Intrinsic randomness as a measure of quantum coherence

Xiao Yuan, Hongyi Zhou, Zhu Cao, and Xiongfeng Ma

Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China

Based on the theory of quantum mechanics, intrinsic randomness in measurement distinguishes quantum effects from classical ones. From the perspective of states, this quantum feature can be summarized as coherence or superposition in a specific (classical) computational basis. Recently, by regarding coherence as a physical resource, Baumgratz *et al.* [Phys. Rev. Lett. **113**, 140401 (2014)] presented a comprehensive framework for coherence measures. Here, we propose a quantum coherence measure essentially using the intrinsic randomness of measurement. The proposed coherence measure provides an answer to the open question in completing the resource theory of coherence. Meanwhile, we show that the coherence distillation process can be treated as quantum extraction, which can be regarded as an equivalent process of classical random number extraction. From this viewpoint, the proposed coherence measure also clarifies the operational aspect of quantum coherence. Finally, our results indicate a strong similarity between two types of quantumness—coherence and entanglement.

I. INTRODUCTION

As one of the fundamental laws of quantum mechanics, Born's rule [1] endows the real world with true randomness that does not exist in the classical Newtonian theory. Such is the counterintuitiveness of the result that Einstein was quoted as saying, "God does not play dice." Nevertheless, the intrinsically random nature of measurement outcomes is now considered a key characteristic that distinguishes quantum mechanics from classical theory [2].

As a key feature of quantum mechanics, coherence is often considered as a basic ingredient for quantum technologies [3,4]. Considerable effort has been undertaken to theoretically formulate quantum coherence [5–12]. Recently, a comprehensive framework of coherence quantification was established [10], by which coherence is considered to be a resource that can be characterized, quantified, and manipulated in a manner similar to that of another important feature—quantum entanglement [13–16]. Within the resource framework of coherence, several coherence monotones are proposed based on relative entropy and l_1 matrix norm [10], and on skew information [12]. A thorough understanding of the resource theory of coherence is left as an interesting open question [10].

In measurement theory, decoherence, breaking coherence, or superposition, in a specific (classical) computational basis, results in random outcomes [17]. Intuitively, from the resource perspective, randomness can be generated by consuming coherence of a quantum state. In order to quantitatively establish this connection, one needs to find a proper way to assess the randomness of measurement, which normally contains quantum and classical processes. The superficially random outcomes in classical processes are generally not truly random, although they might appear so if information is ignored. Thus, such classical part of randomness should be precluded when quantifying a quantum feature—coherence. A quantum process, on the other hand, can generate genuine randomness, which we call intrinsic (quantum) randomness. Observing such intrinsic random outcomes of measurements would indicate nonclassical (quantum) features of objects.

As an example, let us consider the famous Schrödinger's cat gedanken experiment as shown in Fig. 1. In a classical world, a cat might be either alive or dead before observation, which can be described by the density matrix $\rho_{\mathrm{cat}}^{\mathrm{C}} = (|\mathrm{live}\rangle\langle\mathrm{live}| + |\mathrm{dead}\rangle\langle\mathrm{dead}|)/2$ for the case of being alive and dead equally likely, see Fig. 1(a). The observation result of whether the cat is alive or dead looks random, which is due to the lack of knowledge of the cat system. After considering some hidden variables or an ancillary system E that purifies $\rho_{\mathrm{cat}}^{\mathrm{C}}$, $|\Psi\rangle = (|\mathrm{live}\rangle|0\rangle_E + |\mathrm{dead}\rangle|1\rangle_E)/\sqrt{2}$, we can simply observe the system E to infer whether the cat is alive or dead. In quantum mechanics, the cat can be in a coherent superposition of the states of alive and dead, $\rho_{\mathrm{cat}}^{\mathrm{Q}} = |\psi\rangle\langle\psi|$, where $|\psi\rangle = (|\mathrm{live}\rangle + |\mathrm{dead}\rangle)/\sqrt{2}$, see Fig. 1(b). The observation outcome would be intrinsically random according to Born's rule. That is, without directly accessing the system of the cat and breaking the coherence, we can never predict whether the cat is alive or dead better than by blindly guessing. Therefore, the existence of intrinsic randomness can be regarded as a witness for quantum coherence.

With such strong evidence of the connection between coherence and intrinsic randomness, a natural question is whether we can consider the intrinsic randomness as a measure of coherence. If this is possible, production of a certain amount of intrinsic randomness will inevitably cause consumption of the same amount of coherence.

In this study, we explicitly answer this question by first proposing a coherence measure using intrinsic randomness and thus show the equivalence of the definitions between intrinsic randomness and quantum coherence. Then we present a coherence distillation protocol for pure states and show that it is equivalent to random number extraction. Our distillation protocol provides an operational meaning to coherence, thus it answers the open question, stated in the literature [10], on the resource aspect of quantum coherence. Next, by noticing the similarity to the entanglement of formation (EOF) [13,18,19], we provide an explicit way to evaluate our coherence measure for the qubit case. It is worth mentioning that the proposed measure is the first convex roof measure for coherence. Finally, we compare the two quantumness measures, coherence and entanglement, in a more general scenario.
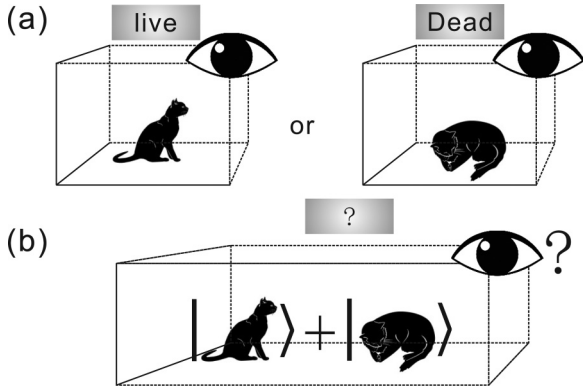
FIG. 1. Illustration of Schrödinger's cat gedanken experiment.

