimes A_{i,L}$ is orthogonal to each other, we can construct quantum channels $\mathcal{N}_i\in\mathfrak{C}(A_{i,K},RA_{i,K})$ such that $\mathcal{N}_i(\rho_{A_{i,K}}) = \rho_{RA_{i,K}}$. Therefore, there exists a quantum map $\mathcal{N} := \bigoplus_i\mathcal{N}_i\otimes\mathrm{id}_{A_{i,L}}\in\mathfrak{C}(A,RA)$ that maps ρ_{AB} into ρ_{RAB}.

9. Proof of Theorem 8

Proof. The essential decomposition of σ_{AB} on B has the form

$$\sigma_{AB} = \sum_i p_i\sigma_{AB_i^Q}\otimes\pi_{B_i^P}. \tag{A33}$$

Now we let $\sigma_A^i := \mathrm{Tr}_{B_i^Q}\sigma_{AB_i^Q}$. The marginal state of A after a general information utilization of B has the form

$$\sum_i p_i\Phi_i\big(\sigma_A^i\big), \tag{A34}$$

where Φ_i are some catalytic maps on A using $\pi_{B_i^Q}$ as the catalyst. We claim that the probability distribution $[\sum_i p_i\lambda_j(\sigma_A^i)]_j$ majorizes $(\lambda_j[\sum_i p_i(\sigma_A^i)])_j$:

$$\begin{aligned}\sum_{1\leqslant j\leqslant k}\lambda_j\left(\sum_i p_i\Phi_i\big(\sigma_A^i\big)\right) &= \max_P\mathrm{Tr}\left[P\sum_i p_i\Phi_i\big(\sigma_A^i\big)\right]\\ &= \max_P\mathrm{Tr}\left[\sum_i p_iP\Phi_i\big(\sigma_A^i\big)\right]\\ &\leqslant \sum_i p_i\max_P\mathrm{Tr}\big[P\Phi_i\big(\sigma_A^i\big)\big].\end{aligned} \tag{A35}$$

In the first equality, the maximization is over rank-k projectors P and we used Fan's Lemma [61]. Applying Fan's Lemma [61] for each maximization in the last term again, we get

$$\sum_{1\leqslant j\leqslant k}\lambda_j\left(\sum_i p_i\Phi_i\big(\sigma_A^i\big)\right)\leqslant\sum_i p_i\sum_{1\leqslant j\leqslant k}\lambda_j\big(\Phi_i\big(\sigma_A^i\big)\big). \tag{A36}$$

Remember that every catalytic map is unital. From the relation between unital maps and majorization, we have $\Phi_i(\sigma_A^i)\prec\sigma_A^i$ for all i, hence $\sum_{1\leqslant j\leqslant k}\lambda_j(\Phi_i(\sigma_A^i))\leqslant\sum_{1\leqslant j\leqslant k}\lambda_j(\sigma_A^i)$ for all i

and k. Therefore, it follows that

$$\sum_{1\leqslant j\leqslant k}\lambda_j\left(\sum_i p_i\Phi_i\left(\sigma_A^i\right)\right)\leqslant\sum_i p_i\sum_{1\leqslant j\leqslant k}\lambda_j\left(\sigma_A^i\right) \tag{A37}$$

for all k. By choosing each Φ_i as a unitary operation that transforms σ_A^i into $\sum_j\lambda_j(\sigma_A^i)|j\rangle\langle j|$ for some common basis $\{|i\rangle\}$, the catalytic transformation of σ_A into $\sum_j[\sum_i p_i\lambda_j(\sigma_A^i)]|j\rangle\langle j|$ is achievable. ■

10. Physicality of information

In the seminal paper [62], Landauer argued that information is physical by reciting the observations that there is no nontrivial minimal energy dissipation accompanying information processing tasks such as computation, copying, and communication. These evidences imply that deletion of information is the only source of nontrivial energy cost, which supports the view that a certain amount of energy corresponds to a certain amount of energy, independent of how it is processed, in favor of the interpretation that information is a physical entity as matter is equivalent to energy through the mass-energy equivalence.

Certainly, Landauer's argument irrefutably shows that the *presence* of information in our physical universe is necessarily physical as Landauer said "Information is not an abstract entity but exists only through a physical representation" [63]. However, the problem with this almost tautological usage of the term "physical" is that it makes every physically perceivable abstract concept physical. For example, *money* can only exist through physical notes and coins or digitalized currencies in physical computers, and *law* must be recorded on some physical representation and can only be enforced with physical methods by a *government*, which is also an abstract concept that exists only through a physical manifestation. We can even say that every abstract concept that involves information exchanges is physical if information is physical. If every concept relevant to a physical agent counts as physical, then this notion of physicality might not be very useful as there would be virtually no nonphysical concept.

