이학박사학위논문

Characterization of Quantum Information Through Catalytic Quantum Randomness

양자 임의도의 촉매 과정을 통한 양자정보의 특징화

2022년 2월

서울대학교 대학원

물리천문학부

이석형

Characterization of Quantum Information Through Catalytic Quantum Randomness

양자 임의도의 촉매 과정을 통한 양자정보의 특징화

정현석 교수님

이 논문을 이학박사 학위논문으로 제출함
2022년 1월

서울대학교 대학원
물리천문학부
이석형

이석형의 박사 학위논문을 인준함
2022년 2월

위 원 장	안 경 원	(인)
부위원장	정 현 석	(인)
위 원	김 도 헌	(인)
위 원	강 병 남	(인)
위 원	이 진 형	(인)

Characterization of Quantum Information Through Catalytic Quantum Randomness

Seok Hyung Lie

Supervised by

Professor **Hyunseok Jeong**

A Dissertation

Submitted to the Faculty of

Seoul National University

in Partial Fulfillment of

the Requirements for the Degree of

Doctor of Philosophy

Jan. 2022

Department of Physics and Astronomy

The Graduate School

Seoul National University

Abstract

Characterization of Quantum Information Through Catalytic Quantum Randomness

Seok Hyung Lie
Department of Physics and Astronomy
The Graduate School
Seoul National University

We generalize the theory of catalytic quantum randomness by Boes et al. to delocalized and dynamical settings. Our result is twofold. First, we expand the resource theory of randomness (RTR) by calculating the amount of (Rényi) entropy catalytically extractable from a correlated or dynamical randomness source. In doing so, we show that no entropy can be catalytically extracted when one cannot implement local projective measurement on randomness source without altering its state. The RTR, as an archetype of the 'concave' resource theory, is complementary to the convex resource theories in which the amount of randomness required to erase the resource is a resource measure. 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. On the other hand, we study the physical properties of information flow. Popularized quotes like “information is physical” by Landauer or “it from bit” by Wheeler suggest the matter-like picture of information that can travel from one place to another with the definite direction while leaving detectable traces on its region of departure. To examine the validity of this picture, we focus on that catalysis of randomness models directional flow of information with the distinguished source and recipient. We show that classical information can always spread from its source without altering its source or its surrounding context, like an immaterial entity, while quantum information cannot. Using the framework developed in this dissertation, we suggest an approach to formal definition of semantic quantum information and claim that utilizing semantic information is equivalent to using a partially depleted information source. By doing so, we unify the utilization of semantic and non-semantic quantum information and conclude that one can always extract more information from a not completely depleted classical randomness source, but it is not possible for quantum randomness sources.

Keywords : Quantum information, Resource theory, Randomness

Student Number : 2016-20311

Contents

List of Figures

List of Publications

This dissertation is largely based on the following research work in progress by the author.

1. **Seok Hyung Lie**, Hyunsek Jeong
   "Delocalized and Dynamical Catalytic Randomness", **in preparation**

The content of this dissertation expands the results of the following first-author publications:

1. **Seok Hyung Lie** and Hyunseok Jeong
   "Randomness cost of masking quantum information and the information conservation law", **Phys. Rev. A 101, 052322** (2020)

2. **Seok Hyung Lie** and Hyunseok Jeong
   "Randomness for quantum channels: Genericity of catalysis and quantum advantage of uniformness", **Phys. Rev. Research 3, 013218** (2021)

3. **Seok Hyung Lie**, Hyukjoon Kwon, MS Kim and Hyunseok Jeong
   "Quantum one-time tables for unconditionally secure qubit-commitment", **Quantum 5, 405** (2021)

4. **Seok Hyung Lie**, Seongjeon Choi and Hyunseok Jeong
   "Min-entropy as a resource for one-shot private state transfer, quantum masking, and state transition", **Phys. Rev. A 103, 042421** (2021)

5. **Seok Hyung Lie** and Hyunsek Jeong
   "Catalytic quantum randomness as a correlational resource", **Phys. Rev. Research 3, 043089** (2021)

This dissertation also contains the results of the following preprints:

1. **Seok Hyung Lie**, Yong Siah Teo and Hyunseok Jeong
   "Hacking Quantum Networks: Extraction and Installation of Quantum Data", **arXiv:2105.13823**

This dissertation also contains the results of the following preprints in preparation:

1. **Seok Hyung Lie**, Hyunsek Jeong
   "Faithfulness and sensitivity for ancilla-assisted process tomography", **in preparation**

2. **Seok Hyung Lie**, Hyunsek Jeong
   "Generalized Transposition, Perfect Tensors, Spacetime and Supertrace", **in preparation**

Although not related to the central theme of this dissertation, during the doctoral course, the following other first-author and co-author publications were produced:

1. **Seok Hyung Lie** and Hyunseok Jeong
   "Limitations of teleporting a qubit via a two-mode squeezed state", **Photonics Research 7(5), A7-A13**, (2019)

2. Changhun Oh, Changhyoup Lee, **Seok Hyung Lie** and Hyunseok Jeong
   "Optimal distributed quantum sensing using Gaussian states", **Phys. Rev. Research 2, 023030** (2020)

Chapter 1

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 space-like 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 any 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 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 the 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 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 spacetime 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, 11, 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 non-convex 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 will say to be *concave*. In these resource theories, the set of resourceful objects, not the free objects, is convex (see FIG. 6). 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's 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 soure can yield. Hence, in a sense, forgetting information could create randomness. Thus, an archetype of concave resource theory is the resource theory of randomness (RTR) [15, 16, 17, 18, 19, 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 [20]. 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 delocalized randomness source, and the simple action of rolling dice itself is a dynamical source of randomness. In this dissertation, we extend the limit of the RTR to encompass utilization of delocalized and dynamical randomness sources by employing the Choi-Jamiołkowski isomorphism [22, 23] and the language of dynamical resource theory [24].

1.1 Preliminaries

1.1.1 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 i-th largest eigenvalue including degeneracy, i.e., it is possible that $\lambda_i(\sigma) = \lambda_{i+1}(\sigma)$. For any Hilbert spaces X and Y, $X \leq Y$ 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 $\text{Ad}_M \in \mathfrak{L}(X)$ be

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

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 used 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 non-increasing 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 it only acts on a part of multipartite quantum channels are called *superchannel* [25, 26, 27, 28, 29, 30, 24] 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 $\mathcal{N} \in \mathfrak{L}(X)$.

The *supertrace* [31] is the superchannel counterpart of the trace operation modelling the loss of dynamical quantum information, denoted by $\mathfrak{Tr}$. The supertrace is defined in such a way that the following diagram is commutative:

$$\begin{array}{ccc} \mathfrak{L}(X) & \xrightarrow{\mathfrak{Tr}} & \mathbb{C} \\ \big\downarrow{\scriptstyle J} & & \big\downarrow{\scriptstyle \mathrm{id}_{\mathbb{C}}} \\ \mathfrak{B}(X \otimes X') & \xrightarrow{\mathrm{Tr}} & \mathbb{C} \end{array} . \tag{1.1}$$

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,

$$\mathfrak{Tr}[\mathcal{M}] := \mathrm{Tr}\big[J^{\mathcal{M}}_{XX'}\big] = \mathrm{Tr}[\mathcal{M}(\pi_X)], \tag{1.2}$$

for all $\mathcal{M} \in \mathfrak{L}(X)$. From (1.2), 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:

$$\begin{array}{ccc} \mathfrak{L}(X) & \xrightarrow{\Theta} & \mathfrak{L}(Y) \\ \big\downarrow{\scriptstyle J} & & \big\downarrow{\scriptstyle J} \\ \mathfrak{B}(X \otimes X') & \xrightarrow{\mathbb{J}[\Theta]} & \mathfrak{B}(Y \otimes Y') \end{array} . \tag{1.3}$$

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 make them mutually orthogonal. One possible implementation is $\bigoplus_i B_i := \sum_i |i\rangle\langle i| \otimes B_i$.

1.1.2 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 modelled with a C^*-algebra [32, 33], and a finite dimensional C^*-algebra is isomorphic to a direct sum of full matrix algebras by the Artin-Wedderburn theorem [34, 35]. In other words, for every finite dimensional C^*-algebra $\mathcal{C}$, there exist finite dimensional Hilbert spaces X_i such that $\mathcal{C} \approx \bigoplus_{i=1}^n \mathfrak{B}(X_i)$.

In fact, it is equivalent to saying that the system X is under *superselection rules* which means that there exists 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. We call the vector $(|X_1|, |X_2|, \cdots, |X_n|)$ the *dimension vector* of $\mathcal{C}$ and n the *dimension rank* of $\mathcal{C}$. To make the dimension vector unique, we assume that $|X_1| \geq |X_2| \geq \cdots$ unless there is a pre-defined order of X_i in the given context. When the dimension rank is larger than 1, we say that $\mathcal{C}$ is partially classical When

$|X_i| = 1$ for every i, we say that $\mathcal{C}$ is (completely) classical. If the dimension rank is 1, we say that $\mathcal{C}$ is (totally) quantum.

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

$$\rho_{AB} = \sum_i p_i \, |i\rangle\langle i|_A \otimes \rho_B^i, \tag{1.4}$$

for some probability distribution $\{p_i\}$ and quantum states $\rho_B^i \in \mathfrak{S}(B)$. 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,

$$\rho_{AB} = \sum_i (\Pi_i \otimes \mathbb{1}_B) \rho_{AB} (\Pi_i \otimes \mathbb{1}_B). \tag{1.5}$$

If (1.5) holds, we also say that ρ_{AB} is generalized block-diagonal with respect to $A = \bigoplus_i A_i$ where $A_i = \mathrm{supp}\,(\Pi_i)$ [36]. 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 and, if it is neither PC-Q nor Q-PC, we will call it totally quantum-quantum (TQ-Q).

Chapter 2

Characterizations of catalytic randomness

In this Chapter, we give an intuitive motivation for the study of resource theory of catalytic randomness. See Ref. [20] for related discussion.

2.1 Internal and external information

There is one interpretation of information which considers that information *we have* about systems is the information those systems carry. This kind of interpretation requires or implicitly assumes a user outside of a system, hence we will call it *external information* of the system. From this perspective, randomness of a state is a *noise*. This is why when a pure state becomes mixed, often it is said that information is destroyed [37]. Similarly, this is why often the no-cloning theorem is interpreted to forbid copying quantum information [38, 39], when the exact statement is that it is impossible to copy an arbitrary single pure state. In this sense, a certain aspect of external information of a system can be quantified with nonuniformity [40]. However, it actually quantifies the *capability* of carrying information rather than the amount of information *per se*. The external perspective often implicitly assumes implications of a certain piece of information has about other systems, say, n-photon state $|n\rangle$ carries more energy than vacuum state

$|0\rangle$. However, this meaning heavily depends on its user and hence is highly subjective.

In this framework, a state only represents the current status of a system, and its *change* is considered to carry information in this interpretation. It requires sender's coding and receiver's decoding, thus external information tends to be more dynamical. In other words, one says that (external) information at region A *does not* flow to region B via a map $\Lambda_{A\to B}$ when $\Lambda_{A\to B}$ is constant, i.e.,

$$\Lambda_{A\to B}(\rho) = \Lambda_{A\to B}(\sigma), \tag{2.1}$$

for every state ρ and σ. If it is not the case, one says that information flows from A to B. Information source that provides information to be encoded is often treated implicitly and assumed to be outside of information transmission processes.

However, there is another line of thought on information that focuses on information contained *inside* a system, or the *internal information*. For example, a cylinder filled with gas can be said to contain a lot of information as one can learn a lot of data by inspecting the configuration of its constituting gas molecules. Simply put, internal information is information of a system when treated as a black box. The Shannon information theory is built on the observation that acquisition of the state of a system is considered more informative when the state appears more random before the acquisition. Hence, classically, the *information content* or *surprisal* $I(x)$ of an event $x \in \mathcal{X}$ is defined as [5, 41]

$$I(x) = -\log_2 \Pr[X = x], \tag{2.2}$$

so that the *average* information content, or the *Shannon entropy* of probability distribution P is

$$H(P) = -\sum_{x \in \mathcal{X}} P(x) \log_2 P(x). \tag{2.3}$$

The von Neumann entropy of a quantum state ρ defined as

$$S(\rho) = -\operatorname{Tr}[\rho \log_2 \rho], \tag{2.4}$$

can be interpreted in the same fashion, so that $S(\rho)$ represents the amount of classical internal information of ρ. (We will elaborate on the meaning of 'classical' afterwards.) Internal information perspective treats information explicitly, for example, since one can calculate the entropy of each local system, it is easy to locate and quantify information. From this perspective, randomness and information are identified, and maximally mixed states are maximally informative states. Since the state completely decides internal information of a system, the role of observer or context is minimal in this interpretation.

From this perspective, correlation is formed when information propagates from its source to other systems. Hence, when system A and B initially prepared in an uncorrelated state $\sigma_A \otimes \rho_B$ interact, one says that (internal) information does not flow from A to B if, for any extension σ_{AR} with some reference system R, systems RB are still uncorrelated after the interaction. If not, information propagates from A to B through the interaction.

These two interpretations look completely contradictory to each other, however, they are actually two complementary views on information. For example, classically, one way to measure external information is the *relative entropy* $D(P\|U)$ from the maximally uniform distribution $U(x) = |\mathcal{X}|^{-1}$, where $D(P\|Q)$ is the relative entropy that measures the statistical separation between two distributions and is given as $D(P\|Q) := \sum_{x\in\mathcal{X}} P(x)\log_2(P(x)/Q(x))$. They are in the following clear-cut trade-off relation,

$$H(P) + D(P\|U) = \log_2 |\mathcal{X}|, \tag{2.5}$$

for the case of the von Neumann entropy the same thing holds *mutatis mutandis*, hence discussion about information inside or about a system are essentially the same except for their opposite signs up to additive constant.

Moreover, two notions of information flows introduced above are actually equivalent to each other [20]; if internal information does not flow, then neither does external information. Therefore, to treat information flow on the same footing with any other flow of physical entities, we will first characterize flow of internal information and try to explain all the other informational phenomena in terms of internal information. This is in line with relational approach to quantum mechanics by Rovelli [42] and Everett [43]. To treat the noisy aspect and the informational aspect of randomness neutrally, we will use 'randomness' and 'information' interchangeably so that all the results can be used regardless of one's interpretation of randomness.

In this context, an information source stripped of its semantic meaning is nothing but a randomness source. Hence, we can say that randomness captures the universal quantitative aspect of information independent of their meaning, and Shannon information theory successfully quantifies this non-semantic information with entropic quantities. Thus, in this dissertation, we will use the term ‘randomness’ to emphasize this semantics-independent quantitative aspect of internal information. This is what referred to as ‘Information-B’ among three types of information in the *Handbook of Philosophy of Information* [44]. (By Ref. [44], ‘Information-A’ focuses on semantics, and ‘Information-C’ focuses on algorithmic complexity.) We will focus on the analysis of non-semantic information first, but we will tackle the problem of analyzing semantic information in Section 3.4.

2.2 Catalytic randomness and information flow

In Introduction, we observed that 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 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 is 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 interactions have *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 a 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.

