Only uniform randomness can yield quantum advantages

Seok Hyung Lee\textsuperscript{1} and Hyunseok Jeong\textsuperscript{1}
\textsuperscript{1}Department of Physics and Astronomy, Seoul National University, Seoul, 151-742, Korea
(Dated: October 29, 2020)

Randomness can help one to implement quantum maps that cannot be realized in a deterministic fashion. Recently, it was discovered that explicitly treating a randomness source as a quantum system could double the efficiency as a catalyst for some tasks. In this work, we generalize this result to general randomness-utilizing processes and show that the gap between the efficiencies of classical and quantum catalytic randomness is generic. To explore the achievability of catalysis of quantum randomness, we first show that the second law of thermodynamics holds for general randomness-utilizing processes: the amount of randomness never decreases. Especially, for two important randomization processes, dephasing and erasure maps, randomness sources are forced to be used catalytically, i.e., in such a way that the randomness is preserved exactly. Second, we show that non-degenerate catalysts should be used classically, which leads to the fact that the quantum advantage of a catalytic process strictly comes from the uniformness of the randomness source. Finally, we discuss a method to circumvent the previous result that achieves quantum advantage with non-degenerate catalyst uniformized by employing extra work space.

Randomness is a universal resource for numerous applications. Its usage ranges from everyday tasks such as shuffling playing cards to information processing tasks such as symmetric-key cryptography \cite{1} and randomized computation \cite{2}. Recently, the role of randomness as a catalyst for the quantum state transition and the information masking process has been studied \cite{3,4}. The catalycity of randomness means that the randomness is not depleted during the process. Remarkably, it was discovered that, for some tasks, the efficiency of a uniform randomness source can be doubled when the source is explicitly treated as a quantum system, compared to the case where the source is treated as a classical randomness source such as coin tossing or dice roll \cite{3,6}.

On the other hand, the resource theory of quantum randomness is still in its initial stage, and many important questions are left unanswered. Is the catalycity of randomness limited only to some specific cases? Can an arbitrary type of randomness be used as a catalyst if its entropic measures are sufficiently high? What is the origin of the advantage of quantum randomness source?

To answer these questions, we advance the theory of quantum randomness for arbitrary randomness sources. We first find that randomness is never used up during an arbitrary randomness-utilizing process if no ancillary system is allowed to be appended to the target system. This means that randomness is different from other usual depletable resources in quantum information theory such as entanglement and coherence. Moreover, we show that only unital quantum maps can be catalytically implemented. Especially, for two important such processes, dephasing and erasure map, it turns out that randomness is forced to be used catalytically.

Second, we prove that uniformness is the source of the advantage of catalytic quantum randomness. To this end, we first show that there exists a gap between the upper bounds of achievable efficiencies of classical and quantum randomness sources therefore quantum advantage is universal for randomness-utilizing processes. It is then demonstrated that non-degenerate randomness sources can be used only as a classical catalyst. In light of the fact that non-degeneracy is generic for probability distributions, it follows that additional efforts such as uniformization are required in order to take advantage of quantum randomness.

Finally, despite the newly found restrictions, adopting an operationally natural generalization of randomness-utilizing processes, we obtain a resource theory of randomness where randomness is depletable and catalycity is nontrivial. In this more general setting, in return for requiring more work space, any randomness source with sufficiently large entropy can be used as catalytic quantum randomness regardless of its degeneracy.

Main results.—We denote quantum systems by upper case alphabets (A, B, . . .) and their corresponding Hilbert spaces as $\mathcal{H}_A$. The space of operators on $\mathcal{H}$ will be written as $\mathcal{B}(\mathcal{H})$. We will say a map defined on $\mathcal{B}(\mathcal{H})$ is $d$-dimensional if $\dim \mathcal{H} = d$. In this work, we will only consider finite-dimensional systems. We say that a quantum process $\Phi$ on $\mathcal{B}(\mathcal{H}_A)$ is randomness-utilizing when it can be expressed as