II. COHERENCE MEASURES

We first briefly review the framework of coherence measures [10]. The following discussion is focused on a general d-dimensional Hilbert space, if not specified. For a classical computational basis $I = \{|i\rangle\}_{i=1,2,...,d}$, which is similar to the alive and dead basis of the cat, quantum coherence can be interpreted as the superposition strength on the classical states from set I. For example, any state that can be represented by a diagonal state of I, that is,

$$\delta = \sum_{i=1}^{d} p_i |i\rangle\langle i|, \tag{1}$$

has no superposition and is thus called an incoherent (classical) state. We label the set of such state by $\mathcal{I}$. Conversely, a maximally coherent state is given by the maximal superposition state

$$|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle, \tag{2}$$

up to arbitrary relative phases between the components $|i\rangle$.

Similar to the definition of local operations and classical communication (LOCC) in entanglement [13–15], the incoherent operations are defined by incoherent completely positive trace preserving (ICPTP) maps $\Phi_{\text{ICPTP}}(\rho) = \sum_n K_n \rho K_n^\dagger$, where the Kraus operators $\{K_n\}$ satisfy $\sum_n K_n K_n^\dagger = I$ and $K_n \mathcal{I} K_n^\dagger \subset \mathcal{I}$. For the case where postselections are enabled, the output state corresponding to the nth Kraus operation is given by $\rho_n = K_n \rho K_n^\dagger / p_n$, where $p_n = \text{Tr}[K_n \rho K_n^\dagger]$ is the probability of obtaining the outcome n.

The amount of coherence can be quantified in a manner similar to entanglement [13–15]. Generally, a measure of coherence is a map C from quantum state ρ to a real nonnegative number that satisfies the properties listed in Table I.

Based on the distance measure, coherence can be quantified by the minimum distance from ρ to all the incoherent states in I [10]. Two examples are, respectively, based on the relative entropy

$$C_{\text{rel,ent}}(\rho) \equiv \min_{\delta \in I} S(\rho||\delta), \tag{3}$$

and the l_1 matrix norm

$$C_{l_1}(\rho) \equiv \min_{\delta \in I} \| \rho - \delta \|_{l_1} = \sum_{i \neq j} |\langle i|\rho|j\rangle|. \tag{4}$$

III. INTRINSIC RANDOMNESS

In quantifying the intrinsic randomness of measurement, we restrict on projective measurements $P_I = \{P_i = |i\rangle\langle i|\}$ in the same classical basis I [20]. Here, we define intrinsic randomness as the random outcomes that cannot be predicted.

For example, when measuring a pure state $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \sum_i a_i |i\rangle$, the measurement outcomes are truly random according to Born's rule. Let $p_i = \text{Tr}[P_i \rho] = |a_i|^2$ be the probability of obtaining the ith outcome, the randomness of the output random variable A can be quantified by $R_I(|\psi\rangle\langle\psi|) = H(A) \equiv -\sum_i p_i \log_2 p_i$, where H is the Shannon entropy function on the probability distribution $\{p_i\}$. Define ρ^{diag} to be the density matrix that has only diagonal terms of ρ in the computational basis I. We can rewrite $R_I(|\psi\rangle\langle\psi|)$ as

$$R_I(|\psi\rangle\langle\psi|) = S(\rho^{\text{diag}}), \tag{5}$$

where S is the von Neumann entropy function. Suppose that the projective measurement is performed on N copies of $|\psi\rangle$, it is evident that the N outcomes are independent and identically distributed (i.i.d.) random variables. With the Shannon source coding theorem [21], these random outcomes can be compressed into about $NH(A)$ bits, thus intuitively explaining why $H(A)$ quantifies the average randomness of the measurement outcome. We emphasize that our results can also be derived with other entropy functions [22], such as min-entropy, which is also widely used to quantify randomness. Here, we only consider the case where the measurement outcomes are i.i.d. and leave the general case in Appendix D.

For a general mixed quantum state ρ, one might naively quantify the randomness in a similar manner to the pure state case. Clearly, this definition overestimates the intrinsic randomness. For instance, consider a maximally entangled bipartite state $|\psi^{AE}\rangle = (|00\rangle + |11\rangle)/2$ shared by Alice and Eve. Alice performs projection measurements on her quantum states to gain random numbers. Suppose that the measurement basis is $I = \{|0\rangle, |1\rangle\}$, Alice's outputs look random, but they can always be predicted by Eve, who simply measures her qubits on the same basis. Equivalently, the system E can be

TABLE I. Properties that a coherence measure should satisfy .

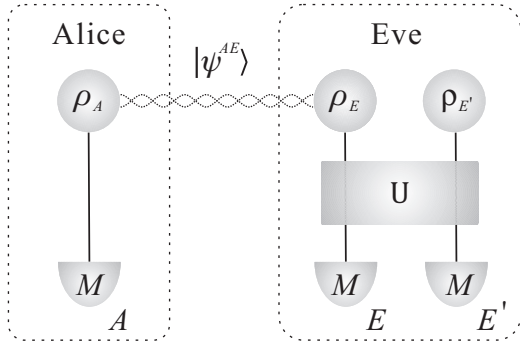|	
(C1)	Coherence vanishes for all incoherent state. That is, $C(\delta) = 0$, for all $\delta \in \mathcal{I}$. A stronger requirement claims that (C1') $C(\delta) = 0$, iff $\delta \in \mathcal{I}$.
(C2)	*Monotonicity*: coherence should not increase under incoherent operations. Thus, (C2a) $C(\rho) \geqslant C(\Phi_{\text{ICPTP}}(\rho))$, and (C2b) $C(\rho) \geqslant \sum_n p_n C(\rho_n)$, where (C2b) is for the case where postselection is enabled.
(C3)	*Convexity*: coherence cannot increase under mixing states, $\sum_e p_e C(\rho_e) \geqslant C(\sum_e p_e \rho_e)$.