We already discussed why randomness is crucial for an information source. Information usage is entropy extraction process, hence correlation between a source and it user is naturally built in the process and the amount

Figure 1: A book is a randomness (or 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.

of correlation formed can be interpreted as the amount of randomness extracted from the source [20].

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/quantum mechanics in closed systems, as there are events 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 (or 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 [20]. 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 dissertation, 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 dissertation. 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, 16, 18, 19, 20].

Note that we do not concern ourselves with the issue 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 pre-existing randomness sources regardless of their generation mechanism. Hence, 'quantum randomness (source)' in this dissertation is not related to what 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 dissertation 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.

Chapter 3

Resource Theory of Randomness

3.1 Catalytic randomness

In this Section, we summarize and review the results of the correlational resource theory of catalytic randomness [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.

$$\operatorname{Tr}_B \operatorname{Ad}_U(\rho_A \otimes \sigma_B) = \mathcal{N}(\rho), \quad \forall \rho \in \mathfrak{S}(A). \tag{3.1}$$

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

$$\operatorname{Tr}_A \operatorname{Ad}_U(\rho_A \otimes \sigma_B) = \sigma_B \quad \forall \rho \in \mathfrak{S}(A). \tag{3.2}$$

The conditions above require the catalyst to be insensitive to dynamically changing state of the target system. This dynamical definition can be re-expressed 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 (3.2) 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 $(\Theta_A \otimes \mathfrak{id}_B)(\mathcal{U})$ fixes the marginal state σ_B, i.e.

$$\mathrm{Tr}_A[(\Theta_A \otimes \mathfrak{id}_B)(\mathcal{U})(\rho_A \otimes \sigma_B)] = \sigma_B. \tag{3.3}$$

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

$$\mathrm{Tr}_A[\mathrm{id}_R \otimes \mathrm{Ad}_U(\tau_{RA} \otimes \sigma_B)] = \tau_R \otimes \sigma_B^{(V)}. \tag{3.4}$$

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

A more detailed discussion on the condition given in terms of superchannels can be found in Section 3.4.

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 (3.1) and (3.2).

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 leads 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 2. 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

$$\mathrm{Tr}_A[\mathrm{id}_R \otimes \mathrm{Ad}_U(\tau_{RA} \otimes \sigma_B)] = \tau_R \otimes \sigma_B. \tag{3.5}$$

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

$$\mathrm{Tr}_A[\mathrm{id}_R \otimes \mathrm{Ad}_U(\rho_{RA} \otimes \sigma_B)] = \rho_R \otimes \sigma_B. \tag{3.6}$$

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 [45] 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 (3.1) and (3.2) 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 (3.1) is catalytic. We will call the bipartite unitary operator used for catalysis a *catalysis unitary* operator.

We will say that U is compatible with σ (and vice versa) if (3.2) holds. If (3.2) 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 [46, 47, 40] 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

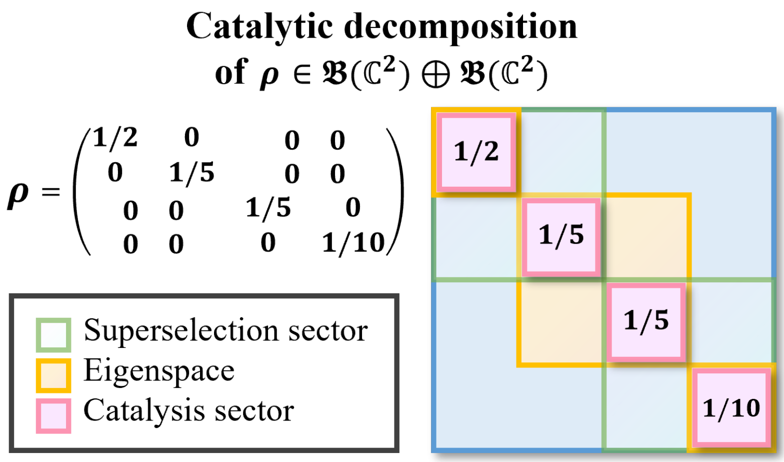


Figure 2: Catalytic decomposition of a density matrix. A superselection rule forbids between subspaces called superselection sectors, and each density matrix has an eigenspace for each distinct eigenvalue. The intersection of a superselection sector and an eigenspace is called a catalysis sector and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

Theorem, we review the characterization of catalytic unitary operators and compatibility.

Theorem 3 ([20])**.** 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 $[U, \mathbb{1}_A \otimes \sigma_B] = 0$.

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 $\mathcal{F}(\rho) = \sigma$ [48]. 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 Ref. [19, 20] that non-degeneracy of eigenvalues of a mixed state restricts catalysis of quantum randomness. Accordingly, *the catalytic Rényi entropy* $S_\alpha^\diamond(\sigma)$ of order $\alpha \geq 0$ 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 $i \mapsto \lambda_i \geq 0$. 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 $\mathrm{supp}\,(\Pi_i) \leq X_{f(i)}$ 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).

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

$$\mathfrak{c}\,(\sigma) = \bigoplus_i \frac{\lambda_i}{r_i} \mathbb{1}_{r_i^2}, \tag{3.7}$$

where $\mathbb{1}_{r_i^2} = \mathrm{diag}(1, \cdots, 1)$ is the identity matrix of size r_i^2. It was shown in Ref.[20] 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 [20], $S_\alpha\,(\mathfrak{c}\,(\sigma))$ 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.

$$S_{\alpha}^{\diamond}(\sigma) := \frac{1}{1-\alpha} \log_2 \left[\sum_i \lambda_i^{\alpha} r_i^{2-\alpha} \right]. \tag{3.8}$$

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

$$\lim_{\alpha \to \infty} S_{\alpha}^{\diamond}(\sigma) = S_{\min}^{\diamond}(\sigma) := -\log_2 \left[\max_i \lambda_i / r_i \right],$$

and the max-catalytic entropy

$$\lim_{\alpha \to 0+} S_{\alpha}^{\diamond}(\sigma) = S_{\max}^{\diamond}(\sigma) := \log_2 \left[\sum_i r_i^2 \right].$$

The catalytic entropies are important because of the following operational meaning.

Theorem 4 ([20])**.** The maximum amount of catalytically extractable Rényi entropy of order $\alpha \geq 0$ 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 5. 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.

3.2 Delocalized 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 delocalized 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 [49]. A way to resolve the confusion is explicitly take account of the correlation, especially the entanglement, between laser light and the laser device. A detailed discussion can be found in Appendix.

The detailed setting of delocalized catalysis of randomness is as follows. Instead of one party, let there be two parties, Alice (A_0) and Alex (A_1), separated in different laboratories. They start with an initial bipartite state $\rho_{A_0A_1}$, and they are provided with a bipartite state $\sigma_{B_0B_1}$ as a randomness source that they should return unchanged. Alice can only control A_0B_0 and Alex can only control A_1B_1. They try to transform their initial state into some other state $\mathcal{N}(\rho_{A_0A_1})$ without altering the randomness source. We allow no communication between them in this process because communication establishes new shared randomness sources between them.

In the quantum setting, Alice will apply unitary operator U_0 to A_0B_0, and Alex will apply U_1 to A_1B_1. Just like the original catalysis scenario, they are required to preserve $\sigma_{B_0B_1}$ after the interaction, regardless of their initial state $\rho_{A_0A_1}$. This requirement can be summarized as

$$\mathrm{Tr}_{B_0B_1}[\mathrm{Ad}_{U_0\otimes U_1}(\rho_{A_0A_1}\otimes\sigma_{B_0B_1})]=\mathcal{N}(\rho_{A_0A_1}), \tag{3.9}$$

with some quantum channel $\mathcal{N}\in\mathfrak{C}(A_0A_1)$ and

$$\mathrm{Tr}_{A_0A_1}[\mathrm{Ad}_{U_0\otimes U_1}(\rho_{A_0A_1}\otimes\sigma_{B_0B_1})]=\sigma_{B_0B_1}, \tag{3.10}$$

for all $\rho_{A_0A_1}\in\mathfrak{S}(A_0\otimes A_1)$. We will call this type of catalysis a *delocal-*

ized catalysis of randomness and when it is needed to emphasize it, we call $\sigma_{B_0B_1}$ in this situation the *delocalized randomness source*. We say that the catalysis unitary operator pair (U_0, U_1) is compatible with $\sigma_{B_0B_1}$ if (3.10) holds, and vice versa, and we say that they are compatible up to local unitary when there exists some $V_i \in \mathfrak{U}(B_i)$ for $i = 0, 1$ such that (3.10) holds with the right hand side substituted with $\mathrm{Ad}_{V_0 \otimes V_1}(\sigma_{B_0B_1})$. If we need to emphasize, we will call the special case $V_i = \mathbb{1}_{A_i}$ for $i = 0, 1$ the *canonical* case. When we focus on the action of each local party, we say that $U \in \mathfrak{U}(A_0B_0)$ is compatible with $\sigma_{B_0B_1}$ on B_0 when $(U, \mathbb{1}_{A_1B_1})$ is compatible with $\sigma_{B_0B_1}$.

We can observe that delocalized catalysis can be considered a special case of catalysis of randomness. Thus, Theorem 3 applies here too, hence $U_0 \otimes U_1$ must be catalytic, implying that U_0 and U_1 must be catalytic unitary operators themselves. Also, for $\sigma_{B_0B_1}$ to be compatible with $U_0 \otimes U_1$, it must be that $[U_0 \otimes U_1, \sigma_{B_0B_1}] = 0$. 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 delocalized catalysis too?

Now, we observe that, in delocalized 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 [50].

Lemma 6 ([50].)**.** 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 not a PC-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 7. No randomness can be catalytically extracted from a bipartite quantum state if and only if it is totally quantum-quantum.

The reason why catalysis sectors were identified in local catalysis of randomness was that they are the maximum subspace within which non-trivial 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 delocalized 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.

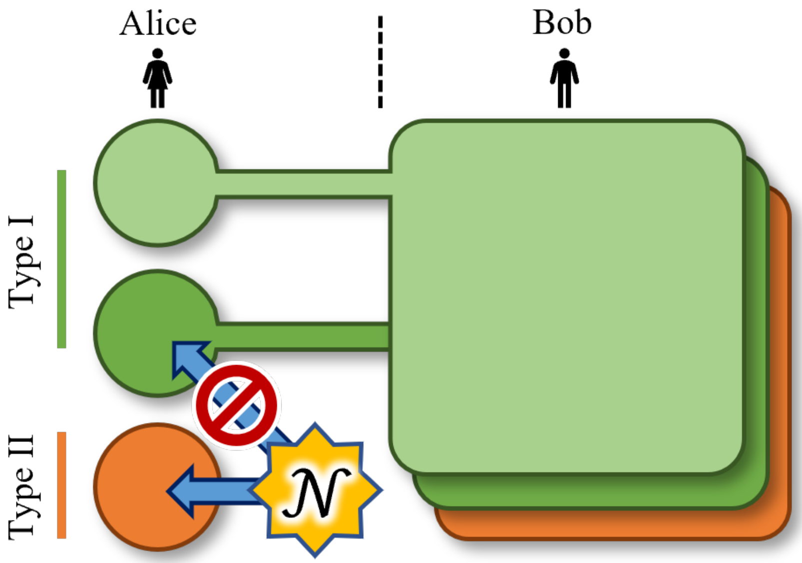


Figure 3: Type I and type II subspaces of the essential decomposition of A (Alice) for ρ_{AB}. Alice is quantumly correlated with B (Bob) on Type I subspaces, hence ρ_{AB} resists the action of unital maps without leaving detectable effects on it. But, Alice is uncorrelated with Bob on type II subspaces, so an arbitrary unital channel can be applied to type II subspaces without changing ρ_{AB}.

Definition 8. Let $\rho_{AB} \in \mathfrak{S}(AB)$ be a bipartite quantum state. $A = \bigoplus_i A_i$ is the *essential decomposition* of A for ρ_{AB}, $(\Pi_i := \mathbb{1}_{A_i})$ if

(i) For every i,

$$[\Pi_i \otimes \mathbb{1}_B, \rho_{AB}] = 0. \tag{3.11}$$

(ii) Each $(\Pi_i \otimes \mathbb{1}_B)\rho_{AB}(\Pi_i \otimes \mathbb{1}_B)$ is either not a PC-Q state ($i \in \mathcal{I}_A$, "type I") or a product state of the form $\pi_{A_i} \otimes \sigma_B$ for some $\sigma \in \mathfrak{S}(B)$ ($i \in \mathcal{II}_A$, "type II") after normalization.

(iii) Whenever any projector P does not commute with some of Π_i, we have $[P \otimes \mathbb{1}_B, \rho_{AB}] \neq 0$.

If none of Π_i is the identity operator on A, we say ρ_{AB} is a PC-Q state with respect to the essential decomposition $A = \bigoplus_i A_i$.

We will use the term "type I (or II)" for the indices i, the corresponding components $(\mathrm{Ad}_{\Pi_i} \otimes \mathrm{id}_B)(\rho_{AB})$ and the subspaces A_i accordingly. The essential decomposition is unique: See Appendix A.5 for the discussion on the uniqueness of essential decomposition. We will call the corresponding decomposition of $\rho_{AB} = \sum_i (\mathrm{Ad}_{\Pi_i} \otimes \mathrm{id}_B)(\rho_{AB})$ the essential decomposition of ρ_{AB} on A.

Why are type I and type II separated? Non PC-Q state are known to be sensitive to the perturbations of unital maps [50], thus it is impossible to interact through a catalytic unitary operator without leaving detectable effects. Hence, non PC-Q components are separated as type I. Any PC-Q state can be further decomposed into non PC-Q state, but if it is in a product state, then they can yield quantum advantage as we will see soon, thus they are separated as type II. On the other hand, the essential decomposition is related with the structure of entropy non-increasing state under unital channels [51, 52], in which there are only two types of components, one which only permits unitary operations (corresponding to type I), and the other which permits any unital subchannel but should be the maximally mixed state (corresponding to type II).

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 partially classical 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 9. A unital channel $\mathcal{N} \in \mathfrak{UC}(A)$ fixes a quantum state ρ_{AB} that is PC-Q with respect to the essential decomposition $A = \bigoplus_i A_i$ (let $\Pi_i := \mathbb{1}_{A_i}$) with corresponding type index sets $\mathcal{I}_A$ and $\mathcal{II}_A$ if and only if $\mathcal{N}$ preserves every subspace A_i and acts trivially on A_i when $i \in \mathcal{I}_A$.

See Appendix A.6 for a deeper analysis of essential decomposition. Now we introduce a bipartite generalization of catalytic decomposition that we will call the *delocalized catalytic decomposition* through the essential decomposition.

Definition 10. Let ρ_{AB} be a bipartite quantum state with the essential decompositions of $A = \bigoplus_i A_i$ and $B = \bigoplus_i B_i$, with $\Pi_i^A := \mathbb{1}_{A_i}$ and $\Pi_j^B := \mathbb{1}_{B_j}$. The type index sets for each decomposition are given as $\mathcal{I}_A$, $\mathcal{II}_A$, $\mathcal{I}_B$ and $\mathcal{II}_B$, respectively. The delocalized catalytic decomposition (DCD) of a bipartite quantum state $\rho_{AB} \in \mathfrak{S}(AB)$ is the spectral decomposition of the following form,

$$\rho_{AB} = \bigoplus_{i,j} (\Pi_i^A \otimes \Pi_j^B) \rho_{AB} (\Pi_i^A \otimes \Pi_j^B). \tag{3.12}$$

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 delocalized 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 *delocalized catalytic Rényi entropy*.