$$\Phi(\rho) = \text{Tr}_B U(\rho \otimes \sigma) U^\dagger, \quad (1)$$

with some unitary operator $U$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ and a randomness source $\sigma$, which is a quantum state on $\mathcal{H}_B$, and $\text{Tr}_A U(\rho \otimes \sigma) U^\dagger$ is a constant quantum process. The second condition is imposed since we only want the randomness source to provide randomness to the given process and do not want it to function as an information storage. In fact, if we do not impose the second condition, any quantum map can be expressed in the form of (1) by using Naimark dilation. We will call the constant output of $\text{Tr}_A U(\rho \otimes \sigma) U^\dagger$ corresponding to a randomness-utilizing quantum process as the residue randomness of the pro-
When the residue randomness has the same spectrum (the set of eigenvalues including degeneracy) with the randomness source, we say the randomness-utilizing process is catalytic or the process uses the randomness catalytically. It is because, in that case, one can use the residue randomness as the randomness source of the same process for another uncorrelated input. In the following we will use the family of Rényi entropies \( S_{\alpha} \) given as

\[
S_{\alpha}(\rho) = \frac{1}{1 - \alpha} \log \text{Tr} \rho^\alpha, \tag{2}
\]

for \( 0 < \alpha \), where the log is the logarithmic function with base 2. We also define the max-entropy \( S_0(\rho) := \lim_{\alpha \to 0} S_{\alpha}(\rho) = \log \text{rank} \rho \) and the min-entropy \( S_{\infty}(\rho) := \lim_{\alpha \to \infty} (\rho) = -\log \max \rho_i \) where \( \{\rho_i\} \) is the spectrum of \( \rho \). Note that \( S_1 := \lim_{\alpha \to 1} S_{\alpha} \) is the usual von Neumann entropy.

Randomness-utilizing processes usually randomizes its input states, and by doing so it decays information. There are the two most typical examples of such processes, dephasing and erasure maps. By dephasing map with respect to a basis \( \{|i\} \) we mean quantum maps of the form

\[
\mathcal{D}(\rho) = \sum_i \langle i | \rho | i \rangle |i\rangle \langle i|. \tag{3}
\]

Similarly by erasure map, we mean quantum maps of the form

\[
\mathcal{E}(\rho) = \tau, \tag{4}
\]

with some fixed quantum state \( \tau \). However, if we try to implement an erasure map as a randomness-utilizing process, then it is proven that [5][7] the output state \( \tau \) should have the von Neumann entropy larger than \( \log d \), where \( d \) is the dimension of the input state’s Hilbert space. Therefore if we insist the output system of the erasure map has the same dimension as the input system, then the output state of the map must be the maximally mixed state, i.e. \( \frac{1}{d} \). Afterwards, by the erasure map, we mean the constant quantum map that outputs the maximally mixed state.

In Ref. [3], a special case of randomness-utilizing dephasing map was studied, where the randomness source is limited to be maximally mixed state, i.e. a uniform randomness source and the whole process is required to be catalytic. The lower bound of the size of the randomness source was derived in Ref. [3] with this restriction, which is half the size of the system being dephased. One might ask, however, if this randomness non-consuming property is a special property that other generic randomness-utilizing processes do not have. First, in the following theorem, we show that actually every randomness-utilizing dephasing and erasure map should be catalytic.

**Theorem 1.** Any randomness-utilizing dephasing and erasure map should preserve the randomness source, i.e. their usage of randomness should be catalytic.

**Proof.** First, consider an arbitrary dephasing map \( \mathcal{D} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_A) \) corresponding to a basis \( \{|i\}\) and its randomness source \( \sigma \). Then there exists a dephasing unitary \( V \) on \( \mathcal{H}_A \otimes \mathcal{H}_B \) such that

\[
\mathcal{D}(\rho) = \text{Tr}_B V(\rho \otimes \sigma)V^\dagger, \tag{5}
\]

for any state \( \rho \). Since already dephased state stays unchanged after dephasing, \( \mathcal{D}(|i\rangle\langle i|) = |i\rangle\langle i| \), which is a pure state, therefore its extension \( V(|i\rangle\langle i| \otimes \sigma)V^\dagger \) should be in a product state with some state \( \tau \), i.e.

\[
V(|i\rangle\langle i| \otimes \sigma)V^\dagger = |i\rangle\langle i| \otimes \tau, \tag{6}
\]

where \( \tau \) should not depend on \( i \) as \( \text{Tr}_A V(|i\rangle\langle i| \otimes \sigma)V^\dagger = \tau \) should be independent of the input \( |i\rangle \) from definition. Since \( |i\rangle \otimes \sigma \) and \( |i\rangle \otimes \tau \) are unitarily related, they should have the same spectrum, which should also hold for \( \sigma \) and \( \tau \). It implies that the dephasing process uses the randomness catalytically.