FIG. 2. Alice performs projection measurement in the I basis on a quantum state ρ_A, which could possibly be entangled with ρ_E.

regarded as a hidden variable that determines the state of Alice with certainty. Therefore, we should not recognize this type of randomness as being intrinsic randomness.

Instead, we consider a purified state, $|\psi^{AE}\rangle$, that is shared by Alice and an adversary, Eve, who attempts to predict the outputs of Alice's measurement as shown in Fig. 2. The intrinsic randomness quantifies the randomness of Alice's measurement outcomes A, conditioned on Eve's predictions E and E'. As the operations of Alice and Eve commute with each other, we can, without loss of generality, imagine that Eve performs her measurement first. For simplicity, suppose that Eve performs the projection measurement $\{|\psi_e^E\rangle\langle\psi_e^E|\}$ on her state. When Eve obtains an outcome e with probability p_e, the state of Alice is $|\psi_e^A\rangle = \langle\psi_e^E|\psi^{AE}\rangle$. As we already know, the measurement randomness that Alice can generate on $|\psi_e^A\rangle$ is given by $R_I(|\psi_e^A\rangle)$. The total randomness can be quantified by $\sum_e p_e R_I(|\psi_e^A\rangle)$, where $\rho_A = \sum_e p_j |\psi_e^A\rangle\langle\psi_e^A|$. As Eve could choose her measurement basis to maximize the probability of guessing Alice's measurement outcome, the intrinsic randomness that Alice can generate should take the minimum of all possible decomposition of ρ_A, that is,

$$R_I(\rho) = \min_{\{p_e, |\psi_e\rangle\}} \sum_e p_e R_I(|\psi_e\rangle), \qquad (6)$$

where $\rho = \sum_e p_e |\psi_e\rangle\langle\psi_e|$ and $\sum_e p_e = 1$. Notice that as the minimization runs over all possible decompositions, the definition $R_I(\rho)$ does not depend on the purification.

For the case when Eve performs general positive-operator valued measures (POVMs), we can first "purify" the measurement and consider projection measurement on a quantum state in a larger Hilbert space as $|\psi^{AEE'}\rangle$, where Alice has A and Eve has EE'. Therefore a similar proof for POVMs follows.

IV. VERIFYING THE PROPERTIES OF R

Now we show that the intrinsic randomness R_I, defined in Eq. 6, satisfies the properties of coherence measure listed in Table I. That is, the requirements of the measures for quantum coherence and intrinsic randomness are equivalent.

In the language of generating randomness, the requirement (C1) in Table I can be interpreted as saying that classical states generate no randomness. This is because an incoherent state δ, defined in Eq. 1, can be understood as a statistical mixture of classical states. We can easily verify that $R_I(\delta) = 0$, since

$R_I(\delta) \leqslant \sum_{i=1}^d p_i R_I(|i\rangle\langle i|) = 0$ from Eq. 1 and $R_I(\rho) \geqslant 0$ by definition. The stronger requirement (C1′) implies that any nonclassical states, which cannot be represented in the form of Eq. 1, could always be used to generate intrinsic randomness. Thus, this result answers why nonzero intrinsic randomness always indicates "quantumness" as discussed above. The proof for (C1′) is provided in Appendix A. We can also show that the upper bound of its intrinsic randomness is given by $R_I(\rho) \leqslant \log_2 d$. The maximally coherent state $|\Psi_d\rangle$, defined in Eq. 2, has the largest intrinsic randomness.

The requirement (C2) implies a monotonicity property of incoherent operations. In the corresponding randomness picture, incoherent operations can be understood as classical operations that map one zero intrinsic randomness (classical) state to another one. An interpretation of (C2a) is that such classical operations should not increase the randomness of a given state. While (C2b) requires that the randomness cannot increase on average when probabilistic strategies are considered. Let us quickly check why (C2b) is true for the pure state case, while leaving the proof for other cases in Appendix A. For a pure state ρ, the randomness measure $R_I(\rho)$ equals the relative entropy of coherence $C_{\text{rel,ent}}(\rho)$, whose monotonicity has been proved [10].

The convexity property (C3) can be understood as a requirement on the randomness generation process. In other words, randomness cannot increase on average by statistically mixing several states. With the convex roof definition of $R_I(\rho)$, given in Eq. 6, we can easily verify the convexity property (C3). The proof follows directly by considering a specific decomposition of $\rho = \sum_n p_n \rho_n$ in (C3). Note that the property (C2a) can be derived when (C2b) and (C3) are fulfilled, thus we also prove (C2a) for $R_I(\rho)$.

In summary, we prove that the intrinsic randomness $R_I(\rho)$ indeed measures the strength of coherence. A state with stronger coherence would therefore indicate larger randomness in measurement outcomes, and vice versa.

V. RANDOMNESS DISTILLATION

As mentioned above, when Alice performs a projective measurement P_I on N identical pure states $|\psi\rangle = \sum_i a_i |i\rangle$, she will obtain N i.i.d. random variables $A_1, A_2, \ldots, A_N$. For the state $|\psi\rangle$ that is not maximally coherent, the randomness of the measurement outcomes is biased. Then, as shown in Fig. 3(a), Alice can perform a randomness extraction process
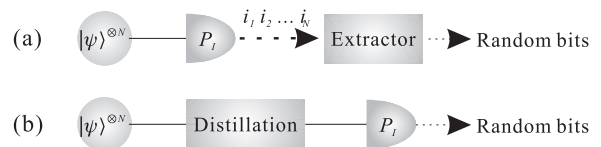

FIG. 3. Random number extraction and coherence distillation. The randomness extraction process can be replicated by first distilling the coherence of the quantum state. Measurement outcomes will directly produce uniformly random bits.

to transform the N biased random numbers to $l \approx N R_I(|\psi\rangle)$ almost uniformly distributed random bits.