Definition 11. For the DCD of ρ_{AB} given in (3.12), we let $\tau_i := |0\rangle\langle 0|$ if $i \in \mathcal{I}_A$ and let $\tau_i := \pi_{T_i}$, where $T_i = \mathbb{C}^{|A_i|^2}$ if $i \in \mathcal{II}_A$. Similarly, we let $\kappa_j := |0\rangle\langle 0|$ if $j \in \mathcal{I}_B$ and let $\kappa_j := \pi_{K_j}$, where $K_j = \mathbb{C}^{|B_j|^2}$ if $j \in \mathcal{II}_B$. Also, let $p_{ij} := \mathrm{Tr}\left[(\Pi_i^A \otimes \Pi_j^B)\rho_{AB}\right]$. Then, the delocalized catalytic Rényi entropy $S_\alpha^{\diamond\diamond}(\rho_{AB})$ of ρ_{AB} is defined as the following way.

$$S_\alpha^{\diamond\diamond}(\rho_{AB}) := S_\alpha\left(\bigoplus_{i,j} p_{ij}\tau_i \otimes \kappa_j\right). \tag{3.13}$$

Here, we call the state $\mathfrak{d}(\rho_{AB}) := \bigoplus_{i,j} p_{ij}\tau_i \otimes \kappa_j$ the delocalized randomness-exhausting output (DREO) of ρ_{AB}.

Just like the catalytic entropies, the delocalized catalytic entropies also have the same kind of operational meaning.

Theorem 12. The maximum Rényi entropy that can be catalytically extracted from a delocalized randomness source $\sigma_{B_0B_1}$ is its delocalized catalytic Rényi entropy.

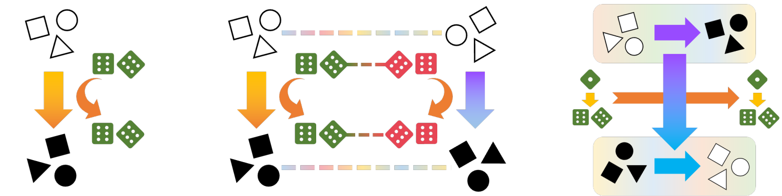
Hence, we successfully quantified the amount of catalytically extractable randomness in the delocalized setting. This analysis of static but delocalized randomness sources can be directly applied to dynamical randomness sources through the Choi-Jamiołkowski isomorphism in the next Section.

Note that if there is no correlation in the delocalized randomness source, i.e., $\sigma_{B_0B_1} = \sigma_{B_0} \otimes \sigma_{B_1}$, then there are no type I subspaces in the essential decompositions, so delocalized catalysis simply reduces to two independent local catalyses with $S_\alpha^{\diamond\diamond}(\sigma_{B_0} \otimes \sigma_{B_1}) = S_\alpha^{\diamond}(\sigma_{B_0}) + S_\alpha^{\diamond}(\sigma_{B_1})$.

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

3.3 Dynamical catalytic randomness

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



(a) Static and local randomness

(b) Delocalized randomness

(c) Dynamical randomness

Figure 4: Comparison of three types of catalysis of quantum randomness. Randomness represented by dices enters the interaction and leaves it locally unchanged but correlated with the system. As it can be seen from diagrams (b) and (c), delocalized catalysis and dynamical catalysis of randomness are intimated related; rotating one diagram by 90 degrees makes it very similar to the other one.

by a static state, i.e., the maximally mixed state π_X, but the action of rolling a dice can be modelled by the depolarizing map $\mathcal{R} \in \mathfrak{C}(X)$,

$$\mathcal{R}(\rho) = \pi_X \operatorname{Tr}[\rho], \tag{3.14}$$

for any initial state ρ of the dice with classical system X. Even in this case, we claim that the requirement of catalytic randomness utilization still holds. In other words, if you have no idea for which game it is used and only observe the dice rolling, then you should not acquire any information of the actual game play. This 'information non-leaking' property is very important for characterizing pure randomness utilization [20], 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. See Section 2 for more discussion. 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 $\mathcal{R}$. (See Section 4.2.) 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 system of a given process, i.e. $\mathfrak{Tr}(\mathcal{N}) := \mathrm{Tr}[\mathcal{N}(\pi_X)]$. (See Section 1.1.1.)

Before considering the most general case, we first analyze a simpler 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 $\Theta \in \mathfrak{SL}(A)$ is *catalytic* when there is a bipartite superunitary operation $\Omega \in \mathfrak{L}(AB)$ and a channel $\mathcal{R} \in \mathfrak{C}(B)$ such that

$$\mathfrak{Tr}_B\Omega(\mathcal{N} \otimes \mathcal{R}) = \Theta(\mathcal{N}), \tag{3.15}$$

and

$$\mathfrak{Tr}_A\Omega(\mathcal{N} \otimes \mathcal{R}) = \mathfrak{Tr}[\mathcal{N}]\mathcal{R}, \tag{3.16}$$

for all $\mathcal{N} \in \tilde{\mathfrak{C}}(A)$. (See Section 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 (3.15) and (3.16) hold for some superchannel Θ and every $\mathcal{N} \in \mathfrak{C}(A)$.

Since a superunitary Ω can be decomposed into the actions of preunitary U_0 and postunitary U_1 [24], i.e., $\Omega(\mathcal{N}) = \mathrm{Ad}_{U_1} \circ \mathcal{N} \circ \mathrm{Ad}_{U_0}$, therefore (3.15) and (3.16) can be expressed as $\mathfrak{Tr}_B[\mathrm{Ad}_{U_1} \circ \mathcal{N} \otimes \mathcal{R} \circ \mathrm{Ad}_{U_0}] = \Theta(\mathcal{N})$ and $\mathfrak{Tr}_A[\mathrm{Ad}_{U_1} \circ \mathcal{N} \otimes \mathcal{R} \circ \mathrm{Ad}_{U_0}] = \mathcal{R}$. By considering the Choi matrices, we get the following expressions

$$\mathrm{Tr}_{BB'}[\mathrm{Ad}_{U_1 \otimes U_0^T}(J^{\mathcal{N}}_{AA'} \otimes J^{\mathcal{R}}_{BB'})] = J^{\Theta(\mathcal{N})}_{AA'}, \tag{3.17}$$

and

$$\mathrm{Tr}_{AA'}[\mathrm{Ad}_{U_1 \otimes U_0^T}(J^{\mathcal{N}}_{AA'} \otimes J^{\mathcal{R}}_{BB'})] = J^{\mathcal{R}}_{BB'}, \tag{3.18}$$

for all $\mathcal{N} \in \tilde{\mathfrak{C}}(A)$. 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 (3.17) and (3.18) are equivalent to the following requirements, in turn:

$$\mathrm{Tr}_{BB'}[\mathrm{Ad}_{U_1 \otimes U_0^T}(\rho_{AA'} \otimes J^{\mathcal{R}}_{BB'})] = \mathbb{J}[\Theta](\rho_{AA'}), \tag{3.19}$$

and

$$\mathrm{Tr}_{AA'}[\mathrm{Ad}_{U_1 \otimes U_0^T}(\rho_{AA'} \otimes J^{\mathcal{R}}_{BB'})] = J^{\mathcal{R}}_{BB'}, \tag{3.20}$$

for every $\rho_{AA'} \in \mathfrak{S}(A \otimes A')$. Here, U_1 acts on AB and U_0^T acts on $A'B'$. Now, we can observe that (3.15) and (3.16) are only a special case of (3.9) and (3.10) after some change of notations, thus we can conclude that Ω is catalytic if and only if $U_0^{T_A} \otimes U_1^{T_{B'}}$ is unitary. It is equivalent to saying both

U_0 and U_1 are catalytic themselves.

Theorem 13. 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 $J^{\mathcal{R}}_{BB'}$, i.e.,

$$[U_1 \otimes U_0^T, \mathbb{1}_{AA'} \otimes J^{\mathcal{R}}_{BB'}] = 0. \tag{3.21}$$

The vanishing commutator condition (3.21) follows from Theorem 3. When $\mathcal{E}(\rho) = \pi_B \operatorname{Tr}[\rho]$ is the depolarizing map on B, its Choi matrix is $J^{\mathcal{E}}_{BB'} = \pi_B \otimes \pi_{B'}$, therefore $[U_1 \otimes U_0^T, \mathbb{1}_{AA'} \otimes J^{\mathcal{E}}_{BB'}] = 0$ 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 operations 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 $S_\alpha\left(J^{\Theta(\mathcal{N})}_{AA'}\right) - S_\alpha\left(J^{\mathcal{N}}_{AA'}\right)$, for every $\alpha \geq 0$, as a measure of extracted randomness. When $\alpha = 1$, $S_\alpha\left(J^{\mathcal{N}}_{AA'}\right)$ is called the map entropy $S^{\text{map}}(\mathcal{N})$ of channel $\mathcal{N}$ [51, 53]. Theorem 13 immediately yields an upper bound to the amount of randomness catalytically extractable from a randomness source channel $\mathcal{R} \in \mathfrak{C}(B)$, namely, $S_\alpha\left(J^{\Theta(\mathcal{N})}_{AA'}\right) - S_\alpha\left(J^{\mathcal{N}}_{AA'}\right) \leq S^{\diamond}_\alpha\left(J^{\mathcal{R}}_{BB'}\right)$, where $J^{\mathcal{R}}_{BB'}$ is interpreted to be an element of $\mathfrak{B}(B \otimes B')$ 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 $AA'BB'$, it is not evident if $S^{\diamond}_\alpha\left(J^{\mathcal{R}}_{BB'}\right)$ 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 delocalized catalysis of randomness, we can simply use the delocalized catalytic entropies to measure the maximally extractable randomness of arbitrary channel.

Definition 14. The catalytic Rényi entropy $S_\alpha^\diamond(\mathcal{R})$ of a quantum channel $\mathcal{R} \in \mathfrak{C}(B)$ is

$$S_\alpha^\diamond(\mathcal{R}) = S_\alpha^{\diamond\diamond}\left(J_{BB'}^{\mathcal{R}}\right). \tag{3.22}$$

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

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 $\mathcal{N} \in \tilde{\mathfrak{C}}(A)$,

$$\mathfrak{Tr}_B\,\mathcal{U}_3 \circ \mathcal{R}_B \circ \mathcal{U}_2 \circ \mathcal{N}_A \circ \mathcal{U}_1 = \Theta(\mathcal{N}), \tag{3.23}$$

and

$$\mathfrak{Tr}_A\,\mathcal{U}_3 \circ \mathcal{R}_B \circ \mathcal{U}_2 \circ \mathcal{N}_A \circ \mathcal{U}_1 = \mathfrak{Tr}[\mathcal{N}]\mathcal{R}, \tag{3.24}$$

with some superchannel $\Theta \in \mathfrak{SC}(A)$ and some unitary operations $\mathcal{U}_i \in \mathfrak{U}(AB)$ for $i = 1, 2, 3$. One can see that the unitary operation $\mathcal{U}_2$ in the middle hinders the transforming this process into a delocalized catalysis process. Although we can show that $\mathcal{U}_1$ must be a catalytic unitary operation by tracing out both sides of (3.24), still many other parts of this process is 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.

3.4 Partially depleted catalyst and semantic information

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 [54] 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 reference systems that are 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 delocalized 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 example is Szilard's engine. 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,

$$\rho_G = \frac{1}{2}\,|l\rangle\!\langle l|_G + \frac{1}{2}\,|r\rangle\!\langle r|_G\,. \tag{3.25}$$

A common precondition of Szilard's engine is the acquisition of information about the position of the molecule. Acquisition of information requires the existence of a information carrier that gets correlated with its reference, hence we spell it out as C, i.e.,

$$\frac{1}{2}\,|\text{“}l\text{”}\rangle\!\langle\text{“}l\text{”}|_C \otimes |l\rangle\!\langle l|_G + \frac{1}{2}\,|\text{“}r\text{”}\rangle\!\langle\text{“}r\text{”}|_C \otimes |r\rangle\!\langle r|_G\,. \tag{3.26}$$

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

$$\left(\frac{1}{2}\,|\text{“}l\text{”}\rangle\!\langle\text{“}l\text{”}|_C + \frac{1}{2}\,|\text{“}r\text{”}\rangle\!\langle\text{“}r\text{”}|_C\right) \otimes |r\rangle\!\langle r|_G\,. \tag{3.27}$$

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 the mere transfer of entropy from G to C, which is the key observation needed to solve Maxwell's demon problem.

Our way of modelling 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” [55].

As we have seen in Theorem 1, we could expect that there exist different characterizations of semantic information in each pictures, dynamical (Heisenberg) and static (Schrödinger). To construct the dynamical characterization, let us go back to the example of Szilard’s engine. 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 Condition (i) of Theorem 1, can be expressed concretely as follows.

Definition 15 (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 $\Theta \in \mathfrak{SC}(A)$,

$$\mathrm{Tr}_A[\mathcal{U}_\Theta(\sigma_{AB})] = \eta_B. \tag{3.28}$$

We remark that such η_B in (3.28) 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 2.

Definition 16 (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

$$\mathrm{Tr}_A[(\mathrm{id}_R \otimes \mathcal{U})(\tau_{RAB})] = (\mathrm{id}_R \otimes \mathrm{Ad}_V)(\tau_{RB}), \tag{3.29}$$

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 delocalized catalysis of randomness and claim the following.

Definition 17 (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 delocalized 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 delocalized catalysis of randomness. Hence, 'using only information of system B in correlated systems $ABC\cdots$' 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 18. Definitions (S:A), (S:B) and (S:C) are equivalent.

Proof is in 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 non-semantic (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. [20]. 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 not Q-PC 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 non-semantic quantum information when you are required not to disturb the information source, just as it is in the classical setting.

Corollary 19. If σ_{AB} is not Q-PC, then no non-product bipartite unitary operation can utilize only semantic information of B in σ_{AB}.

An important example of quantum state that is not Q-PC is pure states with full Schmidt rank. Hence, as pure states were not useful for delocalized 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 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 18, 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 20. 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

$$\mathrm{Tr}_A[\mathrm{Ad}_{U_{AB}} \circ \mathcal{L}_A(\sigma_{RAB})] = \mathrm{Tr}_A[\mathcal{L}_A(\sigma_{RAB})], \tag{3.30}$$

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

$$\mathrm{Tr}_A[\mathrm{Ad}_{U_{AB}}(\sigma_{RAB})] = \sigma_{RB}. \tag{3.31}$$

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 the Szilard engine example we discussed, ((3.25)-(3.27)), if we call the purifying system of (3.26) 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 form 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 21 easily follows from Definition (S:B). Proof is given in Appendix.