A more operational criterion for the physicality of concepts would be asking if usage or action with or involving the concept requires detectable change to physical representation of the concept that is unavoidable, even in an approximate sense. Perhaps, the term *material* might be more appropriate to describe such a property since there are concepts of physical nature that are not material by themselves. For example, "solidness" is represented by a hammer used to drive a nail into the wall, but the hammer, in the practical sense, is not detectably altered after the process. Clearly, solidness is a property of physical nature but not a matterlike concept; solidness did not depart from the hammer to the wall like a particle. Likewise, every catalyst in chemistry and quantum resource theory is also not a physical representation of material concept, albeit they might play a physical role in the respective catalysis process. As a matter of fact, since the terms "physicalism" and "materialism" are often used interchangeably [64], we will not introduce another term and call the property simply "physicality." This is the perspective we take in this work about information, and the argument of Landauer ironically supports the claim that information is not physical in our sense, as Landauer argued that energy cost of information processing other than deletion can be made arbitrarily small.

Our notion of physicality could be relative, as what is expected from an operational concept. Naturally, physicality of information now depends not only on the information storage, but also on the method of utilizing it. For example, software, in contrast to hardware, is usually considered nonphysical because installation, execution, and deletion of software leave no apparent physical trace on the hardware it is running on. However, of course, it is true not only that software accompanies physical traces on hardware detectable with careful inspection, but also one can physically interact with software through input and output devices, hence, software is as physical as hardware for its user equipped with proper devices.

We defined information as something that can spread from its source without altering it, hence, it is required to be nonphysical by definition. Is this notion of information also relative? We first examine it for classical information. Let us consider the classical version of catalytic randomness. Consider interaction between systems 1 and 2, where (i, j) represents the situation where system 1 is in the state i and system 2 is in the state j. We want to formulate a classical version of (6) and (7). Invertible classical operation is permutation, thus, we let $f:(i,j)\mapsto(f_1(i,j),f_2(i,j))$ be a permutation of states of the joint system of 1 and 2, where system 1 is a target system and system 2 is a catalyst. When the initial probability distribution of system 2 is (p_j), then the condition for f to be catalytic permutation compatible with (p_j) is

$$\sum_{j':j=f_2(i,j')}p_{j'}=p_j \tag{A38}$$

for all i and j. Similarly to catalytic quantum randomness, $f_2(i,\cdot)$ must preserve every nondegenerate probability distribution, and can permutate every degeneracy block of (p_j) (the set of j with the same probability p_j). As a special case, for the completely uniform distribution π_2, every permutation f such that $f_2(i,\cdot)$ is a permutation for every i is catalytic permutation compatible with π_2. This fact may come off as weird to some readers because permuting the outcomes of an information source may seem to leak information to the source. However, if the source is not correlated with any other information sources you have, then there is no way to tell if the permutation has taken place: You cannot tell if someone flipped the unknown outcome of a random coin toss.

Even if permutation of degenerate states of catalyst is allowed in pure information utilization, some readers might still wonder why would one want to do that. Indeed, reading a message and scrambling the letters of the message sound weird and look unnecessary when the purpose is simply extracting as much information as possible. In generic cases, however, this permutation is accidental rather than intentional. One can consider each state in each degeneracy block a microscopic state and each degeneracy block of (p_i) a macroscopic state. Turning a page of a book will disturb the molecules in the paper even when it is done extremely carefully. But, if it can be done in a macroscopically undetectable fashion, then the action only permutes the microscopic states belonging to a same macroscopic state. That is, a book whose pages are turned

carefully still contains the same content while its molecular configuration might have changed. Thus, it still counts as pure information utilization on this macroscopicity level.

The intuition that the permutation is invasive is not wrong, nonetheless, as manipulating a part of a correlated information source can indeed leak information. If you tossed a coin and wrote the outcome on a piece of paper, then the coin and the paper are correlated. In this case, if someone flips the coin, then you can detect it by referring to the paper. Actually, this is exactly how classical secret sharing works: encoding information into correlation and correlation only. Nevertheless, if you cannot access the paper, then interactions that might flip the coin can still count as pure information utilization. This shows that physicality of classical information is also relative because the choice of the system that you will treat as information source affects the physicality.