We show in Fig. 3(b) that extraction can be equivalently performed before measurement. Now, extraction becomes a quantum procedure, which we call *quantum extraction*. Considering the equivalence between intrinsic randomness and quantum coherence, quantum extraction can be regarded as a procedure of *coherence distillation*. This concept resembles the distillation procedure of another (more popular) quantumness measure—entanglement [13].

With quantum extraction, we can first distill the input state $|\psi\rangle = \sum_i a_i |i\rangle$ into the maximally coherent state $|\Psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Then, we can directly obtain uniformly distributed random bits by measuring the maximally coherent state. For N copies of $|\psi\rangle$, it is shown in Appendix B that we can asymptotically obtain l copies of $|\Psi_2\rangle$, where l and N satisfy the following condition:

$$l/N \approx R_I(|\psi\rangle). \tag{7}$$

Taking a pure qubit input state as an example, the distillation procedure is summarized as follows:

(i) Prepare N copies of qubit state $|\psi\rangle^{\otimes N} = (\alpha|0\rangle + \beta|1\rangle)^{\otimes N}$, which can be binomially expanded on the computational basis. There are $N + 1$ distinct coefficients, $\beta^N, \alpha^1\beta^{N-1}, \ldots, \alpha^N$, corresponding to different subspaces that have the same number of $|0\rangle$ or $|1\rangle$.

(ii) Perform a projection measurement to distinguish between those subspaces. For the kth subspace, which has coefficient $\alpha^{N-k}\beta^k$, the measurement probability is given by $p_k = \binom{N}{k}|\alpha|^{2(N-k)}|\beta|^{2k}$. The resulting quantum state of the kth outcome corresponds to a maximally coherent state $|\Psi_{D_k}\rangle$ of dimension $D_k = \binom{N}{k}$.

(iii) Suppose that $2^r \leqslant D_k < 2^{r+1}$, then we can directly project onto the 2^r subspace and convert to r copies of $|\Psi_2\rangle$ as desired.

To see why r/N equals the randomness of $|\psi\rangle$ on average, we only need to take account of the operations that cause a loss of coherence. As shown in Appendix B, the only two projection measurements lose negligible amount of coherence, thus we asymptotically have $N R_I(|\psi\rangle) \approx r$.

In Appendix D, we further extend the definition of distillable coherence to mixed quantum states. Compared to the definition of the regularized entanglement of formation [23], we also define coherence of formation and conjecture that it equals the regularized intrinsic randomness measure,

$$R_I^\infty(\rho) = \lim_{N \to \infty} \frac{R_I(\rho^{\otimes N})}{N}. \tag{8}$$

VI. QUBIT EXAMPLE

Here, we give an example of the calculation of $R_I(\rho)$ for a qubit state ρ. We follow a method of deriving the EOF [13,18,19] and refer to Appendix C for details. Denote the Pauli matrices by $\sigma_i, \sigma_x, \sigma_y,$ and σ_z. When measured in the σ_z basis, the randomness $R_z(\rho)$ can be calculated by

$$R_z(\rho) = H\left(\frac{1 + \sqrt{1 - C_z^2}}{2}\right). \tag{9}$$

Here, the C_z term is defined as $C_z = |\sqrt{\eta_1} - \sqrt{\eta_2}|$, which resembles the concurrence [18], where η_1 and η_2 are the eigenvalues of the matrix $M = \rho\sigma_x\rho^*\sigma_x$. In the Bloch sphere representation, the value of C_z of a quantum state $\rho = (\sigma_i + n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)/2$ can be calculated by $C_z = \sqrt{n_x^2 + n_y^2}$. Compared with the l_1 norm coherence measure C_{l_1} defined in Eq. 4, we can easily check that $C_{l_1}(\rho)$ equals the coherence concurrence C_z for the qubit case. We conjecture that the coherence concurrence can be generalized to an arbitrary high-dimensional space by following a similar method to that used for the entanglement concurrence [24–26].

VII. DISCUSSION

As shown in Table II, there exist strong similarities between the frameworks of coherence and entanglement (see also Ref. [27]), our study can be regarded as an extension of the convex roof measure from entanglement to coherence. Similar to the case of EOF, as a convex roof measure for coherence, we expect our proposed measure to play an important role in the research of coherence.

For further research directions, it is interesting to extend the framework of entanglement to coherence. An incomplete list of comparison between the two are shown in Table II. For instance, it is interesting to see whether $C_{rel,ent}(\rho)$ and $R_I(\rho)$ are the unique lower and upper bounds of all coherence measures after regularization, and whether they can coincide. Another interesting and related question is that of quantifying the coherence for an unknown quantum state, similar to the task of using an entanglement witness for quantification. The coherence measure $R_I(\rho)$ given in Eq. 6 ensures the true randomness when measuring a state ρ in the I basis. Such a technique can be utilized to construct a semi-self-testing quantum random number generator. A straightforward way to do this is to first perform tomography on the to-be-measured state ρ and then estimate the randomness of the I basis measurement outcomes according to Eq. 6. As the coherence measure $R_I(\rho)$ quantifies the output randomness in a measurement, our result can also be applied in other randomness generation scenarios [38,43–45].