Corollary 21. 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 of σ_{RAB} such that $I(R:A) = I(R:AB)$, we have

$$\mathrm{Tr}_A[(\mathrm{id}_R \otimes \mathcal{U})(\sigma_{RAB})] = \sigma_{RB}. \tag{3.32}$$

As it was shortly discussed in Ref. [20], a randomness source correlated with a target system can absorb randomness as demonstrated in the example of Szilard engine 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 22. The least disordered state on A that can be made from σ_{AB} using B as an information source is $\sum_j \left(\sum_i p_i \lambda_j(\sigma_A^i)\right) |j\rangle\langle j|_A$ where $\sigma_{AB} = \sum_i p_i \sigma_{AB}^i$ is the essential decomposition of σ_{AB} on B.

Proof can be found in Appendix. Theorem 22 shows that quantum correlation is useless for 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 agree 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 a information source considered in delocalized 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 [54]. 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.

3.5 Superselection rules in delocalized 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 Section 3.1. For delocalized catalysis of randomness, we modify Definition 10 suitably.

Definition 23. For systems A and B in state ρ_{AB} with the essential decomposition $A = \bigoplus_{i\in\mathcal{I}_A\cup\mathcal{II}_A} A_i$, suppose that there is a superselection rule with the superselection sectors $A = \bigoplus_j A'_j$. We let $A^\circ_{(i,j)} := A_i \cap A'_j$ for $i \in \mathcal{II}_A$ and all j, and let $\{(i,j)\}_{i\in\mathcal{II}_A,j}$ be the new $\mathcal{II}_A$. Then, the finer decomposition $A = \bigoplus_{i\in\mathcal{I}_A} A_i \oplus \bigoplus_{k\in\mathcal{II}_A} A^\circ_k$ is the essential decomposition under the superselection.

Note that the superselection sectors cannot intersect nontrivially with type I subspaces 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 type II subspaces by partitioning a large uniform quantum states into the tensor product of smaller ones and forbidding nonclassical interaction between them. Since the catalytic entropies of quantum channels are defined through the delocalized catalytic entropies of their corresponding Choi matrices, this new definition equally affects the definition of the dynamical catalytic entropies.

Definition 23 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 delocalized 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

$$\rho_{E_AAB} = \sum_i |i\rangle\langle i|_{E_A} \otimes (\mathrm{Ad}_{Q_i} \otimes \mathrm{id}_B)(\rho_{AB}), \tag{3.33}$$

when it is treated as a delocalized randomness source. It can 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 delocalized catalysis of randomness nullifies the necessity of introducing C^*-algebra formalism to discuss about catalysts under superselection rules.

3.6 The no-stealth theorem

We consider the following dynamical generalization of the no-hiding theorem [56], or equivalently, the no-masking theorem[57]. 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 an arbitrary consider multipartite channel $\mathcal{N}$. See Appendix A.1.) By hiding, we mean that both of the marginal processes are constant regardless of the process $\mathcal{N}$, (See FIG. 5.) i.e.,

$$\mathfrak{Tr}_B[\Omega(\mathcal{N}_A \otimes \mathrm{id}_B)] = \mathfrak{Tr}[N]\mathcal{E}, \tag{3.34}$$

and

$$\mathfrak{Tr}_A[\Omega(\mathcal{N}_A \otimes \mathrm{id}_B)] = \mathfrak{Tr}[N]\mathcal{F}, \tag{3.35}$$

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 Section 3.3, the duality between delocalized 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

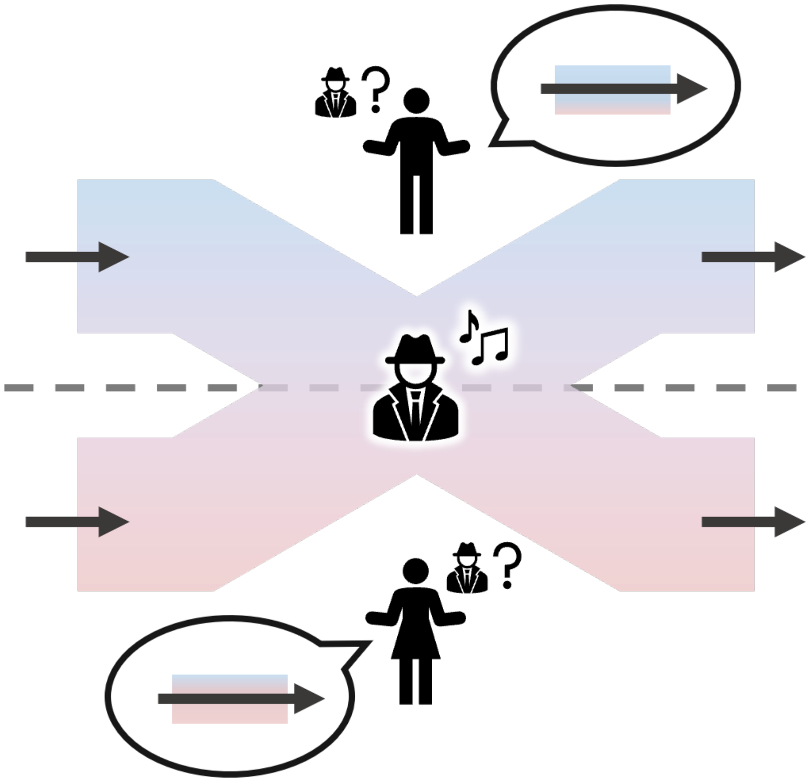


Figure 5: Suppose that input and output systems of a given quantum operation are reversibly distributed to two systems. Is it possible to hide the identity of the operation from the respective systems? In other words, is it possible to implement quantum operations stealthily? The no-stealth theorem says that it is impossible.

$U_1 \in \mathfrak{U}(A'B')$, we want

$$\mathrm{Tr}_{BB'}[\mathrm{Ad}_{U_0\otimes U_1}(\rho_{AA'} \otimes \phi^+_{BB'})] = \eta_{AA'}, \tag{3.36}$$

and

$$\mathrm{Tr}_{AA'}[\mathrm{Ad}_{U_0\otimes U_1}(\rho_{AA'} \otimes \phi^+_{BB'})] = \zeta_{BB'}, \tag{3.37}$$

for some quantum states $\eta_{AA'}$ and $\zeta_{BB'}$. This type of processes were called a randomness-utilizing processes in Ref.[19], 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 delocalized 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 Section 3.3, it is indeed possible to hide quantum processes when there is a randomness source with enough randomness.

3.7 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.

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:

$$\sigma_{AB}^{cc} = \sum_{i,j} p(i,j) \, |i\rangle\langle i| \otimes |j\rangle\langle j| \, , \tag{3.38}$$

with the superselection rules that forbid any superposition between basis elements (i.e. $\{|i\rangle\}$) for both systems. For σ_{AB}^{cc}, every Span$\{|i\rangle\}$ for both systems is type II subspace with dimension 1, therefore the delocalized 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 $\alpha \geq 0$.

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;

$$\mathcal{R}_c(\rho) = \sum_{i,j=1}^{|B|} p(j|i) \, \langle i| \, \rho \, |i\rangle \, |j\rangle\langle j| \, , \tag{3.39}$$

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

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 following form

$$\sigma_{AB}^{pc} = \sum_{i,j} p(i,j) \pi_{A_i} \otimes \pi_{B_j} . \tag{3.40}$$

Then, the corresponding DREO is unitarily similar to

$$\mathfrak{d}\left(\sigma_{AB}^{pc}\right) \approx \sum_{i,j} p(i,j)\pi_{A_i}^{\otimes 2} \otimes \pi_{B_j}^{\otimes 2}, \tag{3.41}$$

hence we have $S_\alpha^{\diamond\diamond}\left(\sigma_{AB}^{pc}\right) = S_\alpha^{\diamond}\left(\sigma_{AB}^{pc}\right)$ 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 is no impediment from the constraints imposed by the delocalized setting when there is no type I subspaces in the essential decompositions.

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 $B = \bigoplus_j B_j$,

$$\mathcal{R}_{mp}(\rho) = \sum_{i,j} p(j|i)\operatorname{Tr}\left[\Pi_i^A \rho\right] \pi_{B_j}, \tag{3.42}$$

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

$$J_{BA}^{\mathcal{R}_{mp}} = \sum_{i,j} p(j|i)a_i\pi_{B_j} \otimes \pi_{A_i}, \tag{3.43}$$

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

$$\mathcal{R}_{cp}(\rho) = \pi_B \operatorname{Tr}[\rho]. \tag{3.44}$$

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 n with respect to a complete set of orthonormal projectors $\{\Pi_i\}$ on B such that $\sum_i \Pi_i = \mathrm{id}_B$, i.e.,

$$\mathcal{R}_d(\rho) = \sum_i \Pi_i \rho \Pi_i. \tag{3.45}$$

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

$$J_{BB'}^{\mathcal{R}_d} = \sum_i b_i |\Gamma_i\rangle\langle\Gamma_i|, \tag{3.46}$$

where $b_i := |B_i|/|B|$, $|\Gamma_i\rangle = |B_i|^{-1/2}(B_i \otimes \mathbb{1}_{B_i'})\sum_j |jj\rangle_{BB'}$ with $B_i = \mathrm{supp}(\Pi_i)$. Here, every subspace B_i is either a type I or 1-dimensional type II subspace. Hence, $S_\alpha^\diamond(\mathcal{R}_d) = S_\alpha^{\diamond\diamond}\left(J_{BB'}^{\mathcal{R}_d}\right) = S_\alpha(\{b_i\}) \leq S_\alpha^\diamond\left(J_{BB'}^{\mathcal{R}_d}\right)$ for all $\alpha \geq 0$. It means that even if there are multiple b_i with the same value, i.e., even if $J_{BB'}^{\mathcal{R}_d}$ has degeneracy, the quantum correlation between two systems hinders the utilization of that correlation without leaving traces.

Chapter 4

Discussion

4.1 Physicality of information

In the seminal article ‘Information is Physical’ (1991) [58], 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 necessarily corresponds to a certain amount of energy, independent of how it is processed, in favor of the perspective from which information is a physical entity similar to matter which is also 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” [59]. 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/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 matter-like 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 [60], we will not introduce another term and call the property simply 'physicality'. This is the perspective we take in this dissertation 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 system 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 (3.1) and (3.2). 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

$$\sum_{j':j=f_2(i,j')} p_{j'} = p_j, \tag{4.1}$$

for all i and j. Similarly to catalytic quantum randomness, $f_2(i,\,\cdot\,)$ must preserve every non-degenerate 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. 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 down the outcome on a piece of paper, then 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 system 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 (3.2)), 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 delocalized catalysis of randomness and Theorem 7 says that totally quantum-quantum (Q-Q) bipartite states cannot yield randomness through delocalized catalysis. But, since every mixed state σ_B has a totally Q-Q 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 24. For any catalysis unitary $U \in \mathfrak{U}(A_0B_0)$ compatible with σ_{B_0}, there exists an extension $\sigma_{B_0B_1}$ of σ_{B_0} such that (U_0, U_1) is not compatible with $\sigma_{B_0B_1}$ for any $U_1 \in \mathfrak{U}(A_1B_1)$.

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.

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.

4.2 Concave resource theories

As it was briefly outlined in 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 $\mathfrak{R}$, $O_{\mathfrak{R}}$. 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 $0 \leq \lambda \leq 1$. 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

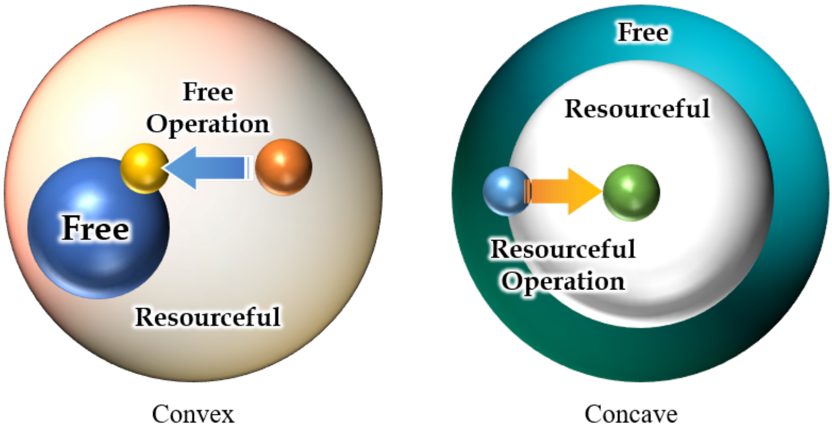


Figure 6: Comparison of convex and concave resource theories. In a convex resource theory, a statistical mixture of two free object is still free, and the action of free operation can only draw a resourceful object closer to the set of free objects. However, in a 'concave' resource theory, any statistical mixture of two resourceful object is resourceful, and there is no universal 'resource destroying operation'. However, there are resourceful operations that never makes a resourceful object free.

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 it. Albeit it is a concave resource theory, catalytic entropies are not concave functions. For example, slightly mixing the maximally mixed state with a non-degenerate 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 it 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. (See Section 2.)

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 entangle state shared by two parties, which is a very useful resource in entanglement theory, is completely useless in delocalized catalysis of randomness. In general, whenever there is quantum correlation in a bipartite quantum state, there exists a type I subspace in the essential decomposition, and it hinders catalytic extraction of randomness (See Section 3.7). It is because states with quantum correlation are sensitive to the action of local unital channels [50].

However, it does not mean that every quantumness is an obstacle in randomness extraction. For example, local coherence is helpful for maximizing extractable randomness of type II subspaces. This is the very reason why there are dimension-doubling effects in REO or DREO of randomness sources. However, again, it does not mean that coherence is 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 motivates the further study of quantum randomness to reveal its true nature and the extent of its power.

4.3 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 $n \geq 1$ 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 $S_\alpha(\rho_{n+1}) \leq S_\alpha^\diamond(\rho_n)$ by Theorem 4. On the other hand, if every system A_n is quantum, then the amount of randomness can increase *exponentially* over n. This is because $S_\alpha^\diamond(\rho_n) \geq S_\alpha(\rho_n)$ 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 back-flow 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 dissertation, we can see that the same phenomenon could also 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 $\Omega_n \in \mathfrak{SL}(A_{n+1}A_n)$ compatible with the catalyst $\mathcal{N}_n$ for every $n \geq 0$ 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 depolarising 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 type II subspaces that could yield quantum advantage of randomness extraction (See Section 3.7).

Chapter 5

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 dissertation, 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 delocalized and dynamical randomness sources. The delocalized 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 delocalized 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 [56], the no-stealth theorem, that forbids unitarily hiding quantum processes by distributing it to two delocalized parties.

Furthermore, we critically examined the slogan ‘information is physical’ by Landauer [58, 59], and concluded that when we focus more on utilization of information rather than on mere presence of information, classical information is rather nonphysical, or can be made nonphysical with proper optimization, independently of perspective. On the other hand, we showed that utilization of quantum information cannot be universally deemed to be nonphysical. It is essentially because quantum correlation, especially entanglement of pure quantum state, is strong enough to remember every action acted on a local system.