Next, we consider an erasure map \( \mathcal{E} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_A) \) and its randomness source \( \theta \) with corresponding erasing unitary \( W \) on \( \mathcal{H}_A \otimes \mathcal{H}_B \) such that

\[
\mathcal{E}(\rho) = \text{Tr}_B W(\rho \otimes \theta)W^\dagger = \frac{1}{d}, \tag{7}
\]

for any state \( \rho \). We set input-independent state \( \eta := \text{Tr}_A W(\rho \otimes \theta)W^\dagger \). Now we define \( \rho_{AB} := W(\frac{\eta}{d} \otimes \theta)W^\dagger \). Then we evaluate the \( \alpha \)-Rényi entropy of \( \rho_{AB} \), i.e. \( S_\alpha(\rho_{AB}) \), which is same as \( S_\alpha(\frac{\eta}{d} \otimes \theta) = \log d + S_\alpha(\theta) \), because of the fact that unitary operators do not change the Rényi entropy and the additivity of the Rényi entropy.

Next, from the weak subadditivity of the Rényi entropy [8], i.e.

\[
S_\alpha(\rho_{AB}) \leq S_0(\rho_A) + S_\alpha(\rho_B), \tag{8}
\]

we have \( \log d + S_\alpha(\theta) = S_0(\frac{\eta}{d}) + S_\alpha(\tau) = \log d + S_\alpha(\tau) \) since \( S_0(\frac{\eta}{d}) = \log d \). Thus we get \( S_\alpha(\theta) \leq S_\alpha(\tau) \) for any \( \alpha \geq 0 \).

From the duality of masking processes [5][6], the existence of such \( \mathcal{E} \) implies the existence of another erasure map that consumes \( \eta \) and produces \( \theta \) as the residue randomness. Then, from the same argument we get \( S_\alpha(\tau) \leq S_\alpha(\theta) \). Consequently we have \( S_\alpha(\tau) = S_\alpha(\theta) \) for any \( \alpha \geq 0 \), which implies that \( \tau \) and \( \theta \) have the same spectrum. Therefore the erasing process uses the randomness catalytically.

Actually, the weak subadditivity argument can be applied to any randomness-utilizing process. It follows that actually no consumption of randomness can happen in any of such processes. See Supplemental Materials [9] for the proof.
Corollary 2. No randomness-utilizing process degrades randomness of its randomness source, i.e. if its randomness source is $\sigma$ and its residue randomness is $\tau$, we have $S_\alpha(\sigma) \leq S_\alpha(\tau)$ for any $\alpha \in [0, \infty]$. Therefore, any maximally mixed randomness source is a catalyst. Furthermore, any non-unital map strictly increases every Renyi entropy and hence cannot be implemented catalytically and any quantum map that maps a pure state to a pure state should be implemented catalytically.

This result is fairly natural in the light of the second law of thermodynamics and provides an important perspective on the randomness consumption of quantum processes: it is not randomness per se that is consumed in the process, but it is its uncorrelatedness with other system, which is often referred to as privacy.

Next, we investigate the nature of catalytic quantum randomness. To do so, we first examine the previously assumed conditions on randomness sources. In Ref. [10], noisy operations were considered, which are the quantum maps of the form of $U$ but with uniform randomness sources. In the resource theory of nonequilibrium, maximally mixed states are considered free since it can be interpreted that they have reached equilibrium, so that they are useless in the thermodynamic setting. In Ref. [3], however, the same noisy operation formalism is adopted for resource-theoretic approach to randomness. From that perspective, maximally mixed state is no longer free but a highly desirable form of randomness compared to nonuniform randomness [11, 12].

However, randomness sources are in general nonuniform and usually require some kind of uniformization for applications [13]. A canonical example of such randomness source is thermal state with non-degenerate Hamiltonian. In fact, almost every finite probability distribution and quantum state is non-degenerate and any degenerate probability distribution can be turned into a non-degenerate one with arbitrarily small perturbation. The following theorem shows that almost every randomness source cannot be used quantumly. The proof is given in Supplemental Materials [9].