APPENDIX A: VERIFYING THE PROPERTIES OF *R*

The requirements of coherence measures are listed in Table I. The intrinsic randomness measure is defined by

$$R_I(\rho) = \min_{\{p_e, |\psi_e\rangle\}} \sum_e p_e R_I(|\psi_e\rangle), \tag{A1}$$

where the minimum runs over all possible decompositions of ρ, $\rho = \sum_e p_e |\psi_e\rangle\langle\psi_e|$ and $\sum_e p_e = 1$.

In this section, we will show that the intrinsic randomness measure $R_I(\rho)$ satisfies the requirements of coherence

TABLE II. Comparing the frameworks of coherence and entanglement. DI: device-independent; MDI: measurement-device-independent; QKD: quantum key distribution; QRNG: quantum random number generation.

Properties	Coherence	Entanglement
Classical operation	Inherent operation [10]	LOCC [13]
Classical state	Incoherent state, Eq. 1	Separable state
Distance measure	$C_{\mathrm{rel,ent}}(\rho)$, Eq. 3	Relative entropy distance [14]
Convex roof measure	$R_I(\rho)$, Eq. 6	EOF [13,18,19]
Distillation	Coherence distillation (Appendix B)	Entanglement distillation [16,28]
Formation (cost)	Coherence formation	Entanglement cost [16,23]
Foundation tests	Further research direction	Nonlocality tests [2,29]
Interconvertibility	[30,31]	Deterministic [32], stochastic [33]
Catalysis effect	Further research direction	Entanglement catalysis [34,35]
Witness	Further research direction	Entanglement witness (EW)
DI applications	Further research direction	DIQKD [36,37], DIQRNG [38]
MDI applications	Further research direction	MDIQKD [39,40], MDIEW [41,42]

measures. Here, we only show how to prove (C1′) and (C2b), the proofs for the other requirements can be found in the main text.

1. Proof of (C1′)

To prove that $R_I(\rho)$ satisfies (C1′), consider a state $\rho \notin \mathcal{I}$ that has $R_I(\rho) = 0$. From the definition of R_I, there exists a decomposition $\rho = \sum_e p_e |\psi_e\rangle\langle\psi_e|$ such that $R_I(|\psi_e\rangle\langle\psi_e|) = 0$ for all e. As any pure state with zero randomness is in the basis I, we have $|\psi_e\rangle = |i_e\rangle \in I$, and $\rho = \sum_e p_e |i_e\rangle\langle i_e|$, which belongs to the set $\mathcal{I}$, which is a contradiction.

2. Proof of (C2b)

As mentioned in the main text, the monotonicity requirement of (C2b) is satisfied for the pure state,

$$R_I(|\psi\rangle) \geqslant \sum_n p_n R_I(|\psi_n\rangle), \tag{A2}$$

where $|\psi_n\rangle = K_n |\psi\rangle / \sqrt{p_n}$, and $p_n = \mathrm{Tr}[K_n |\psi\rangle\langle\psi|]$. This is because for a pure state ρ, the intrinsic randomness $R_I(\rho)$ equals the relative entropy coherence measure $C_{\mathrm{rel,ent}}(\rho)$ [10], whose monotonicity has already been proved.

For a general mixed state ρ, suppose that the optimal decomposition that achieves the minimum in Eq. 6 is given by $\rho = \sum_e p_e |\psi_e\rangle\langle\psi_e|$. Then, we have

$$R_I(\rho) = \sum_e p_e R_I(|\psi_e\rangle). \tag{A3}$$

Now suppose that the incoherent operation defined in the main text is acted on ρ. What we need to prove is that

$$R_I(\rho) \geqslant \sum_n p_n R_I(\rho_n), \tag{A4}$$

where $\rho_n = K_n \rho K_n^\dagger / p_n$ and $p_n = \mathrm{Tr}[K_n \rho K_n^\dagger]$. Since $\rho = \sum_e p_e |\psi_e\rangle\langle\psi_e|$, we have

$$
\begin{aligned}
\rho_n &= \frac{K_n \rho K_n^\dagger}{p_n} \\
&= \sum_e \frac{p_e}{p_n} K_n |\psi_e\rangle\langle\psi_e| K_n^\dagger \\
&= \sum_e \frac{p_e}{p_n} p_{en} \rho_{en},
\end{aligned}
\tag{A5}
$$

where we denote $p_{en} = \mathrm{Tr}[K_n |\psi_e\rangle\langle\psi_e| K_n^\dagger]$ and $\rho_{en} = K_n |\psi_e\rangle\langle\psi_e| K_n^\dagger / p_{en}$, and we have $p_n = \sum_e p_e p_{en}$. Then, we can finish the proof

$$
\begin{aligned}
R_I(\rho) &= \sum_e p_e R_I(|\psi_e\rangle) \\
&\geqslant \sum_e p_e \sum_n p_{en} R_I(\rho_{en}) \\
&= \sum_n p_n \sum_e \frac{p_e p_{xn}}{p_n} R_I(\rho_{en}) \\
&\geqslant \sum_n p_n R_I\left(\sum_e \frac{p_e p_{en}}{p_n} \rho_{en}\right) \\
&= \sum_n p_n R_I(\rho_n),
\end{aligned}
\tag{A6}
$$

where the first inequality is based on the conclusion for pure states in Eq. (A2) and the last inequality is due to the convexity of R_I.

APPENDIX B: COHERENCE DISTILLATION PROCEDURE

A coherence distillation procedure refers to a series of incoherent operations by which a large number of identical partly coherent states can be transformed into a smaller number of maximally coherent states. In this section, we introduce a coherence distillation procedure for pure qubit states. With N copies of states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we show that we can asymptotically obtain l copies of $|\Psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$,

where l and N satisfy $l/N \approx R_I(|\psi\rangle)$. The derivation method can be generalized to an arbitrary dimension.