Nonetheless, a question on the possibility of universally nonphysical classical information still remains: Is it possible to utilize information of a classical system regardless of its relation with the outer world? Indeed, every permutation f that fixes every j, i.e., $f_2(i, j) = j$ for all i is compatible with every extension of system 2, i.e., a combination of system 2 and any system 3 that is arbitrarily correlated with system 2. Such a permutation corresponds to simply "reading" j and implementing a permutation on system 1 conditioned on j. One can easily see that this action never changes the joint probability distribution of systems 2 and 3. This is the notion of classical information we are familiar with: information that can be freely read and distributed and does not necessitate a nontrivial minimum amount of physical effect on information carriers.

Does the same conclusion hold for quantum information? In our definition [see (7)], utilizing only information in quantum state σ_B means leaking no information to it. In other words, we defined utilization of quantum information to be nonphysical as well. However, just like classical information sources, a quantum information source could be correlated with other systems, i.e., σ_B could be a marginal state of its extension σ_{AB}. We can easily observe that interacting with a part of correlated information source exactly corresponds to distributed catalysis of randomness and Theorem 4 says that TQ-TQ bipartite states cannot yield randomness through distributed catalysis. But, since every mixed state σ_B has a TQ-TQ extension σ_{AB}, namely, its purification. Hence, every utilization of quantum information can be detected by someone with enough amount of side information; there is no universally nonphysical quantum information, contrary to classical information. This observation can be summarized as follows.

Theorem 9. For any catalysis unitary $U_A \in \mathfrak{U}(A_S A_C)$ compatible with σ_{A_C}, there exists an extension $\sigma_{A_C B_C}$ of σ_{A_C} such that (U_A, U_B) is not compatible with $\sigma_{A_C B_C}$ for any $U_B \in \mathfrak{U}(B_S B_C)$.

One of the goals of establishing the framework of catalysis of quantum randomness is to distinguish "quantum state" and "quantum information," two terms that are often mixed up in quantum information community. This distinction is needed since quantum state describes every physically accessible properties of a quantum system, be it informational or not. Thus, accepting this distinction, the no-cloning theorem only forbids cloning of quantum state, not quantum information. In fact, the task of "cloning quantum information" must be carefully redefined. Nonetheless, the fact that there is no universally nonphysical quantum information hints that the gist of the no-cloning theorem still lives on for quantum information. The fact that cloning and distribution of classical state can be freely done strongly suggests that classical information is a nonphysical entity operationally independent of its physical representation, and vice versa. In contrast to this, quantum information is firmly bound to its physical representation, which can be interpreted to be strongly related to the fact quantum state is unclonable.

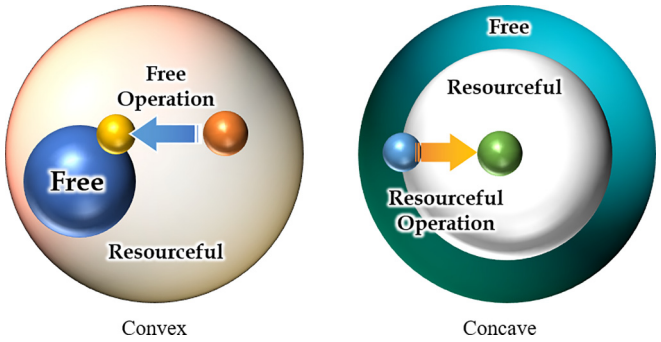


FIG. 8. Comparison of convex and concave resource theories. In a convex resource theory, a statistical mixture of two free objects is still free, and the action of free operation can only draw a resourceful object closer to the set of free objects. However, in a "concave" resource theory, any statistical mixture of two resourceful objects is resourceful, and there is no universal "resource destroying operation." However, there are resourceful operations that never make a resourceful object free.

We may summarize the results of this section with a slogan "quantum information is physical from a broader perspective" to emphasize the difference between classical and quantum information. In our formalism, pure information utilization is required to be nonphysical for a given information source in the first place, hence, the slogan should be interpreted as that for every pure quantum information utilization there exists an agent who perceives it not as a purely informational interaction, whereas the same may not hold for classical information. After all, as we pointed out, physicality of information depends on its definition and perspective of user.