Theorem 3. Any randomness-utilizing process using non-degenerate randomness source as a catalyst is a random unitary map in which randomness is used classically.

When we say a probability distribution $\{p_i\}$ is used classically, we mean that it is used to implement the convex sum of deterministic processes, i.e. unitary maps, in the form of random unitary $\sum_i p_i U_i \rho U_i^\dagger$. Note that even if we give up the exact implementation of the desired map, the requirement of catalycity still forces the approximate map to be a random unitary map. Being forced to use randomness classically undermines the efficiency of randomness-utilizing process.

Hereby we examine the quantum advantage of randomness usage in resource theory of randomness for non-degenerate randomness sources. The following Theorem unifies the pre-existing results on the advantage of using quantum randomness sources. The proof can be found in Supplemental Materials [9].

Randomness-utilizing process $\Phi(\rho) = \text{Tr}_B U(\rho \otimes \sigma) U^\dagger = \Psi(\rho) \otimes \tau$

![FIG. 1: A generalized randomness-utilizing process $\Phi$. If one intends to implement a certain quantum map $\Psi$ utilizing a randomness source $\sigma$ which has large enough min-entropy but is not a uniform random state, it could be implemented if one employs a broader notion of catalycity and allows the uncorrelated leftover randomness in the output state.](image)

Theorem 4. A $d$-dimensional randomness-utilizing unital channel with the entanglement-assisted classical capacity $C_{EA}$ requires a classical randomness source with at least $2 \log d - C_{EA}$ of min-entropy or a quantum randomness source with at least $\log d - \frac{1}{2} C_{EA}$ of min-entropy.

For example, by noting that a dephasing map has $C_{EA} = \log d$ and the erasure map has $C_{EA} = 0$, the known bounds for randomness costs for dephasing maps and erasure maps [3, 6, 14] can be derived from Theorem 4. Note that Theorem 4 shows the existence of a gap between classical and quantum bounds but the bounds may not be tight. For instance, there are some unital maps that do not permit classical catalytic implementation [15]. Nevertheless, the min-entropy in the region between $\log d - \frac{1}{2} C_{EA}$ and $2 \log d - C_{EA}$ is forbidden for any classical catalyst, we will say that catalysis with min-entropy in that region achieves the quantum advantage of randomness usage. Hence, Theorem 3 implies that the quantum advantage cannot be attained if the randomness source is non-degenerate.

We summarize the implication of the previous results for the two most important randomness-utilizing process as the following corollary.

Corollary 5. If the randomness source of a $d$-dimensional randomness-utilizing dephasing (erasure) map is non-degenerate, it should have the min-entropy larger than or equal to $\log d (2 \log d)$. 

This lower bound is twice larger than the minimal values of \( \frac{1}{2} \log d \) for dephasing maps \([3]\) and \( \log d \) for erasure maps \([4, 5]\). Considering that the maximally mixed state, which could attain the minimal randomness cost, can be arbitrarily close to a non-degenerate state, we can see that being uniform is the key property for a quantum randomness source.

On the other hand, classical randomness source need not be uniform to function properly. For example, a non-degenerate randomness source given as \((1/8, 3/8, 1/2)\) can implement a dephasing map. See that by applying \( I \) for the first and the second outcome and applying the Pauli \( Z \) operator to a qubit system for the last outcome, one can completely dephase the qubit with respect to the computational basis. More generally, for a given probability distribution \( \{ p_m \} \), if one can find a family of real parameters \( \{ \theta_{nm} \} \) such that

\[
\sum_{nm} p_m \exp \left( i \theta_{nm} - i \theta_{n'm} \right) = \delta_{nn'},
\]

then one can dephase a quantum system with a randomness source with the spectrum \( \{ p_m \} \) and the set of unitary operators \( \{ Z_m := \sum_n \exp \left( i \theta_{nm} \right) |n\rangle\langle n| \} \). However, to the best of our knowledge, there is no known complete characterization of classical randomness source that can be used for dephasing or erasure maps. The contrast against classical randomness characterizes uniformness as the essence of quantum catalytic randomness.