1. Qubit distillation

First we prepare MN copies of a partially coherent qubit state which will be uniformly divided into M groups. The initial state of each group can be expressed according to

$$|\psi\rangle^{\otimes N} = (\alpha|0\rangle + \beta|1\rangle)^{\otimes N}. \qquad (B1)$$

A binomial expansion on the computational basis contains $N+1$ distinct coefficients $\beta^N, \alpha^1\beta^{N-1}, \dots, \alpha^N$. Thus we can divide the original 2^N-dimensional Hilbert space into $N+1$ subspaces according to the coefficients. For the kth coefficient $\alpha^{N-k}\beta^k$, the corresponding kth subspace is a $D_k = C_N^k$ dimensional Hilbert space, whose bases are denoted by

$$\alpha^{N-k}\beta^k : \left\{ |e_1^k\rangle, |e_2^k\rangle, \cdots, |e_{D_k}^k\rangle \right\}. \qquad (B2)$$

When considering the computational basis, $|e_i^k\rangle$ $(i = , 1, 2, \dots, D_k)$ is an N-qubit basis with $(N-k)$ $|0\rangle$s and k $|1\rangle$s.

Next, we perform a projection measurement on $|\psi\rangle^{\otimes N}$ to the subspaces. In our case, the projection operator that maps onto the kth subspace is given by

$$P_k = |e_1^k\rangle\langle e_1^k| + |e_2^k\rangle\langle e_2^k| + \cdots + |e_{D_k}^k\rangle\langle e_{D_k}^k|. \qquad (B3)$$

The probability of obtaining the kth outcome is

$$p_k = C_N^k |\alpha|^{2N-2k}|\beta|^{2k}. \qquad (B4)$$

Note that as the coefficients for the expansion are the same, the postselection of the kth outcome corresponds to a maximally coherent state $|\Psi_{D_k}\rangle$ of dimension D_k.

If $D_k = 2^r$, we can directly convert to r copies of $|\Psi_2\rangle$ as desired. Or we can repeat this process M times, and take the tensor product of the postselected state to obtain a maximally coherent state of dimension D,

$$|\Psi_D\rangle = |\Psi_{D_{k_1}}\rangle|\Psi_{D_{k_2}}\rangle \cdots |\Psi_{D_{k_M}}\rangle, \qquad (B5)$$

where k_j is the outcome of the jth measurement, and the total dimension is $D = D_{k_1} D_{k_2} \cdots D_{k_M}$. The total dimension D will lie between 2^r and $2^r(1+\epsilon)$ $(0 < \epsilon < 1)$ for some power r. It can be proved [13] that as M increases, ϵ will asymptotically approach 0.

Therefore, we can perform a second projection measurement to the 2^r-dimensional Hilbert subspace and directly obtain a final state

$$|\Psi_2\rangle^{\otimes r} = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right)^{\otimes r}. \qquad (B6)$$

Using the above procedure, NM copies of a partly coherent qubit state $\alpha|0\rangle + \beta|1\rangle$ have been distilled into r copies of maximally coherent state $|\Psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

In the following, we will show that all the operations of the distillation protocol are incoherent operations. In addition, we will show that the number of distilled maximally coherent states r and the number of initial qubits MN satisfy the relation $NMR_I(|\psi\rangle) \approx r$.

2. Incoherent operations

Because the only operations are the two projective measurements, we only need to prove the following lemma.

Lemma. Suppose an n-dimensional Hilbert space has a complete basis $I_n = \{|1\rangle, |2\rangle, \dots, |n\rangle\}$. A projection measurement that divides I_n into its complementary subsets is an incoherent operations on the basis of I_n.

Proof. Suppose that the basis I_n is divided into m complementary subsets $I_{n_1}, I_{n_2}, \dots, I_{n_m}$, such that $I_{n_\alpha} \cap I_{n_\beta} = \emptyset$, for all $\alpha \neq \beta \in \{1, 2, \dots, m\}$, and $I_n = I_{n_1} \cup I_{n_2} \cup \cdots \cup I_{n_m}$. Denote the projector that projects onto the I_{n_α} subspace by P_α. Thus, we can show that the projection measurement is a set of Kraus operators $\{\hat{P}_\alpha\}$ that satisfy $\hat{P}_\alpha^\dagger \hat{P}_\beta = \delta_{\alpha,\beta}\hat{P}_\alpha$ and $\sum_\alpha P_\alpha = I_n$. To prove the projection measurement to be an incoherent operation, we additionally need to show that $\hat{P}_\alpha \mathcal{I}_n \hat{P}_\alpha^\dagger \subset \mathcal{I}_n$, where $\mathcal{I}_n$ is the set of all incoherent states that can be represented by $\delta = \sum_{i=1}^n \delta_i |i\rangle\langle i|$. As the definition of P_α, we have

$$P_\alpha|i\rangle = \delta(|i\rangle \in I_{n_\alpha})|i\rangle, \qquad (B7)$$

where $\delta(|i\rangle \in I_{n_\alpha}) = 1$ if $|i\rangle \in I_{n_\alpha}$ and $\delta(|i\rangle \in I_{n_\alpha}) = 0$ otherwise. Thus, we can show that for an arbitrary state $\delta = \sum_{i=1}^d \delta_i |i\rangle\langle i| \in \mathcal{I}_n$, we have

$$\hat{P}_\alpha \delta \hat{P}_\alpha^\dagger = \hat{P}_\alpha \sum_{i=1}^n \delta_i |a_i\rangle\langle a_i| \hat{P}_\alpha^\dagger$$
$$= \sum_{i=1}^n \delta_i \delta(|i\rangle \in I_{n_\alpha})|a_i\rangle\langle a_i| \in \mathcal{I}_n. \qquad (B8)$$

Therefore, we have proven that the operations in the distillation protocol are incoherent.