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

Models of information used in this dissertation are rather too simple to cover every aspect of information theory and one may find the definition of information given in this dissertation unsatisfactory or even disagree with it. Nonetheless, we reckon that the framework developed here successfully captures a certain aspect of information as a relatively nonphysical entity whose physical representation can affect the physical world without being affected and is presented in a concise modern quantum information language easily accessible by physicists. Indeed, the field of information theory is so vast that a single definition of information cannot explain every aspect of information as Shannon warned:

"It is hardly to be expected that a single concept of information would satisfactorily account for the numerous possible applications of this general field."

— Shannon (1953) [61].

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 fundamental nature of randomness in physics, 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.

Chapter A

Appendix : Technical results

A.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 (3.16). However, in contrast to that every subnormalized quantum state can be made into a normalized one by simply multiplying by some positive number, not every CP map can be made into a quantum channel (CPTP map) in the same way. Hence, one might suspect that requiring condition (3.16) 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,

$$\mathfrak{Tr}_A\left[(\mathfrak{id}_{E_0\to E_1} \otimes \Omega)(\mathcal{N} \otimes \mathcal{R})\right] = \mathfrak{Tr}_A[\mathcal{N}] \otimes \mathcal{R} \tag{A.1}$$

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 non-leakage through Ω can be re-interpreted as the requirement of no formation of correlation between the systems that did not interact directly through $\Omega \in \mathfrak{S}\mathfrak{C}(AB)$. 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 POVM $\{M_0, M_1\}$ with $M_0 + M_1 = \mathbb{1}_{E_0}$ on E_0 and

$$\mathcal{N}_i(\rho) = \mathrm{Tr}_{E_0}[(\mathbb{1}_A \otimes M_i)\mathrm{Ad}_U(\rho \otimes |0\rangle\langle 0|_{E_0})], \tag{A.2}$$

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

$$\mathcal{N}(\rho) := \mathcal{N}_0 \otimes |0\rangle\langle 0|_{E_1} + \mathcal{N}_1 \otimes |1\rangle\langle 1|_{E_1}. \tag{A.3}$$

With this expression, (A.1) requires that

$$\mathfrak{Tr}_A\left[(\mathfrak{id}_{E_0\to E_1} \otimes \Omega)(\mathcal{N} \otimes \mathcal{R})\right] = \sigma_{E_1} \otimes \mathcal{R}, \tag{A.4}$$

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

$$\langle i|_{E_1} \mathcal{N} \,|i\rangle_{E_1} = \mathcal{N}_i, \tag{A.5}$$

for $i = 0, 1$, therefore by contracting $|i\rangle\langle i|_{E_1}$ with the both sides of (A.4), using $\langle i|_{E_1} \sigma_{E_1} |i\rangle_{E_1} = \mathfrak{Tr}[\mathcal{N}_i]$, we get

$$\mathfrak{Tr}_A \Omega(\mathcal{N}_i \otimes \mathcal{R}) = \mathfrak{Tr}[\mathcal{N}_i]\mathcal{R}. \tag{A.6}$$

Since $\mathcal{N}_0$ was chosen arbitrarily in $\tilde{\mathfrak{C}}(A)$, we can see that (A.1) implies condition (3.16).

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 (3.16) 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 (A.1) follows. Therefore, (3.16) and (A.1) are equivalent.

A.2 Proof of Proposition 5

증명 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 $|\Sigma\rangle_{XX'}$ ($\mathrm{Tr}_{X'} |\Sigma\rangle\langle\Sigma|_{XX'} = \sigma_X$) [20]. 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. $\square$

A.3 Discssion on Mølmer's conjecture

Mølmer's conjecture [49] insists that the quantum state of laser light should not be represented by a pure coherent state

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{A.7}$$

but the mixed state

$$\frac{1}{2\pi} \int_0^{2\pi} \left| |\alpha| e^{i\theta} \right\rangle \left\langle |\alpha| e^{i\theta} \right| d\theta = e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} |n\rangle \langle n| \,, \tag{A.8}$$

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* [62, 63]. 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

$$\sum_{\phi} p(\phi)\, |\phi\rangle\langle\phi|_A \otimes |``\phi"\rangle\langle``\phi"|_C\,, \tag{A.9}$$

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

$$\sum_{\phi} p(\phi)\, |\phi\rangle\langle\phi|_A^{\otimes n} \otimes |``\phi"\rangle\langle``\phi"|_C\,. \tag{A.10}$$

Or, systems AC can even be entangled;

$$\sum_{\phi} \sqrt{p(\phi)}\, |\phi\rangle_A \otimes |``\phi"\rangle_C\,. \tag{A.11}$$

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.

A.4 Proof of Theorem 7

증명 The assumption that no randomness can be catalytically extracted from $\sigma_{B_0B_1}$ means that any catalytic unitary operators compatible with $\sigma_{B_0B_1}$ is a product unitary operator. Therefore, any action applied to $\sigma_{B_0B_1}$ is also of the form of product unitary operations, i.e. $\sigma_{B_0B_1} \mapsto \text{Ad}_{V_0\otimes W_1}(\sigma_{B_0B_1})$ with some $V_0 \in \mathfrak{U}(B_0)$ and $W_1 \in \mathfrak{U}(B_1)$. As a special case, assume that $U_0 = \mathbb{1}_{A_0B_0}$. It implies that $V_0 = \mathbb{1}_{B_0}$. Note that, in this case, W_1 should be also proportional to the identity operator. It is because, if $W_1 \not\propto \mathbb{1}_{B_1}$, then the random unitary operation given as $\frac{1}{2}(\text{id}_{B_1} + \text{Ad}_{W_1})$ on B_1 that is not a unitary operation also fixes $\sigma_{B_0B_1}$. This contradicts the previous result that any action on $\sigma_{B_0B_1}$ should be a unitary operation. It is equivalent to saying that whatever catalytic map is applied to system B_1, if it fixes $\sigma_{B_0B_1}$, then it should the identity operation. This property is called sensitivity to catalytic maps according to the definition given in Ref. [50]. 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.[50], it follows that it is equivalent to that $\sigma_{B_0B_1}$ is not a Q-PC state. The same argument can be applied when the roles of B_0 and B_1 are switched, thus $\sigma_{B_0B_1}$ is neither a PC-Q state.

Conversely, assume that $\sigma_{B_0B_1}$ is totally Q-Q. Let $U_0 \in \mathfrak{U}(A_0B_0)$ and $U_1 \in \mathfrak{U}(A_1B_1)$ be arbitrary catalytic unitary operators and $\mathcal{N}_0 := \mathfrak{Tr}_{A_0} \circ \text{Ad}_{U_0} \in \mathfrak{UC}(B_0)$ and $\mathcal{N}_1 := \mathfrak{Tr}_{A_1} \circ \text{Ad}_{U_1} \in \mathfrak{UC}(B_1)$ be induced catalytic maps on B_0 and B_1 respectively. For $\sigma_{B_0B_1}$ to be compatible with U_0 and U_1, $\mathcal{N}_0 \otimes \mathcal{N}_1$ must fix $\sigma_{B_0B_1}$. However, since catalytic maps can never decrease the von Neumann entropy, it means that both $\mathcal{N}_0$ and $\mathcal{N}_1$

fix the von Neumann entropy of $\sigma_{B_0B_1}$. By Theorem 2.1 of Ref.[51], it is equivalent to that both $\mathcal{N}_0^\dagger \circ \mathcal{N}_0$ and $\mathcal{N}_1^\dagger \circ \mathcal{N}_1$ fix $\sigma_{B_0B_1}$. Since $\sigma_{B_0B_1}$ is totally Q-Q, it is sensitive to unital channels on both sides [50], hence it follows that $\mathcal{N}_0^\dagger \circ \mathcal{N}_0 = \mathrm{id}_{B_0}$ and $\mathcal{N}_1^\dagger \circ \mathcal{N}_1 = \mathrm{id}_{B_1}$. It is equivalent to that both $\mathcal{N}_0$ and $\mathcal{N}_1$ are unitary operations, therefore U_0 and U_1 are product unitary operators. It follows that no randomness can be extracted from $\sigma_{B_0B_1}$. $\square$

A.5 Uniqueness of essential decomposition

Recall the three criteria, (i), (ii) and (iii) of Definition 8. Because of (i) and (iii), any two essential decompositions of the same state should commute with each other. (By saying decompositions commute with each other, we mean that projectors corresponding to their subspaces are mutually commutative.) If their type I subspaces do not match, then, since ρ_{AB} is still generalized block-diagonal with the intersections of both decompositions, some of type I component of ρ_{AB} permits further decomposition on A, hence become a PC-Q state, which violates (ii).

If there is a mismatch of type II subspaces between two essential decompositions (However, their spans should match because they are the perpendicular complement of the span of the same type I subspaces because of the previous paragraph), it leads to a violation of (iii) since there always is a projector that commutes with one decomposition that does not with the other. Say, A_1 is a type II subspace of the first decomposition that intersects with two type II subspaces of the second decomposition, A_1' and A_2'. Pick arbitrary $|\phi_1\rangle \in A_1 \cap A_1'$ and $|\phi_2\rangle \in A_1 \cap A_2'$, and let P be the rank-1 projector onto $|\phi'\rangle := 2^{-1/2}(|\phi_1\rangle + |\phi_2\rangle)$. Since $|\phi'\rangle$ lies in A_1 (on which ρ_{AB} is proportional to the identity operator on A so that it commutes with every operator on A_1), P commutes with ρ_{AB} but it does not commute with the projectors onto A'_1 or A'_2. Thus, the essential decomposition is unique.

A.6 Other results on essential decomposition

The following two Propositions are not directly used in the rest of Section, but give insight into the structure of bipartite fixed points of quantum channels.

Proposition 25. If the product of unital maps $\mathcal{N} \otimes \mathcal{M}$ fixes a quantum state ρ_{AB}, then they also fix every projector onto each of its eigenspaces, Π_i. Also, $\mathcal{N}$ fixes $\operatorname{Tr}_B \Pi_i$ and $\mathcal{M}$ fixes $\operatorname{Tr}_A \Pi_i$.

Proposition 26. Assume that Π is a projector on AB such that $\operatorname{Tr}_B \Pi \propto \mathbb{1}_A$ and $\operatorname{Tr}_A \Pi \propto \mathbb{1}_B$, and $\Pi = \sum_i \Pi_i$ where Π_i is a projector supported on $\mathfrak{B}(AB_i)$ with $B = \bigoplus_i B_i$. If $\mathcal{N} \otimes \mathrm{id}_B$ fixes Π, then it also fixes Π_i.

증명 By applying $M = \sum_i \lambda_i \Pi_{\text{supp}(B_i)}$ on B, with injective $i \mapsto \lambda_i$, we can transform Π into $\sum_i \lambda_i \Pi_i$, so that they each Π_i is a projector onto eigenspaces corresponding to a unique eigenvalue, and $\mathcal{N}$ still preserves this operator. Thus the unital map $\mathcal{N} \otimes \mathrm{id}_B$ should preserve it. Consequently, $\mathcal{N}(\operatorname{Tr}_B \Pi_i) = \operatorname{Tr}_B \Pi_i$. $\square$

Proposition 27. A quantum state ρ_{AB} is PC-Q with respect to the essential decomposition $A = \bigoplus_i A_i$ (let $\Pi_i := \mathbb{1}_{A_i}$) with corresponding type index sets $\mathcal{I}_A$ and $\mathcal{II}_A$ if and only if for any $M \in \mathfrak{B}(A)$, $[M \otimes \mathbb{1}_B, \rho_{AB}] = 0$

is equivalent to $M = \left(\bigoplus_{i\in\mathcal{I}_A} \alpha_i \Pi_i\right) \oplus \left(\bigoplus_{i\in\mathcal{II}_A} M_i\right)$ for some complex numbers α_i for all $i \in \mathcal{I}_A$ and some $M_i \in \mathfrak{B}(A_i)$ for all $i \in \mathcal{II}_A$ (we will say that "M is in the standard form").

증명 Assume that ρ_{AB} is a PC-Q state given as in the statement of Proposition. Let $M \in \mathfrak{H}(A)$ commute with ρ_{AB} but be not of the form $M = \left(\bigoplus_{i\in\mathcal{I}_A} \Pi_i\right) \oplus \left(\bigoplus_{i\in\mathcal{II}_A} M_i\right)$. It is impposible as it should be one of the following cases.

(i) M is not block-diagonal with respect to the decomposition $A = \bigoplus_i A_i$: M has the spectral decomposition $M = \sum_i m_i P_i$ (m_i is unique for each i), but some P_i does not commute with some of $\{\Pi_i\}$. Since ρ_{AB} commutes with $M \otimes \mathbb{1}_B$, ρ_{AB} is also generalized block-diagonal with respect to the eigenspaces of M, i.e., $[P_i \otimes \mathbb{1}_B, \rho_{AB}] = 0$ for all i. It violates (iii) of Definition 8.

(ii) M is block-diagonal with respect to the decomposition $A = \bigoplus_i A_i$, but for some $i \in \mathcal{I}_A$, $\Pi_i M \Pi_i \not\propto \Pi_i$: We assume $[\Pi_i \otimes \mathbb{1}_B, \rho_{AB}] = 0$ for all i (See (i) above). Let $M_i := \Pi_i M \Pi_i$ and $\rho_i := (\Pi_i \otimes \mathbb{1}_B)\rho_{AB}(\Pi_i \otimes \mathbb{1}_B)$. We have $[M_i \otimes \mathbb{1}_B, \rho_i] = 0$, hence ρ_i is PC-Q state with respect to the nontrivial eigenspaces of M_i. It violates (ii) of Definition 8.

For general $M \in \mathfrak{B}(A)$, one can consider its real and imaginary parts $M_R := (M + M^\dagger)/2$ and $M_I := -i(M - M^\dagger)/2$, which are Hermitian operators commuting with ρ_{AB} themselves. The same argument applies to each of them, and the desired result follows for M: $A = \bigoplus_i A_i$ cannot be the essential decomposition of A for ρ_{AB}.

Likewise, let M be given as $M = \left(\bigoplus_{i\in\mathcal{I}_A} \Pi_i\right) \oplus \left(\bigoplus_{i\in\mathcal{II}_A} M_i\right)$ but assume that $[M \otimes \mathbb{1}_B, \rho_{AB}] \neq 0$. However, it is impossible if $A = \bigoplus A_i$ is the essential decomposition for ρ_{AB} since type II components of ρ_{AB} only can be in the form of $\pi_{A_i} \otimes \sigma_B$ for some $\sigma \in \mathfrak{S}(B)$, so that $M \otimes \mathbb{1}_B$ of the standard form must commute with ρ_{AB}. It follows that $A = \bigoplus_i A_i$ cannot be the essential decomposition of A for ρ_{AB}.

Conversely, $A = \left(\bigoplus_{i \in \mathcal{I}_A} A_i\right) \oplus \left(\bigoplus_{i \in \mathcal{II}_A} A_i\right)$ be an arbitrary nontrivial decomposition of A with $\Pi_i := \mathbb{1}_{A_i}$. Assume that for any $M \in \mathfrak{B}(A)$, $[M \otimes \mathbb{1}_B, \rho_{AB}] = 0$ is equivalent to M being in the standard form, i.e. $M = \left(\bigoplus_{i \in \mathcal{I}_A} \alpha_i \Pi_i\right) \oplus \left(\bigoplus_{i \in \mathcal{II}_A} M_i\right)$ for some complex numbers α_i for all $i \in \mathcal{I}_A$ and some $M_i \in \mathfrak{B}(A_i)$ for all $i \in \mathcal{II}_A$. We check if the decomposition $A = \bigoplus_i A_i$ satisfies the three criteria of Definition 8.