Are generic non-degenerate randomness sources useless as a quantum randomness source, after all? We show that, if we generalize the definition of randomness-utilizing process, any randomness source with high enough min-entropy can be used as a quantum randomness source. We will say that a quantum map \( \Phi \) is a generalized randomness-utilizing implementation of another process \( \Psi \) on \( \mathcal{B}(\mathcal{H}_A) \) if there exists a bipartite unitary \( U \) on \( \mathcal{H}_A \otimes \mathcal{H}_B \) and a randomness source \( \sigma \) such that

\[
\Phi(\rho) = \Tr_B U(\rho \otimes \sigma)U^\dagger = \mathcal{T}(\Psi(\rho)),
\]

where \( \mathcal{T} \) is an invertible quantum map, i.e. there exists another quantum map \( \mathcal{R} \) such that \( \mathcal{R} \circ \mathcal{T} = \mathcal{I} \). This generalized definition says that, intuitively, if we can restore the output of the desired process deterministically from the output of an actually implemented process, we will consider it legitimate implementation. However, from the result of Ref. \([16]\), every invertible quantum map can be expressed as paring with an ancillary state followed by a unitary operation, i.e. the form of \( \mathcal{T} \) without partial trace \( \Tr_B \). Thus, by making \( U \) in \( \Phi \) absorb the unitary operators in \( \mathcal{T} \), we can actually re-express the definition of generalized randomness-utilizing implementation \( \Phi \) of process \( \Psi \)

\[
\Phi(\rho) = \Tr_B U(\rho \otimes \sigma)U^\dagger = \Psi(\rho) \otimes \tau,
\]

with some constant quantum state \( \tau \) independent of input \( \rho \). (See Fig. 1). In every practical sense, this definition is operationally legitimate. Every machine producing a certain type of product always produces accompanying byproducts such as noise, heat, dust or vibration. Nevertheless, as long as those byproducts can be unambiguously separated from the desired output, it is natural to say that the process was implemented as desired. Therefore we will call the uncorrelated byproduct \( \tau \) of \( \Phi \) as the leftover randomness of the randomness-utilizing process \( \Phi \).

We also generalize the notion of catalycity. If the residue randomness of \( \Phi \) in \( \Phi(\rho) \) can be repeatedly used for another generalized randomness-utilizing implementation (which can be different from the original implementation) of the same process as the randomness source, we will say that the randomness usage in the implementation is catalytic. This generalization is also operationally reasonable since the exact form of a catalyst need not be preserved as long as its ‘catalytic power’ is conserved during the process. This generalization is depicted in Fig. 1 as the transformation of the randomness source \( \sigma \) to \( \sigma' \), which can be recycled for another round of randomness-utilizing process.

We remark that in this generalized setting, non-decreasing property of randomness is not forced unlike the original setting. The proof of Corollary 2 depends on the fact that the output system of the process has the same dimension as the input system, but in the generalized setting the output system can be much larger than the input system. In fact, extracting randomness of a randomness source and injecting it into the output state is allowed, therefore randomness can be actually consumed in this setting.

Nevertheless, in this generalized setting, it is indeed possible to catalytically use a non-degenerate state as a quantum randomness source. The following Theorem is proved in Ref. \([17]\), and we state it here for completeness.

**Proposition 6.** \([17]\) Any quantum state \( \sigma \) with \( S_{\infty}(\sigma) \geq \log d \) (or \( S_{\infty}(\sigma) \geq 2\log d \)) can be catalytically used as the randomness source for a generalized randomness-utilizing implementation of a \( d \)-dimensional dephasing map (or the erasure map).

A sketch of proof is as follows: by the Birkhoff-von Neumann theorem \([18, 19]\), every finite probability distribution with the min-entropy larger than or equal to \( \log d \) can be expressed as a convex sum of uniform distribution with the supporter of size \( d \). Therefore, by conditionally generating a randomness source, we can randomly choose one of those uniform distributions and extract it. This randomness can be generated by creating its purification and distributing it to two local systems. It is possible because the creation of entangled pure state can be done via unitary operation. By using the extracted uniform randomness, we can implement the desired process. As a result, both parties have some leftover randomness but it is allowed from the definition of the generalized randomness-utilizing process.
randomness-utilizing processes. A detailed proof can be found in Ref. 17.