3. Coherence loss

To explain why we have $NMR_I(|\psi\rangle) \approx r$, we only need to consider the coherence loss during the distillation process. The initial state in each group can be rewritten as

$$|\psi\rangle^{\otimes N} = \sum_{k=0}^N \sqrt{C_N^k} \alpha^{N-k}\beta^k |\Psi_{D_k}\rangle, \qquad (B9)$$

where $|\Psi_{D_k}\rangle$ is a maximally coherent state of dimension D_k. Thus the density matrix of the initial state is

$$\rho = \sum_{k,k'} \sqrt{C_N^k}\sqrt{C_N^{k'}} \alpha^{N-k}\beta^k (\alpha^*)^{N-k'}(\beta^*)^{k'} |\Psi_k\rangle\langle\Psi_{k'}|. \quad (B10)$$

Because the coherence of ρ is defined by the von Neumann entropy of its diagonal terms, we first look at ρ^{diag}. That is,

$$\rho^{\text{diag}} = \sum_{i=1}^{2^N} \langle e_i|\rho|e_i\rangle |e_i\rangle\langle e_i|$$
$$= \sum_{i=1}^{2^N} \sum_{k,k'} \sqrt{C_N^k}\sqrt{C_N^{k'}} \alpha^{N-k}\beta^k (\alpha^*)^{N-k'}(\beta^*)^{k'}$$
$$\langle e_i|\Psi_k\rangle\langle\Psi_{k'}|e_i\rangle |e_i\rangle\langle e_i|. \qquad (B11)$$

Here we can see that when $k \neq k'$, $\langle e_i | \Psi_k \rangle \langle \Psi_{k'} | e_i \rangle = 0$. Therefore Eq. (B11) can be simplified as

$$\rho^{\text{diag}} = \sum_{k=0}^{N} C_N^k |\alpha|^{2N-2k} |\beta|^{2k} (|e_i\rangle\langle e_i|)^{\text{diag}} = \sum_{k=0}^{N} p_k \rho_k^{\text{diag}}.$$

(B12)

Here ρ^{diag} has the decomposition $\{p_k, \rho_k^{\text{diag}}\}$. Thus, we have

$$S(\rho^{\text{diag}}) = H(p_k) + \sum_{k=0}^{N} p_k S(\rho_k^{\text{diag}}),$$

(B13)

where $S(\rho^{\text{diag}})$ is the von Neumann entropy of ρ^{diag} and $H(p_k)$ is the Shannon entropy. Considering our coherence (intrinsic randomness) definition, Eq. (B13) is equivalent to

$$C(\rho) = H(p_k) + \sum_{k=0}^{N} p_k C(\rho_k),$$

(B14)

where $C(\rho)$ is the average initial coherence and $\sum_{k=0}^{N} p_k C(\rho_k)$ is the average coherence left after the first projection measurement. Therefore, the coherence loss in the first operation is

$$H(p_k) = -\sum_{k=0}^{N} p_k \log_2(p_k) \leqslant \log_2 N.$$

(B15)

The coherence loss for the second projection measurement can be easily estimated by $\log_2(1 + \epsilon) \approx \epsilon$. Thus the total coherence loss has an upper bound given by

$$M \log_2 N + \log_2(1 + \epsilon),$$

(B16)

which is negligible relative to the initial coherence $MNC(|\psi\rangle)$ when M and N are large.

APPENDIX C: QUBIT EXAMPLE

Here, we derive the intrinsic randomness formula of the qubit state. We denote the Pauli matrices by $\sigma_i, \sigma_x, \sigma_y, \sigma_z$. When measured in the σ_z basis, the intrinsic randomness for a pure qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is given by

$$R_z(|\psi\rangle) = H(|\alpha|^2) = H(|\beta|^2),$$

(C1)

where $H(p) = p \log p + (1 - p) \log(1 - p)$. If we define $n_x = \langle\psi|\sigma_x|\psi\rangle = \alpha^*\beta + \alpha\beta^*$ and $n_y = \langle\psi|\sigma_y|\psi\rangle = -i\alpha^*\beta + i\alpha\beta^*$, then it is easy to check that

$$R_z(|\psi\rangle) = H\left(\frac{1 + \sqrt{1 - n_x^2 - n_y^2}}{2}\right).$$

(C2)

For a general mixed state ρ, we can follow the method for deriving the entanglement of formation [19]. In this case, we need to first define $|\tilde{\psi}\rangle = \sigma_x|\psi^*\rangle = \beta^*|0\rangle + \alpha^*|1\rangle$, and the coherent concurrence by

$$C_z(|\psi\rangle) = |\langle\psi|\tilde{\psi}\rangle| = 2|\alpha\beta|.$$

(C3)

Then it is easy to check that

$$R_z(|\psi\rangle) = H\left(\frac{1 + \sqrt{1 - C_z^2}}{2}\right).$$

(C4)

The randomness $R_I(\rho)$ can be obtained according to Eq. (C2) by first calculating the coherent concurrence. Follow the method of deriving the entanglement of formation, the C_z value can be obtained by $C_z = |\sqrt{\eta_1} - \sqrt{\eta_2}|$, where η_1 and η_2 are the eigenvalues of the matrix $M = \rho\sigma_x\rho^*\sigma_x$. In the Bloch sphere representation, the value of C_z of a quantum state $\rho = (\sigma_i + n_x\sigma_x + n_y\sigma_y + n_z\sigma_z)/2$ can be calculated by

$$C_z = \sqrt{n_x^2 + n_y^2}.$$

(C5)