(i) Each Π_i is obviously in the standard form, thus $[\Pi_i \otimes \mathbb{1}_B, \rho_{AB}] = 0$. The decomposition is assumed to be nontrivial, thus no Π_i is equal to $\mathbb{1}_A$.

(ii) For some $i \in \mathcal{I}_A$, if $(\Pi_i \otimes \mathbb{1}_B)\rho_{AB}(\Pi_i \otimes \mathbb{1}_B)$ is PC-Q, then, it has its own essential decomposition of $A_i = \bigoplus_j A_i^j$, which can give a finer decomposition of A and makes $\mathbb{1}_{A_i^j} \otimes \mathbb{1}_B$ commute with ρ_{AB} even though $\mathbb{1}_{A_i^j}$ is not of the standard form. For some $i \in \mathcal{II}_A$, if $(\Pi_i \otimes \mathbb{1}_B)\rho_{AB}(\Pi_i \otimes \mathbb{1}_B) \not\propto \mathbb{1}_{A_i} \otimes \sigma_B$ for some $\sigma \in \mathfrak{S}(B)$, there exists some $W \in \mathfrak{B}(A_i)$ such that $[W_A \otimes \mathbb{1}_B, \rho AB] \neq 0$ even though it is of the standard form.

(iii) Any projector P on A that does not commute with some Π_i is not of the standard form, thus $[P \otimes \mathbb{1}_B, \rho_{AB}] \neq 0$.

$\square$

Here, we provide a proof of Theorem 9.

Theorem 9. A unital channel $\mathcal{N} \in \mathfrak{UC}(A)$ fixes a quantum state ρ_{AB}

that is PC-Q with respect to the essential decomposition $A = \bigoplus_i A_i$ (let $\Pi_i := \mathbb{1}_{A_i}$) with corresponding type index sets $\mathcal{I}_A$ and $\mathcal{II}_A$ if and only if $\mathcal{N}$ preserves every subspace A_i and acts trivially on A_i when $i \in \mathcal{I}_A$.

증명 If $\mathcal{N}$ preserves every subspace A_i and acts trivially on $\mathfrak{B}(A_i)$ when $i \in \mathcal{I}_A$, then $\mathcal{N} \circ \mathrm{Ad}_{\Pi_i} = \mathrm{Ad}_{\Pi_i}$ for all i, so that $\mathcal{N} \circ (\sum_i \mathrm{Ad}_{\Pi_i}) = \sum_i \mathcal{N} \circ \mathrm{Ad}_{\Pi_i} = \sum_i \mathrm{Ad}_{\Pi_i}$. Therefore, ρ_{AB}, which is fixed by $\sum_i \mathrm{Ad}_{\Pi_i} \otimes \mathrm{id}_B$, is also fixed by $\mathcal{N}$.

Conversely, assume that a unital channel $\mathcal{N}$ fixes a PC-Q quantum state ρ_{AB} with the structure given in the assumption. Hence, for every Kraus operator K_j of $\mathcal{N}$, i.e., $\mathcal{C} = \sum_i \mathrm{Ad}_{K_j}$, we have $[K_j \otimes \mathbb{1}_B, \rho_{AB}] = 0$ [64, 19, 20]. By Proposition 27, it follows that $K_j = \left(\bigoplus_{i\in\mathcal{I}_A} \alpha_i^{(j)} \Pi_i\right) \oplus \left(\bigoplus_{i\in\mathcal{II}_A} K_i^{(j)}\right)$ for some complex numbers α_i for all $i \in \mathcal{I}_A$ and some $K_i^{(j)} \in \mathfrak{B}(A_i)$ for all $i \in \mathcal{II}_A$. By the trace preserving condition, $\sum_j K_j^\dagger K_j = \mathbb{1}_A$, we have $\sum_j |\alpha_i^{(j)}|^2 = 1$. From the forms of K_j, we can see that $\mathcal{C} = \left(\bigoplus_{i\in\mathcal{I}_A} \mathrm{id}_{A_i}\right) \oplus \left(\bigoplus_{i\in\mathcal{II}_A} \mathcal{C}_i\right)$, with $\mathcal{C}_i = \sum_j \mathrm{Ad}_{K_j^{(i)}}$ for every $i \in \mathcal{II}_A$. It proves the desired result. $\square$

Lemma 28. For a unital channel $\mathcal{N} \in \mathfrak{UC}(A)$, if $\mathcal{N}^\dagger \circ \mathcal{N}(\Pi_i) = \Pi_i$ for some partition of unity (i.e. $\{\Pi_i\}$ are projectors and $\sum_i \Pi_i = \mathbb{1}_A$), then there exists $U \in \mathfrak{U}(A)$ and $\mathcal{M} \in \mathfrak{UC}(A)$ such that $\mathcal{N} = \mathrm{Ad}_U \circ \mathcal{M}$ and $\mathcal{M}(\Pi_i) = \Pi_i$ for all i.

증명 As $\mathcal{N}$ is unital, $\mathcal{N}(\Pi_i) \prec \Pi_i$, but $\mathcal{N}^\dagger \circ \mathcal{N}(\Pi_i) = \Pi_i$, i.e, $S(\pi_i) = S(\mathcal{N}(\pi_i))$ [51] where $\pi_i = |\Pi_i|^{-1}\Pi_i$. Because the von Neumann entropy is strictly Schur concave [65], it means that there exists $U_i \in \mathfrak{U}(A)$ such that $\mathcal{N}(\Pi_i) = \mathrm{Ad}_{U_i}(\Pi_i)$. Hence $\mathbb{1}_A = \mathcal{N}(\mathbb{1}_A) = \sum_i \mathcal{N}(\Pi_i) = \sum_i \mathrm{Ad}_{U_i}(\Pi_i)$.

From this we can deduce that $\sum_{i\neq j}\Pi_i = \sum_{i\neq j}\mathrm{Ad}_{U_j^\dagger U_i}(\Pi_i)$. Thus,

$$\mathrm{Tr}\Big[\Pi_j \mathrm{Ad}_{U_j^\dagger U_i}(\Pi_i)\Big] = \mathrm{Tr}\big[\mathrm{Ad}_{U_j}(\Pi_j)\mathrm{Ad}_{U_i}(\Pi_i)\big] = 0$$

for any i and j. Hence $\{U_i\Pi_i U_i^\dagger\}$ is another partition of unity with the same ranks, so there exists some unitary operator $V \in \mathfrak{U}(A)$ such that $\mathrm{Ad}_{U_i}(\Pi_i) = \mathrm{Ad}_V(\Pi_i)$. It follows that $\mathcal{M} := \mathrm{Ad}_{V^\dagger}\circ\mathcal{N}$ is a unital channel on A that preserves every Π_i and $\mathcal{N} = \mathrm{Ad}_V\circ\mathcal{M}$. □

Corollary 29. A unital channel $\mathcal{N}\in\mathfrak{UC}(A)$ does not increase the entropy of a quantum state ρ_{AB} that is PC-Q with respect to the essential decomposition $A = \bigoplus_i A_i$ ($\Pi_i := \mathbb{1}_{A_i}$) with corresponding type index sets $\mathcal{I}_A$ and $\mathcal{II}_A$ if and only if $\mathcal{N}$ can be decomposed into $\mathcal{N} = \mathrm{Ad}_V\circ\mathcal{N}'$ with some unitary operator $V\in\mathfrak{U}(A)$ and a unital channel $\mathcal{N}'$ that preserves every subspace A_i and acts trivially on A_i when $i\in\mathcal{I}_A$.

증명 By Theorem 9 and Lemma 28, $\mathcal{N}$ can be decomposed into $\mathcal{N} = \mathrm{Ad}_{V'}\circ\mathcal{M}$ with some $V'\in\mathfrak{U}(A)$ and a unital channel $\mathcal{M}\in\mathfrak{UC}(A)$ that preserves every subspace A_i. Let $p_i := \mathrm{Tr}[\Pi_i\rho_A]$ and $\rho^i_{AB} := p_i^{-1}(\mathrm{Ad}_{\Pi_i}\otimes \mathrm{id}_B)(\rho_{AB})$. Then, there exists $\mathcal{M}_i\in\mathfrak{UC}(A_i)$ such that $(\mathcal{M}\otimes\mathrm{id}_B)(\rho^i_{AB}) = (\mathcal{M}_i\otimes\mathrm{id}_B)(\rho^i_{AB})$ because each ρ^i_{AB} is supported on $A_i\otimes B$ for every i. For N to preserve the von Nuemann entropy of ρ_{AB}, it is required for every $\mathcal{M}_i$ to preserve the von Neumann entropy of ρ^i_{AB}. For type I indices, i.e., when $i\in\mathcal{I}_A$, it means that $\mathcal{M}_i^\dagger\circ\mathcal{M}_i$ fixes ρ^i_{AB} [51]. However, since ρ^i_{AB} is not PC-Q as a state of A_iB, it follows that $\mathcal{M}_i$ is a unitary operation on A_i (See the proof of Theorem 7), i.e., $\mathcal{M}_i = \mathrm{Ad}_{W_i}$ for some $W_i\in\mathfrak{U}(A_i)$. If we let

$V := V'R$ where $R := \left(\bigoplus_{i\in\mathcal{I}_A} W_i \oplus \bigoplus_{i\in\mathcal{II}_A} \Pi_i\right)$ and $\mathcal{N}' := \mathrm{Ad}_{R^\dagger} \circ \mathcal{M}$, then $\mathcal{N} = \mathrm{Ad}_V \circ \mathcal{N}'$ is the desired decomposition of $\mathcal{N}$. $\square$

Corollary 30. Let a delocalized catalysis unitary operator pair (U_0, U_1) be compatible with a delocalized randomness source $\sigma_{B_0B_1}$ with the DCD

$$\sigma_{B_0B_1} = \bigoplus_{ij} (\Pi_i^{B_0} \otimes \Pi_j^{B_1})\sigma_{B_0B_1}(\Pi_i^{B_0} \otimes \Pi_j^{B_1}), \tag{A.12}$$

and the essential decompositions $B_0 = \bigoplus_i B_{0i}$ and $B_1 = \bigoplus_i B_{1i}$. It follows that there exist $W_i \in \mathfrak{U}(B_i)$ for $i = 0, 1$ ($\Pi_k^{B_i} := \mathbb{1}_{B_{ik}}$) such that $U_i = (\mathbb{1}_{A_i} \otimes W_i)\left(\bigoplus_k U_{ik}\right)$ where $U_{ik} \in \mathfrak{U}(A_iB_{ik})$ is a catalysis unitary operator compatible with $(\Pi_k^{B_0} \otimes \mathbb{1}_B)\sigma_{B_0B_1}(\Pi_k^{B_0} \otimes \mathbb{1}_B)$ for $i = 0$ and $(\mathbb{1}_A \otimes \Pi_k^{B_1})\sigma_{B_0B_1}(\mathbb{1}_A \otimes \Pi_k^{B_1})$ for $i = 1$.

증명 Consider the maximally mixed initial state $\pi_{A_0} \otimes \pi_{A_1}$ for the catalysis and let $\mathcal{N}_i \in \mathfrak{UC}(B_i)$ given as $\mathcal{N}_i := \mathfrak{Tr}_{A_i} \circ \mathrm{Ad}_{U_i}$ be the induced catalytic map on B_i acting on the delocalized catalyst $\sigma_{B_0B_1}$ for $i = 0, 1$. Since (U_0, U_1) and $\sigma_{B_0B_1}$ are compatible with each other, we have $(\mathcal{N}_0 \otimes \mathcal{N}_1)(\sigma_{B_0B_1}) = \sigma_{B_0B_1}$. It follows that both of $\mathcal{N}_i$ do not increase the entropy of $\sigma_{B_0B_1}$. By Corollary 29, the Kraus operators $\{R_k^i\}$ of $\mathcal{N}_i$ all have the form $R_k^i = W_i L_K^i$ where $W_i \in \mathfrak{U}(B_i)$ is a unitary operator and L_k^i is the Kraus operator of another unital map in the standard form. However, we recall that $K_{nm}^i := |A_i|^{-1/2}(\langle n|_{A_i} \otimes \mathbb{1}_{B_i})U_0(|m\rangle_{A_i} \otimes \mathbb{1}_{B_i})$ are the Kraus operators of $\mathcal{N}_i$ for $i = 0, 1$. Let the standard form expression of K_{nm}^i given as follows:

$$|A_i|^{1/2}K^i_{nm} = \left(\bigoplus_{k\in\mathcal{I}_{B_i}} \alpha_k^{(i,n,m)}\Pi_k^{B_i}\right) \oplus \left(\bigoplus_{k\in\mathcal{II}_{B_i}} K_k^{(i,n,m)}\right). \tag{A.13}$$

Now, we let

$$U_{ik} := \sum_{nm} |n\rangle\langle m|_{A_i} \otimes \left(\alpha_k^{(i,n,m)}\Pi_k^{B_i}\right)$$

for $k \in \mathcal{I}_{B_i}$ and $U_{ik} := \sum_{nm} |n\rangle\langle m|_{A_i} \otimes K_k^{(i,n,m)}$ for $k \in \mathcal{II}_{B_i}$ and the desired result follows. □

A.7 Proof of Theorem 12

증명 For the given randomness source $\sigma_{B_0B_1}$, we again let

$$p_{ij} := \mathrm{Tr}\left[(\Pi_i^{B_0} \otimes \Pi_j^{B_1})\sigma_{B_0B_1}\right]$$

and $\sigma^{ij} := p_{ij}^{-1}(\mathrm{Ad}_{\Pi_i^{B_0}} \otimes \mathrm{Ad}_{\Pi_j^{B_1}})(\sigma_{B_0B_1})$. We first show that it is achievable. To match the notations with (3.9) and (3.10), we set $\sigma_{B_0B_1}$ as our delocalized randomness source. (Consider that $A \to B_0$ and $B \to B_1$ in Definition 8 and 11.) We let $B_0 = \bigoplus_i B_{0i}$ and $B_1 = \bigoplus_i B_{1i}$ be their respective essential decompositions. For the sake of simplicity, assume that $\mathcal{I}_{B_i} = \{1, 2, \cdots, |\mathcal{I}_{B_i}|\}$ and $\mathcal{II}_{B_i} = \{|\mathcal{I}_{B_i}| + 1, \cdots, |\mathcal{I}_{B_i}| + |\mathcal{II}_{B_i}|\}$ for $i = 0, 1$. Also, let the dimension of A_i be $|\mathcal{I}_{B_i}| + \sum_{j\in\mathcal{II}_{B_i}} |B_{ij}|^2$ for