Proposition 6 shows that when extra work space is allowed, one can generate ‘bound’ randomness by sharing an entangled state in the extra space that can be used for uniformizing a non-degenerate randomness source. This, in a sense, demonstrates the usage of ‘catalyst for catalyst’. This type of ‘expanding space to achieve uniformity’ was also used in Ref. 20.

Conclusion.—We showed that when randomness is utilized to implement quantum maps, it is not expendable but inevitably reusable. Especially, for the two most important randomization maps, dephasing and erasure maps, randomness sources cannot be used non-cata-
ystically. We further found that the quantum advantage of randomness is common for arbitrary randomness-utilizing processes and it requires uniformness of the randomness source. Even if the source’s entropic measures are arbitrarily high, it cannot be used as a quantum catalyst if it is non-degenerate. These two restrictions distinguish the resource theory of randomness from other types of quantum resource theories, but we also found that allowing expansion of dimension after randomness-utilizing process could circumvent both restrictions. It was done by showing that it is still possible to take advantage of catalytic quantum randomness in the generalized setting if the randomness source’s min-entropy is high enough.

We remark that we focused on exact realizations of catalysis in contrast to Ref. 20, 21 where the framework was generalized to approximate realizations but with the cost of having to prepare arbitrary many and arbitrarily large catalysts to achieve the desired level of accuracy. This work is more relevant to a realistic situation where the user has one given randomness source, not a set of multiple sources, and tries to assess its capability for various tasks. Furthermore, Theorem 4 can be applied for arbitrary quantum maps, hence actually one can still use the results of this work to analyze approximate catalysis.

An interesting direction for future works is proving the existence of and constructing catalytic implementations achieving the lower bounds of Theorem 4 for both classical and quantum catalyst cases. Another intriguing topic is rigorously establishing the resource theory of uncorrelatedness of randomness sources as mentioned in this work.

This work was supported by the National Research Foundation of Korea (NRF) through grants funded by the the Ministry of Science and ICT (Grants No. NRF-2019M3E4A1080074 and No. NRF-2020R1A2C1008609).

[1] H. Delfs and H. Knebl, Symmetric-key encryption, in Introduction to Cryptography (Springer, 2007) pp. 11–31.
[2] M. Smid, Closest-point problems in computational geometry, in Handbook of computational geometry (Elsevier, 2000) pp. 877–935.
[3] P. Boes, H. Wilming, R. Gallego, and J. Eisert, Catalytic quantum randomness, Physical Review X 8, 041016 (2018).
[4] P. Boes, J. Eisert, R. Gallego, M. P. Müller, and H. Wilming, Von neumann entropy from unitarity, Physical Review Letters 122, 210402 (2019).
[5] S. H. Lie, H. Kwon, M. Kim, and H. Jeong, Unconditionally secure qubit commitment scheme using quantum masks, arXiv preprint arXiv:1903.12304 (2019).
[6] S. H. Lie and H. Jeong, Randomness cost of masking quantum information and the information conservation law, Physical Review A 101, 052322 (2020).
[7] H. Imai, J. Müller-Quade, A. C. Nascimento, P. Tuyls, and A. Winter, An information theoretical model for quantum secret sharing, Quantum Information & Computation 5, 69 (2005).
[8] W. van Dam and P. Hayden, Renyi-entropic bounds on quantum communication, arXiv preprint quant-ph/0204093 (2002).
[9] S. H. Lie and H. Jeong, Supplementary Materials (2020).
[10] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Y. Halpern, The resource theory of informational nonequilibrium in thermodynamics, Physics Reports 583, 1 (2015).
[11] J. L. Mceliece and B. Pinkas, On the impossibility of private key cryptography with weakly random keys, in Conference on the Theory and Application of Cryptography (Springer, 1990) pp. 421–435.
[12] Y. Dodis, S. J. Ong, M. Prabhakaran, and A. Sahai, On the (im) possibility of cryptography with imperfect randomness, in 45th Annual IEEE Symposium on Foundations of Computer Science (IEEE, 2004) pp. 196–205.
[13] J. Von Neumann, 13. various techniques used in connection with random digits, Appl. Math Ser 12, 5 (1951).
[14] P. O. Boykin and V. Roychowdhury, Optimal encryption of quantum bits, Physical review A 67, 042317 (2003).
[15] L. Landau and R. Streater, On birkhoff’s theorem for doubly stochastic completely positive maps of matrix algebras, Linear algebra and its applications 193, 107 (1993).
[16] A. Nayak and P. Sen, Invertible quantum operations and perfect encryption of quantum states, Quantum Information & Computation 7, 103 (2007).
[17] S. H. Lie, S. Choi, and H. Jeong, in preparation (2020).
[18] G. Birkhoff, Three observations on linear algebra, Univ. Nac. Tacuman, Rev. Ser. A 5, 147 (1946).
[19] J. Von Neumann, A certain zero-sum two-person game equivalent to the optimal assignment problem, Contributions to the Theory of Games 2, 5 (1953).
[20] F. Brandao, M. Horodecki, N. Ng, J. Oppenheim, and S. Wehner, The second laws of quantum thermodynamics, Proceedings of the National Academy of Sciences 112, 3275 (2015).
[21] M. P. Müller, Correlating thermal machines and the second law at the nanoscale, Physical Review X 8, 041051 (2018).
[22] A. Arias, A. Gheondea, and S. Gudder, Fixed points of quantum operations, Journal of Mathematical Physics 43, 5872 (2002).
[23] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Entanglement-assisted classical capacity of noisy quantum channels, Physical Review Letters 83, 3081
Appendix : Supplemental Materials