11. Concave resource theories

As it was briefly outlined in the Introduction, we define *concave resource theory* as a theory that consists of the state of *resourceful states* $\mathfrak{R}$ ("the resourceful set") and the set of *resourceful operations*, operations that preserve $\mathfrak{R}$, $O_{\mathfrak{R}}$ (see Fig. 8). Here, the resourceful set $\mathfrak{R}$ is required to be convex, i.e., if $\rho, \sigma \in \mathfrak{R}$, then $\lambda\rho + (1-\lambda)\sigma \in \mathfrak{R}$ for any $0 \leqslant \lambda \leqslant 1$. Any state that is not resourceful is called *free*. In contrast to the fact that usually the distance to the concave set of free states is used as a measure of resource, it is natural to measure how deep inside a state is placed in the resourceful set in a concave resource theory. The most typical concave resource theory would be that of entropies, whose resource measures are Schur-concave entropic quantities.

As entropic measures like the von Neumann entropy are already a well-studied topic, one might consider concave resource theories are more or less trivial. However, there could be still other types of resource theories of randomness and the theory of catalytic quantum randomness is one of them. Albeit it is a concave resource theory, catalytic entropies are not concave functions. For example, slightly mixing the maximally mixed state with a nondegenerate state significantly decreases its catalytic entropy because it destroys the degeneracy of it.

Nevertheless, we could anticipate that superunitary operations must be a part of free operations of generic concave resource theories. Our definition of superunitary operation does not have one of the most distinct characteristics of the physical implementation of superchannels: the effect of memory system. This is because discarding subsystem is no longer a free operation in resource theory of randomness. There is only one exception and that is discarding a quantum system that is not allowed to change its marginal state because discarding such a system will not lead to any leakage of information, and that fits our definition of utilizing randomness and randomness only.

The resource theory of randomness (RTR), as a concave resource theory, has many implications that go against our intuition built from conventional convex resource theories. The resource in the RTR is randomness, which is not inherently a quantum property, hence not every object with large quantumness is superior compared to its classical counterpart. For example, a maximally entangled state shared by two parties, which is a very useful resource in entanglement theory, is completely useless in distributed catalysis of randomness. In general, whenever there is quantum correlation in a bipartite quantum state, there exist correlated parts the DCD, and it hinders catalytic extraction of randomness (see Sec. III I). It is because states with quantum correlation are sensitive to the action of local unital channels [49].

One should not understand it as that every quantumness is an obstacle in randomness extraction. For example, local coherence is helpful for maximizing extractable randomness of local parts. This is the very reason why there are dimension-doubling effects in catalytic quantum randomness. However, again, it does not mean that coherence already present in the state helps catalysis of quantum randomness. When we say that local coherence boosts catalytic quantum randomness, it means that exploiting coherent quantum operation boosts the efficiency of catalytic randomness extraction. The ambivalent roles of quantumness as presented here motivate the further study of quantum randomness to reveal its true nature and the extent of its power.