$i=0,1$. We use catalysis unitary operators

$$U_0=\sum_{i\in\mathcal{I}_{B_0}} Z_0^i\otimes\Pi_i^{B_0}+\sum_{i\in\mathcal{II}_{B_0}}\sum_{j,k=0}^{|B_{0i}|-1} Z_0^{S_i^0+j|B_{0i}|+k}\otimes E_{jk}^{(0i)}, \tag{A.14}$$

and

$$U_1=\sum_{i\in\mathcal{I}_{B_1}} Z_1^i\otimes\Pi_i^{B_1}+\sum_{i\in\mathcal{II}_{B_1}}\sum_{j,k=0}^{|B_{1i}|-1} Z_1^{S_i^1+j|B_{1i}|+k}\otimes E_{jk}^{(1i)}. \tag{A.15}$$

Here, $E_{jk}^{(im)}:=\omega_{im}^{jk}\left|m_j^i\middle\rangle\middle\langle m_k^i\right|$, where ω_{im} is the $|B_{im}|$-th root of the unity, and $\{\left|m_j^i\right\rangle\}$ is an orthonormal basis of B_{im}. are an arbitrary orthonormal unitary operator on B_{0i} and B_{1i}, respectively. Also, $Z_i=\sum_k |k\oplus 1(\text{mod }|A_i|)\rangle\langle k|$ is the generalized Pauli-Z operator on A_i, and $S_k^i:=|\mathcal{I}_{B_i}|+\sum_{l=0}^{k-1}|B_{il}|^2$ assuming $|B_{i0}|=0$ for $i=0,1$. Now, we suppose that system A_0A_1 is prepared in a maximally entangled state $|\phi^+\rangle_{A_0A_0'}|\phi^+\rangle_{A_1A_1'}$ with auxiliary systems A_0' and A_1'. After the catalysis, the final state of $A_0A_1A_0'A_1'$ is

$$\begin{aligned}&\sum_{\substack{i\in\mathcal{I}_{B_0},\\ j\in\mathcal{I}_{B_1}}} p_{ij}\phi^i_{A_0A_0'}\otimes\phi^j_{A_1A_1'}+\sum_{\substack{i\in\mathcal{I}_{B_0},\\ j\in\mathcal{II}_{B_1}}} p_{ij}\phi^i_{A_0A_0'}\otimes\Xi^1_j\\ &+\sum_{\substack{i\in\mathcal{II}_{B_0},\\ j\in\mathcal{I}_{B_1}}} p_{ij}\Xi^0_i\otimes\phi^j_{A_1A_1'}+\sum_{\substack{i\in\mathcal{II}_{B_0},\\ j\in\mathcal{II}_{B_1}}} p_{ij}\Xi^0_i\otimes\Xi^1_j.\end{aligned} \tag{A.16}$$

Here, $\phi^m_{A_iA_i'}:=\mathrm{Ad}_{Z_i^m}\otimes\mathrm{id}_{A_i'}(\phi^+_{A_iA_i'})$ are mutually orthogonal Bell states for $i=0,1$. Also, Ξ_i^0 and Ξ_j^1 are given as

$$\Xi_i^0:=\frac{1}{|B_{0i}|^2}\sum_{k=0}^{|B_{0i}|^2-1}\phi^{S_i^0+k}_{A_0A_0'}, \tag{A.17}$$

and

$$\Xi_j^1 := \frac{1}{|B_{1j}|^2} \sum_{l=0}^{|B_{1j}|^2-1} \phi_{A_1 A_1'}^{S_j^1+l}, \tag{A.18}$$

for all $i \in \mathcal{II}_{B_0}$ and $j \in \mathcal{II}_{B_1}$. Note that Ξ_i^0 and Ξ_j^1 are unitarily similar with $\pi_{\mathbb{C}^{|B_{0i}|^2}}$ and $\pi_{\mathbb{C}^{|B_{1j}|^2}}$, respectively. Since every term in (A.16) is mutually orthogonal to each other, it is unitarily similar to $\bigoplus_{i,j} p_{ij} \tau_i \otimes \kappa_j$ in (3.13), after the changes of labels.

Conversely, by Corollary 30, every component in the DCD of a delocalized catalyst is compatible up to 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_0 and U_1 by using $\sigma_{B_0 B_1}$ as the catalyst. In other words, $\mathcal{C}(\rho) := \mathrm{Tr}_{B_0 B_1}[(\mathrm{Ad}_{U_0} \otimes \mathrm{Ad}_{U_1})(\rho_{A_0 A_1} \otimes \sigma_{B_0 B_1})]$. Now we let $\mathcal{C}_{ij}$ be given as $\mathcal{C}_{ij}(\rho) := \mathrm{Tr}_{B_0 B_1}[(\mathrm{Ad}_{U_0} \otimes \mathrm{Ad}_{U_1})(\rho_{A_0 A_1} \otimes \sigma_{B_0 B_1}^{ij})]$, which is a catalytic map by itself, then we have $\mathcal{C} = \sum_{ij} p_{ij} \mathcal{C}_{ij}$. For arbitrary pure initial state $\rho_{A_0 A_1}$ (recall that the maximum entropy production is made with a pure state input), we have the following.

$$\begin{aligned} \mathcal{C}(\rho) = \sum_{ij} p_{ij} \mathcal{C}_{ij}(\rho) &\succ \bigoplus_{ij} p_{ij} \mathcal{C}_{ij}(\rho) \\ &\succ \bigoplus_{ij} p_{ij} \tau_i \otimes \kappa_j. \end{aligned} \tag{A.19}$$

The first majorization relation follows from the fact that a convex sum of quantum states always majorizes the direct sum of the same summands [66]. The last majorization relation follows because whenever $k \in \mathcal{I}_{B_i}$, U_i can only act unitarily on B_{ik}, hence no randomness can be extracted on that side, and when $l \in \mathcal{II}_{B_i}$, then the catalyst is in a product state in that component, thus it simply functions as a single party randomness source. It means that τ_l (or κ_l) functions as the REO. We also used the fact that a direct sum of quantum states majorizes another when its individual summand majorizes that of the other. Since every Rényi entropy of order $\alpha \geq 0$ is Schur-concave, the desired result follows. $\square$

A.8 Proof of Theorem 18

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

Lemma 31. If $U \in \mathfrak{U}(AB)$ and $\sigma_{AB} \in \mathfrak{S}(AB)$ are given as in Definition 15, then U is a catalysis unitary operator compatible with σ_B as a catalyst up to local unitary.

증명 As any superchannel can be decomposed into pre- and post-processing channels, (3.28) is equivalent to

$$\mathrm{Tr}_A[\mathcal{U} \circ (\mathcal{N}_A \otimes \mathrm{id}_B)(\sigma_{AB})] = \eta_B, \tag{A.20}$$

for any channel $\mathcal{N} \in \mathfrak{C}(A)$. Here, $\mathcal{N}$ is the partial trace of the arbitrarily chosen pre-processing channel of $\Theta_{A\to B}$ in (3.28). 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

$$\mathrm{Tr}_A[\mathcal{U}(\tau_A \otimes \sigma_B)] = \eta_B, \tag{A.21}$$

for any $\tau \in \mathfrak{S}(A)$. By the result of Ref. [19], there exists a unitary operator V such that $\eta_B = \mathrm{Ad}_V(\sigma_B)$, thus by the definition given in (3.2), 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 (A.20) becomes equivalent to

$$\mathrm{Tr}_A[\mathcal{U}(\rho_A \otimes \sigma_B)] = \sigma_B, \tag{A.22}$$

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 (3.2), we get the desired result.

((S:B) $\Rightarrow$ (S:A)) It immediately follows from the fact that any superchannel can be decomposed into pre- and post- processes. Note that the output of the transformed channel on A is immediately discarded, the post-process is irrelevant. The process $\mathcal{N}_{A\to RA}$ can be considered the pre-process 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

$$\mathrm{Tr}_{A'} \circ \mathrm{Ad}_{U_{A'B}}(\sigma_{AB}) = \mathrm{Tr}_{A'} \otimes \sigma_{AB}. \tag{A.23}$$

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

$$\mathrm{Tr}_A \circ \mathrm{Ad}_{U_{AB}} \circ \mathcal{L}_A(\sigma_{AB}) = \mathrm{Tr}_A \circ \mathcal{L}_A(\sigma_{AB}). \tag{A.24}$$

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

$$\mathrm{Tr}_A \circ \mathrm{Ad}_{U_{AB}} \circ \mathcal{N}_{A\to RA}(\sigma_{AB}) = \mathrm{Tr}_A \circ \mathcal{N}_{A\to RA}(\sigma_{AB}). \tag{A.25}$$

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 32. 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 same for every $\mathcal{N} \in \mathfrak{C}(A, B)$, there exists a quantum channel $\mathcal{P} \in \mathfrak{C}(C, AD)$ such that

$$\Theta(\mathcal{L}) = (\mathrm{Tr}_B \circ \mathcal{L}_{A\to B} \otimes \mathrm{id}_D) \circ \mathcal{P}_{C\to AD}, \tag{A.26}$$

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

증명 A basis of $\mathfrak{L}(A, B)$ is $\{\mathcal{E}_{ij} := Y_j \mathrm{Tr}\left[X_i^\dagger \cdot\right]\}$, where $\{X_i\}$ and $\{Y_j\}$ are orthonormal basis 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 following form,

$$\mathcal{L} = \sum_{ij} \mathcal{E}_{ij} \mathrm{Tr}\left[Y_j^\dagger \mathcal{L}(X_i)\right]. \tag{A.27}$$

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

$$\Theta(\mathcal{L}) = \sum_{ij} \mathcal{F}_{ij} \operatorname{Tr}\Big[Y_j^{\dagger} \mathcal{L}(X_i)\Big]. \tag{A.28}$$

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

$$\Theta(\mathcal{L}) = \mathcal{C} \operatorname{Tr}[\mathcal{L}(\pi_A)] + \sum_{i>0} \mathcal{F}_{i0} \operatorname{Tr}[\mathcal{L}(X_i)]. \tag{A.29}$$

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

$$\mathcal{P} := \pi_A \otimes \mathcal{C} + \sum_{i>0} X_i \otimes \mathcal{F}_{i0}. \tag{A.30}$$

From (A.29), we can see that if $\mathcal{Q} \in \mathfrak{C}(C, AE)$ and $\mathcal{R} \in \mathfrak{C}(BE, D)$ are pre- and post-processing 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 (A.29) and (A.30) , we get the desired result

$$\Theta(\mathcal{L}) = (\operatorname{Tr}_B \circ \mathcal{L}_{A\to B} \otimes \mathrm{id}_D) \circ \mathcal{P}_{C\to AD}. \tag{A.31}$$

$\square$

Indeed, as we can observe that the left hand side of (A.20) is a constant superchannel when $\mathcal{N}$ is considered an input, we can apply Lemma 32.

Therefore, there exists a quantum state (which is a special type of quantum channel) τ_{AB} such that

$$\mathrm{Tr}_A[\mathcal{U} \circ (\mathcal{L}_A \otimes \mathrm{id}_B)(\sigma_{AB})] = \mathrm{Tr}_A[(\mathcal{L}_A \otimes \mathrm{id}_B)(\tau_{AB})], \tag{A.32}$$

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

$$\mathrm{Tr}_{A'}[\,(\mathcal{U}_{A'B} \otimes \mathrm{id}_A)(\rho_{A'} \otimes \sigma_{AB})] = \tau_{AB}, \tag{A.33}$$

for all $\rho_{A'} \in \mathfrak{S}(A')$. In other words, the mapping $\rho_{A'} \mapsto \tau_{AB}$ is constant. If one interpret (A.33) as that $U_{A'B} \otimes \mathbb{1}_A$ utilizes σ_{AB} as a randomness source, by the result of Ref. [19], τ_{AB} must have the same spectrum, thus also the same entropy, with σ_{AB}. Then, by Corollary 29, 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.

A.9 Proof of Corollary 21

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

Lemma 33 ([67])**.** 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

$$\rho_{RAB} = \bigoplus_i p_i \rho_{RA_{i,K}} \otimes \rho_{A_{i,L}B}, \tag{A.34}$$

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 33, ρ_{RAB} has the form of (A.34). Therefore, its marginal state on AB must have a form of

$$\rho_{AB} = \bigoplus_i p_i \rho_{A_{i,K}} \otimes \rho_{A_{i,L}B}. \tag{A.35}$$

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}.

A.10 Proof of Theorem 22

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

$$\sigma_{AB} = \sum_{i \in \mathcal{I}_B} p_i \sigma^i_{AB} + \sum_{i \in \mathcal{II}_B} \sigma^i_A \otimes \sigma^i_B. \tag{A.36}$$

The marginal state of A after a general information utilization of B has the following form.

$$\sum_{i \in \mathcal{I}_B} p_i \mathrm{Ad}_{V_i}(\sigma^i_A) + \sum_{i \in \mathcal{II}_B} p_i \Phi_i(\sigma^i_A), \tag{A.37}$$

where Φ_i are some catalytic maps on A and $V_i \in \mathfrak{U}(A)$. Since unitary operations are a special case of catalytic maps, one can simplify the expression and get

$$\sum_i p_i \Phi_i(\sigma_A^i). \tag{A.38}$$

We claim that the probability distribution $\big(\sum_i p_i \lambda_j(\sigma_A^i)\big)$ majorizes $\big(\lambda_j(\sum_i p_i(\sigma_A^i))\big)$. This is because of Fan's Lemma [68].

$$\begin{aligned}
&\sum_{1\le j\le k} \lambda_j \left(\sum_i p_i \Phi_i(\sigma_A^i)\right) = \max_P \operatorname{Tr}\left[P \sum_i p_i \Phi_i(\sigma_A^i)\right] \\
&= \max_P \operatorname{Tr}\left[\sum_i p_i P \Phi_i(\sigma_A^i)\right] \le \max_P \sum_i p_i \operatorname{Tr}\big[P\Phi_i(\sigma_A^i)\big],
\end{aligned} \tag{A.39}$$

where the maximization is over rank-k projectors P. Again by using Fan's Lemma [68], we get

$$\sum_{1\le j\le k} \lambda_j \left(\sum_i p_i \Phi_i(\sigma_A^i)\right) \le \sum_i p_i \sum_{1\le j\le k} \lambda_j(\Phi_i(\sigma_A^i)). \tag{A.40}$$

From the relation between unital maps and majorization, we have $\Phi_i(\sigma_A^i) \succ \sigma_A^i$ for all i, hence $\sum_{1\le j\le k} \lambda_j(\Phi_i(\sigma_A^i) \le \sum_{1\le j\le k} \lambda_j(\sigma_A^i)$ for all i and k. Therefore, it follows that

$$\sum_{1\le j\le k} \lambda_j \left(\sum_i p_i \Phi_i(\sigma_A^i)\right) \le \sum_i p_i \sum_{1\le j\le k} \lambda_j(\sigma_A^i), \tag{A.41}$$

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.

□

Bibliography

[1] I. Alexeev, K. Kim, and H. Milchberg, "Measurement of the superluminal group velocity of an ultrashort bessel beam pulse," *Physical review letters*, vol. 88, no. 7, p. 073901, 2002.

[2] A. Kaya, "Hubble's law and faster than light expansion speeds," *American Journal of Physics*, vol. 79, no. 11, pp. 1151–1154, 2011.