Proof of Corollary 2

We start from the proof of Theorem 1 except that $\mathcal{E}$ is now an arbitrary map instead of an erasure map. Now, by using the weak subadditivity of Rényi entropy again for the maximally mixed input state case (6), we get

$$\log d + S_\alpha(\theta) \leq S_\alpha \left( \frac{1}{d} \right) + S(\tau). \quad (10)$$

Hence, since $S_0 \left( \frac{1}{d} \right) \leq \log d$, we get $S_\alpha(\theta) \leq S_\alpha(\tau)$. Especially, if $\theta$ is already maximally mixed, i.e. $S_\alpha(\theta) = \log d_B$, then we get that $S_\alpha(\theta) = S_\alpha(\tau)$ for all $\alpha$.

Now, from the subadditivity of the von Neumann entropy, we have

$$\log d + S(\theta) \leq S \left( \frac{1}{d} \right) + S(\tau). \quad (11)$$

Therefore, if $\mathcal{E}$ is not unital, then $S \left( \mathcal{E} \left( \frac{1}{d} \right) \right) < \log d$ and therefore the von Neumann entropy of the randomness source strictly increases. It implies that a non-unital quantum map cannot be implemented catalytically.

That any quantum map that maps a pure state to a pure state is catalysis follows from the same argument of the proof of Theorem 1 for dephasing maps.

Proof of Theorem 3

We continue from the proof for erasure map of Theorem 1 but we can assume that now $\mathcal{E}$ is an arbitrary unital map by Corollary 2. As $\theta = R_\eta R_\eta^\dagger$ for some unitary operator $R$, by making $W$ absorb $R$, without loss generality we can assume $\theta = \eta$. Let us define the ‘complementary’ channel of $\mathcal{E}$ for each input $\rho$,

$$\hat{\mathcal{E}}_\rho(\xi) := \text{Tr}_A W(\rho \otimes \xi) W^\dagger. \quad (12)$$

(Note that this is different from the conventional definition of complementary channels.) Observe that $\theta$ is a fixed point of $\hat{\mathcal{E}}_\rho$ for arbitrary $\rho$. Consider the case of $\rho = \frac{1}{d}$. For this case, $\hat{\mathcal{E}}_{\frac{1}{d}}$ is an unital quantum channel and one can decompose $\hat{\mathcal{E}}_{\frac{1}{d}}$ into Kraus operators $\{K_{nm}\}$ such that $\hat{\mathcal{E}}_{\frac{1}{d}}(\xi) = \frac{1}{d} \sum_{nm} K_{nm} \xi K_{nm}^\dagger$ given as $K_{nm} = (|n\rangle \otimes 1) W (|m\rangle \otimes 1)$. Since $\mathcal{H}_A$ is a finite-dimensional Hilbert space, $\theta$ being a fixed point of $\hat{\mathcal{E}}_{\frac{1}{d}}$ implies that every $K_{nm}$ commutes with $\theta$ [22]. However, since $\theta$ is assumed to be non-degenerate, it implies that every $K_{nm}$ is diagonal in the eigenbasis of $\theta$. As a result the bipartite unitary $W$ is diagonal in the system $B$, i.e. $W$ is a controlled unitary of the form