[1] I. Alexeev, K. Y. Kim, and H. M. Milchberg, Phys. Rev. Lett. **88**, 073901 (2002).
[2] A. Kaya, Am. J. Phys. **79**, 1151 (2011).
[3] G. Diener, Phys. Lett. A **223**, 327 (1996).
[4] D. Beckman, D. Gottesman, M. A. Nielsen, and J. Preskill, Phys. Rev. A **64**, 052309 (2001).
[5] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[6] P. Hayden and J. Preskill, J. High Energy Phys. 09 (2007) 120.
[7] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[8] A. Streltsov, G. Adesso, and M. B. Plenio, Rev. Mod. Phys. **89**, 041003 (2017).
[9] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[10] B. Regula, K. Bu, R. Takagi, and Z.-W. Liu, Phys. Rev. A **101**, 062315 (2020).
[11] B. Regula and R. Takagi, Nat. Commun. **12**, 4411 (2021).
[12] K. C. Tan, V. Narasimhachar, and B. Regula, Phys. Rev. Lett. **127**, 200402 (2021).
[13] J. Polchinski, in *New Frontiers in Fields and Strings: TASI 2015 Proceedings of the 2015 Theoretical Advanced Study Institute in Elementary Particle Physics* (World Scientific, Singapore, 2017), pp. 353–397
[14] M. Blum, ACM SIGACT News **15**, 23 (1983).
[15] S. H. Lie, H. Kwon, M. Kim, and H. Jeong, Quantum **5**, 405 (2021).
[16] S. H. Lie, S. Choi, and H. Jeong, Phys. Rev. A **103**, 042421 (2021).
[17] S. H. Lie and H. Jeong, Phys. Rev. A **101**, 052322 (2020).
[18] S. H. Lie and H. Jeong, Phys. Rev. Res. **3**, 013218 (2021).
[19] S. H. Lie and H. Jeong, Phys. Rev. Res. **3**, 043089 (2021).
[20] P. Boes, H. Wilming, R. Gallego, and J. Eisert, Phys. Rev. X **8**, 041016 (2018).
[21] E. Chitambar and G. Gour, Rev. Mod. Phys. **91**, 025001 (2019).
[22] M.-D. Choi, Linear Algebra Appl. **10**, 285 (1975).
[23] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
[24] G. Gour and C. M. Scandolo, arXiv:2101.01552.
[25] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Europhys. Lett. **83**, 30004 (2008).
[26] G. Gour, IEEE Trans. Inf. Theory **65**, 5880 (2019).
[27] G. Chiribella, G. M. DAriano, and P. Perinotti, Phys. Rev. A **80**, 022339 (2009).
[28] J. Burniston, M. Grabowecky, C. M. Scandolo, G. Chiribella, and G. Gour, Proc. R. Soc. A **476**, 20190832 (2020).
[29] A. Bisio and P. Perinotti, Proc. R. Soc. A **475**, 20180706 (2019).
[30] G. Chiribella, G. M. DAriano, P. Perinotti, and B. Valiron, Phys. Rev. A **88**, 022318 (2013).
[31] P. Daly, arXiv:2210.00370.
[32] S. H. Lie and H. Jeong, (unpublished).
[33] N. P. Landsman, arXiv:math-ph/9807030.
[34] U. Haagerup and M. Musat, Commun. Math. Phys. **303**, 555 (2011).
[35] E. Artin, in *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, Vol. 5 (Springer, Berlin, 1927), pp. 251–260.
[36] J. Wedderburn, Proc. London Math. Soc. **s2-6**, 77 (1908).
[37] M. M. Wolf, lecture notes available at http://www-m5.ma.tum.de/foswiki/pubM.
[38] L. Chen and L. Yu, Ann. Phys. **351**, 682 (2014).
[39] K. R. Zwier, Philos. Sci. **84**, 1303 (2017).
[40] K. Modi, Sci. Rep. **2**, 581 (2012).
[41] M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. A **67**, 062104 (2003).

[42] J. Scharlau and M. P. Mueller, Quantum **2**, 54 (2018).
[43] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Y. Halpern, Phys. Rep. **583**, 1 (2015).
[44] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).
[45] K. Mølmer, Phys. Rev. A **55**, 3195 (1997).
[46] S. Daftuar and M. Klimesh, Phys. Rev. A **64**, 042314 (2001).
[47] T. V. Kondra, C. Datta, and A. Streltsov, Phys. Rev. Lett. **127**, 150503 (2021).
[48] C. Datta, T. V. Kondra, M. Miller, and A. Streltsov, arXiv:2202.05228.
[49] S. H. Lie and H. Jeong, arXiv:2206.05899.
[50] L. Zhang and J. Wu, Phys. Lett. A **375**, 4163 (2011).
[51] F. Hiai, M. Mosonyi, D. Petz, and C. Bény, Rev. Math. Phys. **23**, 691 (2011).
[52] W. Roga, M. Fannes, and K. Życzkowski, J. Phys. A: Math. Theor. **41**, 035305 (2008).
[53] L. Floridi, *The Philosophy of Information* (Oxford University Press, Oxford, 2013).
[54] A. Korzybski, *Science and Sanity: An Introduction to Non-Aristotelian Systems and General Semantics* (Institute of General Semantics, Englewood, NJ, 1958).
[55] S. L. Braunstein and A. K. Pati, Phys. Rev. Lett. **98**, 080502 (2007).
[56] K. Modi, A. K. Pati, A. SenDe, and U. Sen, Phys. Rev. Lett. **120**, 230501 (2018).
[57] P. Kok and S. L. Braunstein, Phys. Rev. A **61**, 042304 (2000).
[58] K. Nemoto and S. L. Braunstein, Phys. Lett. A **333**, 378 (2004).
[59] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Commun. Math. Phys. **246**, 359 (2004).
[60] M. A. Nielsen, Phys. Rev. A **62**, 052308 (2000).
[61] X. Zhan, *Matrix Theory*, Vol. 147 (American Mathematical Society, Providence, RI, 2013).
[62] R. Landauer, Phys. Today **44**, 23 (1991).
[63] R. Landauer, Phys. A (Amsterdam) **263**, 63 (1999).
[64] D. Stoljar, Stanford Encyclopedia of Philosophy, https://plato.stanford.edu.