[3] G. Diener, "Superluminal group velocities and information transfer," *Physics Letters A*, vol. 223, no. 5, pp. 327–331, 1996.

[4] D. Beckman, D. Gottesman, M. A. Nielsen, and J. Preskill, "Causal and localizable quantum operations," *Physical Review A*, vol. 64, no. 5, p. 052309, 2001.

[5] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[6] P. Hayden and J. Preskill, "Black holes as mirrors: quantum information in random subsystems," *Journal of high energy physics*, vol. 2007, no. 09, p. 120, 2007.

[7] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Reviews of modern physics*, vol. 81, no. 2, p. 865, 2009.

[8] A. Streltsov, G. Adesso, and M. B. Plenio, "Colloquium: Quantum coherence as a resource," *Reviews of Modern Physics*, vol. 89, no. 4, p. 041003, 2017.

[9] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, p. 621, 2012.

[10] B. Regula, K. Bu, R. Takagi, and Z.-W. Liu, “Characterizing one-shot distillation in general resource theories,” *arXiv preprint arXiv:1909.11677*, 2019.

[11] B. Regula and R. Takagi, “Fundamental limitations on distillation of quantum channel resources,” *Nature Communications*, vol. 12, no. 1, pp. 1–12, 2021.

[12] K. C. Tan, V. Narasimhachar, and B. Regula, “Fisher information universally identifies quantum resources,” *arXiv preprint arXiv:2104.01763*, 2021.

[13] J. Polchinski, “The black hole information problem,” in *New Frontiers in Fields and Strings: TASI 2015 Proceedings of the 2015 Theoretical Advanced Study Institute in Elementary Particle Physics*, pp. 353–397, World Scientific, 2017.

[14] M. Blum, “Coin flipping by telephone a protocol for solving impossible problems,” *ACM SIGACT News*, vol. 15, no. 1, pp. 23–27, 1983.

[15] P. Boes, H. Wilming, R. Gallego, and J. Eisert, “Catalytic quantum randomness,” *Physical Review X*, vol. 8, no. 4, p. 041016, 2018.

[16] S. H. Lie, H. Kwon, M. Kim, and H. Jeong, “Unconditionally secure qubit commitment scheme using quantum maskers,” *arXiv preprint arXiv:1903.12304*, 2019.

[17] S. H. Lie, S. Choi, and H. Jeong, “Min-entropy as a resource for one-shot private state transfer, quantum masking, and state transition,” *Physical Review A*, vol. 103, no. 4, p. 042421, 2021.

[18] S. H. Lie and H. Jeong, “Randomness cost of masking quantum information and the information conservation law,” *Physical Review A*, vol. 101, no. 5, p. 052322, 2020.

[19] S. H. Lie and H. Jeong, “Randomness for quantum channels: Genericity of catalysis and quantum advantage of uniformness,” *Physical Review Research*, vol. 3, no. 1, p. 013218, 2021.

[20] S. H. Lie and H. Jeong, "Correlational resource theory of catalytic quantum randomness under conservation law," *arXiv preprint arXiv:2104.00300*, 2021.

[21] E. Chitambar and G. Gour, "Quantum resource theories," *Reviews of Modern Physics*, vol. 91, no. 2, p. 025001, 2019.

[22] M.-D. Choi, "Completely positive linear maps on complex matrices," *Linear algebra and its applications*, vol. 10, no. 3, pp. 285–290, 1975.

[23] A. Jamiołkowski, "Linear transformations which preserve trace and positive semidefiniteness of operators," *Reports on Mathematical Physics*, vol. 3, no. 4, pp. 275–278, 1972.

[24] G. Gour and C. M. Scandolo, "Dynamical resources," *arXiv preprint arXiv:2101.01552*, 2020.

[25] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Transforming quantum operations: Quantum supermaps," *EPL (Europhysics Letters)*, vol. 83, no. 3, p. 30004, 2008.

[26] G. Gour, "Comparison of quantum channels by superchannels," *IEEE Transactions on Information Theory*, vol. 65, no. 9, pp. 5880–5904, 2019.

[27] G. Chiribella, G. M. D'Ariano, and P. Perinotti, "Theoretical framework for quantum networks," *Physical Review A*, vol. 80, no. 2, p. 022339, 2009.

[28] J. Burniston, M. Grabowecky, C. M. Scandolo, G. Chiribella, and G. Gour, "Necessary and sufficient conditions on measurements of quantum channels," *Proceedings of the Royal Society A*, vol. 476, no. 2236, p. 20190832, 2020.

[29] A. Bisio and P. Perinotti, "Theoretical framework for higher-order quantum theory," *Proceedings of the Royal Society A*, vol. 475, no. 2225, p. 20180706, 2019.

[30] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, "Quantum computations without definite causal structure," *Physical Review A*, vol. 88, no. 2, p. 022318, 2013.

[31] S. H. Lie and H. Jeong, "Generalized transposition, perfect tensors, spacetime and supertrace," *In preparation*, 2021.

[32] N. P. Landsman, "Lecture notes on c*-algebras, hilbert c*-modules, and quantum mechanics," *arXiv preprint math-ph/9807030*, 1998.

[33] U. Haagerup and M. Musat, "Factorization and dilation problems for completely positive maps on von neumann algebras," *Communications in Mathematical Physics*, vol. 303, no. 2, pp. 555–594, 2011.

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

[35] J. Wedderburn, "On hypercomplex numbers," *Proceedings of the London Mathematical Society*, vol. 2, no. 1, pp. 77–118, 1908.

[36] L. Chen and L. Yu, "On the schmidt-rank-three bipartite and multipartite unitary operator," *Annals of Physics*, vol. 351, pp. 682–703, 2014.

[37] D. Suter and G. A. Álvarez, "Colloquium: Protecting quantum information against environmental noise," *Reviews of Modern Physics*, vol. 88, no. 4, p. 041001, 2016.

[38] D. Dieks, "Communication by epr devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, 1982.

[39] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[40] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Y. Halpern, "The resource theory of informational nonequilibrium in thermodynamics," *Physics Reports*, vol. 583, pp. 1–58, 2015.

[41] D. McMahon, *Quantum computing explained*. John Wiley & Sons, 2007.

[42] C. Rovelli, "Relational quantum mechanics," *International Journal of Theoretical Physics*, vol. 35, no. 8, pp. 1637–1678, 1996.

[43] H. Everett, "" relative state" formulation of quantum mechanics," *The Many Worlds Interpretation of Quantum Mechanics*, pp. 141–150, 2015.

[44] P. Adriaans and J. Van Benthem, "Philosophy of information," *Handbook of the Philosophy of Science*, no. 8, 2008.

[45] K. Modi, "Operational approach to open dynamics and quantifying initial correlations," *Scientific reports*, vol. 2, no. 1, pp. 1–5, 2012.

[46] M. Horodecki, P. Horodecki, and J. Oppenheim, "Reversible transformations from pure to mixed states and the unique measure of information," *Physical Review A*, vol. 67, no. 6, p. 062104, 2003.

[47] J. Scharlau and M. P. Mueller, "Quantum horn's lemma, finite heat baths, and the third law of thermodynamics," *Quantum*, vol. 2, p. 54, 2018.

[48] J. Watrous, *The theory of quantum information*. Cambridge university press, 2018.

[49] K. Mølmer, "Optical coherence: A convenient fiction," *Physical Review A*, vol. 55, no. 4, p. 3195, 1997.

[50] S. H. Lie and H. Jeong, "Faithfulness and sensitivity for ancilla-assisted process tomography," *In preparation*, 2021.

[51] L. Zhang and J. Wu, "Von neumann entropy-preserving quantum operations," *Physics Letters A*, vol. 375, no. 47, pp. 4163–4165, 2011.

[52] F. Hiai, M. Mosonyi, D. Petz, and C. Bény, "Quantum f-divergences and error correction," *Reviews in Mathematical Physics*, vol. 23, no. 07, pp. 691–747, 2011.

[53] W. Roga, M. Fannes, and K. Życzkowski, "Composition of quantum states and dynamical subadditivity," *Journal of Physics A: Mathematical and Theoretical*, vol. 41, no. 3, p. 035305, 2008.

[54] L. Floridi, *The philosophy of information*. OUP Oxford, 2013.

[55] A. Korzybski, *Science and sanity: An introduction to non-Aristotelian systems and general semantics*. Institute of GS, 1958.

[56] S. L. Braunstein and A. K. Pati, "Quantum information cannot be completely hidden in correlations: implications for the black-hole information paradox," *Physical review letters*, vol. 98, no. 8, p. 080502, 2007.

[57] K. Modi, A. K. Pati, A. Sen, U. Sen, *et al.*, "Masking quantum information is impossible," *Physical review letters*, vol. 120, no. 23, p. 230501, 2018.

[58] R. Landauer *et al.*, "Information is physical," *Physics Today*, vol. 44, no. 5, pp. 23–29, 1991.

[59] R. Landauer, "Information is a physical entity," *Physica A: Statistical Mechanics and its applications*, vol. 263, no. 1-4, pp. 63–67, 1999.

[60] D. Stoljar, "Physicalism," *Stanford Encyclopedia of Philosophy*, 2001.

[61] C. Shannon, "The lattice theory of information," *Transactions of the IRE professional Group on Information Theory*, vol. 1, no. 1, pp. 105–107, 1953.

[62] P. Kok and S. L. Braunstein, "Postselected versus nonpostselected quantum teleportation using parametric down-conversion," *Physical Review A*, vol. 61, no. 4, p. 042304, 2000.

[63] K. Nemoto and S. L. Braunstein, "Quantum coherence: myth or fact?," *Physics Letters A*, vol. 333, no. 5-6, pp. 378–381, 2004.

[64] A. Arias, A. Gheondea, and S. Gudder, "Fixed points of quantum operations," *Journal of Mathematical Physics*, vol. 43, no. 12, pp. 5872–5881, 2002.

[65] P. Aniello, “Quantum entropies, schur concavity and dynamical semigroups,” in *Journal of Physics: Conference Series*, vol. 804, p. 012003, IOP Publishing, 2017.

[66] M. A. Nielsen, “Probability distributions consistent with a mixed state,” *Physical Review A*, vol. 62, no. 5, p. 052308, 2000.

[67] P. Hayden, R. Jozsa, D. Petz, and A. Winter, “Structure of states which satisfy strong subadditivity of quantum entropy with equality,” *Communications in mathematical physics*, vol. 246, no. 2, pp. 359–374, 2004.

[68] X. Zhan, *Matrix theory*, vol. 147. American Mathematical Soc., 2013.

국 문 초 록

이 논문에서는 Boes 등에 의해 제시된 양자임의도의 촉매 이론을 일반화하여 비국소적, 동적 상황에서 상관관계가 있거나 절차적인 임의도 원천을 활용할 수 있는 이론을 전개한다. 이 논문의 내용은 크게 두 가지로 나뉜다. 첫째로, 임의도 자원이론을 확장해서 상관관계가 있거나 동적인 임의도 원천으로부터 추출 할 수 있는 최대 Rényi 엔트로피의 값을 계산했다. 그 과정에, 만약 임의도 원천이 비침습적인 국소 측정 행위를 허용하지 않는다면 비국소적인 임의도 촉매 작용을 통한 엔트로피 추출은 불가능함을 보였다. 임의도 자원이론은 '오목한' 자원 이론의 전형으로서, 현재 양자자원이론의 지배적인 연구 대상이며 일반적으로 자원들이 그 자원을 삭제하는데 필요한 임의도의 양으로 측정되는 볼록한 자원 이론에 상보적인 역할을 한다. 응용으로, 숨김-금지 정리의 동적 일반화인, 양자정보처리 과정은 단순히 그 입출력을 두 지역으로 분산시키는 것만으로 숨길 수 없다는 암행-금지 정리를 증명했다. 두번째로, 정보 흐름의 물리적 성질을 탐구했다. Landauer의 "정보는 물리적이다" 혹은 Wheeler의 "그것은 비트로부터"와 같은 유명한 문구들은 정보가 한 지점에서부터 다른 지점으로 흔적을 남기며 이동해야하는 물질과 같은 거동을 할 것이라는 추측을 하게 한다. 이 추측을 검사하기 위해서, 임의도 촉매 작용이 정보의 일방통행을 묘사하는 과정임에 주목했다. 그 결과로 고전적인 정보는 그 출발지나 그 주변 환경에 흔적을 남기지 않고 명확한 방향을 가지고 전파될 수 있으나, 양자정보는 그렇지 못함을 보였다. 본 연구에서 개발된 이론을 이용해서, 의미론적 정보의 물리적 정의를 내리는 한 접근법을 제시했고, 그것이 부분적으로 사용된 촉매를 이용하는 것과 동치인

과정임을 보였다. 그로부터 부분적으로 사용된 고전 임의도 원천으로부터는 언제든지 정보를 더 추출할 수 있으나, 양자 임의도 원천으로는 그럴 수 없음을 보였다.

주요어 : 양자정보, 자원이론, 임의도

학번 : 2016-20311

감사의 글

먼저 양자정보이론의 세계에 발디디게 해주시고 한 명의 연구자가 될 수 있는 기회를 주신 정현석 교수님께 감사의 말씀을 드립니다. 근본적인 물리학 이론과 간결한 수학, 그리고 무궁무진한 응용이 맞닿아 있는 양자정보이론을 연구할 수 없었다면 저는 이미 오래 전에 물리학에의 흥미를 잃었지도 모릅니다.

연구실 생활에서 가장 좋았던 것 중 하나를 꼽으라면 연구실 선후배들과 열린 분위기에서 온갖 연구 이야기와 탁상공론을 나눌 수 있었던 점이라 하겠습니다. 이제는 모두 어엿하게 훌륭한 박사들이 되신 영롱, 호용, 채연, 혁준, 대건, 인우, 창훈, 성전이형들 덕분에 연구실 생활 즐겁게 보낼 수 있었습니다. 항상 제가 연구실 막내일 것 같았는데 어느 새 제 뒤에 연구실을 가득 채운 작은 석형, 성욱, 혁건, 병선, 규동에게, 대학원 생활이 참 길다 생각할 수도 하지만 떠날 때가 되면 무척 짧게 느껴지니 논문을 부지런히 쓰길 바랍니다. 항상 친절하게 저희를 대해주셨던 정갑균 박사님, always hardworking and cool guy Bobby, very diligent and fun but also humble Yong-Siah, wish you all the luck in your future, Omkar, and hope you have nice time in Korea, Bose. Thank you for the fun moments we shared. 박사 과정 마지막 순간을 런던에서 보낼 수 있게 친절을 베풀어 주신 김명식 교수님께 특별히 감사의 말씀을 드립니다.

현우, 도원, 혁준에게, 하늘채 터줏대감이 이제야 하늘채를 떠납니다. 주승에게도 감사합니다. 대학, 대학원 시절 내내 어울려 줬던 상현이형에게도 왕감사 드립니다.

끝나지 않을 것 같았던 제 학생 생활의 끝까지 오랜 시간 지원해주신

어머니, 저희 형에게 고맙습니다. 제가 곧 박사가 된다는 말에 언제나 뛸듯이 기뻐하시던 외할머니께 드디어 박사가 됐다는 말씀을 드릴 수 있어서 기쁩니다.