$$W = \sum_m W_m^A \otimes |m\rangle \langle m|_B, \quad (13)$$

where $W_m$ are unitary operators on $\mathcal{H}_A$ and $\theta = \sum_m q_m |m\rangle \langle m|$ is the unique spectral decomposition of $\theta$. Therefore we get the following random unitary expression of the erasure channel $\mathcal{E}$,

$$\mathcal{E}(\rho) = \sum_m q_m W_m \rho W_m^\dagger. \quad (14)$$

It implies that the usage of randomness in this process is classical, i.e. $\mathcal{E}$ is implemented by applying $W_m$ depending on the random variable $m$ sampled from the distribution $\{q_m\}$.

Proof of Theorem 4

Theorem 1 follows from Theorem 2 of [9]. We state it here for the completeness.

Theorem 7. Consider a quantum channel $N$, a convex sum of quantum channels $\{N_i\}$, i.e. $\sum p_i N_i = N$. For all $i$, the difference of the entanglement-assisted classical capacity $C_{EA}(N_i)$ of $N_i$ and $N$ has the following upper bound,

$$C_{EA}(N_i) - C_{EA}(N) \leq -\log p_i. \quad (15)$$

Every randomness-utilizing process $\Phi(\rho) = \text{Tr}_B U(\rho \otimes \sigma) U^\dagger$ can be expressed as a convex sum of the form $\Phi(\rho) = \sum_i p_i \Phi_i(\rho)$ with $\Phi_i(\rho) = \text{Tr}_B U(\rho \otimes |i\rangle \langle i|) U^\dagger$ when the randomness source $\sigma$ has the spectral decomposition of $\sigma = \sum_i p_i |i\rangle \langle i|$. We define the complementary channel for each $\Phi_i$ as $\hat{\Phi_i}(\rho) = \text{Tr}_A U(\rho \otimes |i\rangle \langle i|) U^\dagger$. Note that $\Phi := \sum_i p_i \Phi_i$ should be a constant channel from the definition of randomness-utilizing processes, thus $C_{EA}(\Phi) = 0$.

Using the following expression [23, 24] of the entanglement-assisted classical capacity of $N : A' \to B$,

$$\max_{\rho_{AA'}} I(A : B)_{\tau_{AA'}} = C_{EA}(N), \quad (16)$$

where $\rho_{AA'}$ is a pure state on $AA'$ and $\tau_{AA'} = (1_{AA} \otimes N_{A'\to B})(\rho_{AA'} \otimes 1_{BB})$, we get the following bound by applying Theorem 7 for each $\Phi_i$ and $\hat{\Phi_i}$,

$$\max_{\rho_{AA'}} I(A : B)_{\tau_{AA'}} - C_{EA}(\Phi) \leq -\log p_i. \quad (17)$$

for an arbitrarily given bipartite pure state $\rho_{AA'}$ with $\tau_{AB} = (1_{RR} \otimes U)(\rho_{RA} \otimes |i\rangle \langle i|_B)(1_{RR} \otimes U^\dagger)$ and $C_{EA} := C_{EA}(\Phi)$. From the information conservation law for pure tripartite states [9],

$$2S(R) = I(R : A) + I(R : B), \quad (18)$$
by choosing an arbitrary maximally entangled state $\phi_{RA}$ we get

$$\min\{2 \log d - C_{EA} - I, +I\} \leq -\log p_i, \quad (19)$$

where $I := I(R : B)_{\tau_{RB}}$. Now, for classical catalysis, $U$ should be a conditional unitary conditioning on the eigenbasis of $\sigma$, so we get $I = 0$. The lower bound $S_{\min}(\sigma) = -\max_i \log p_i \geq 2 \log d - C_{EA}$ follow from the minimization over $i$. The general bound for quantum catalysis follows from the minimization the lower bound over $I$, which is achieved at $I = \log d - \frac{1}{2} C_{EA}$, and we get $S_{\min}(\sigma) \geq \log d - \frac{1}{2} C_{EA}$. 