Compared to the l_1 norm coherence measure C_{l_1} [10], which is defined by the sum of the off-diagonal elements

$$C_{l_1}(\rho) = \sum_{i \neq j} |\rho_{ij}|,$$

(C6)

one can easily check that $C_{l_1}(\rho)$ equals the concurrence C_z for the qubit case. This is because

$$\begin{aligned}
C_{l_1}(\rho) &= |\langle 0|\rho|1\rangle| + |\langle 1|\rho|0\rangle| \\
&= \left|\frac{1}{2}(n_x - in_y)\right| + \left|\frac{1}{2}(n_x + in_y)\right| \\
&= \sqrt{n_x^2 + n_y^2}.
\end{aligned}$$

(C7)

APPENDIX D: GENERAL DEFINITIONS FOR COHERENCE MEASURE

Generally, when considering the intrinsic randomness of multiple copies of ρ, we can define the average intrinsic randomness in a manner similar to the definition of entanglement cost [15,16,23] by

$$R_I^C(\rho) = \inf\left\{ r : \lim_{N \to \infty}\left[\inf_{\Phi_{\text{ICPTP}}} D(\rho^{\otimes N}, \Phi_{\text{ICPTP}}(|\Psi_{2^{rN}}\rangle)) \right] = 0 \right\},$$

(D1)

where $D(\rho_1, \rho_2)$ is a suitable measure of distance, which, for instance, could be the trace norm. In this case, the intrinsic randomness is understood as the average coherence cost in preparing ρ. Compared to the definition of the regularized entanglement of formation [23], we conjecture that $R_I^C(\rho)$ equals the regularized intrinsic randomness measure,

$$R_I^\infty(\rho) = \lim_{N \to \infty} \frac{R_I(\rho^{\otimes N})}{N}.$$

(D2)

In the other direction, we can apply intrinsic operations to transform N nonmaximally coherent copies of ρ to l maximally coherent state $|\Psi_2\rangle$. Similarly, we can define the distillable coherence by the supremum of l/N over all possible distillation protocols [15,16,28],

$$R_I^D(\rho) = \sup\left\{ l : \lim_{N \to \infty}\left[\inf_{\Phi_{\text{ICPTP}}} D(\Phi_{\text{ICPTP}}(\rho^{\otimes N}) \right.\right.$$
$$\left.\left. - |\Psi_{2^{lN}}\rangle) \right] = 0 \right\}.$$

(D3)

This distillable coherence $R_I^D(\rho)$ can thus be considered as the amount of intrinsic randomness when a quantum extractor is performed before measurement, as shown in the main text. For a general reasonable regularized coherence measure $C_I^\infty(\rho)$

similar to Eq. (8), we conjecture that the two measures R_I^D and R_I^C are equivalent for all possible distance measures. They serve as two extremal measures, such that $R_I^D(\rho) \leqslant C_I^\infty(\rho) \leqslant R_I^C(\rho)$ for all regularized coherence measures $C_I^\infty(\rho)$.

[1] M. Born, Z. Phys. **37**, 863 (1926).

[2] J. S. Bell, *On the Einstein-Podolsky-Rosen Paradox. Physics 1, 195–200 (1964)*, Speakable and Unspeakable in Quantum Mechanics (Cambridge University, New York, 1987).

[3] V. Giovannetti, S. Lloyd, and L. Maccone, Nat. Photon. **5**, 222 (2011).

[4] N. Lambert, Y.-N. Chen, Y.-C. Cheng, C.-M. Li, G.-Y. Chen, and F. Nori, Nat. Phys. **9**, 10 (2013).

[5] R. Glauber, Phys. Rev. **131**, 2766 (1963).

[6] E. Sudarshan, Phys. Rev. Lett. **10**, 277 (1963).

[7] S. Luo, Theor. Math. Phys. **143**, 681 (2005).

[8] J. Åberg, arXiv:quant-ph/0612146.

[9] A. Monras, A. Chęcińska, and A. Ekert, New J. Phys. **16**, 063041 (2014).

[10] T. Baumgratz, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **113**, 140401 (2014).

[11] J. Åberg, Phys. Rev. Lett. **113**, 150402 (2014).

[12] D. Girolami, Phys. Rev. Lett. **113**, 170401 (2014).

[13] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[14] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[15] M. B. Plbnio and S. Virmani, Quantum Info. Comput. **7**, 1 (2007).

[16] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[17] W. H. Zurek, Nat. Phys. **5**, 181 (2009).

[18] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[19] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[20] The definitions of coherence and intrinsic randomness are based on a specific computational basis. In this perspective, the quantum feature can be quantified by the superposition strength on the measurement basis. Alternatively, we can define similar quantumness as the ability of measurements. For an arbitrary pure quantum state, if we can choose the measurement basis that is complementary to the state, a quantum feature similar to coherence can also be maximally revealed. The definitions of coherence based on the property of quantum state with a given measurement basis and the property of measurement is similar to the relationship between the pictures of Schrödinger and Heisenberg. The current definition of coherence thus follows from the routine of the Schrödinger picture.

[21] C. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).

[22] A. Rényi, in *Fourth Berkeley Symposium on Mathematical Statistics and Probability* (University of California, Berkeley, 1961), p. 547.

[23] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A: Math. Gen. **34**, 6891 (2001).

[24] P. Rungta, V. Bužek, C. M. Caves, M. Hillery, and G. J. Milburn, Phys. Rev. A **64**, 042315 (2001).

[25] K. Audenaert, F. Verstraete, and B. De Moor, Phys. Rev. A **64**, 052304 (2001).

[26] P. Badziag, P. Deuar, M. Horodecki, P. Horodecki, and R. Horodecki, J. Modern Optics **49**, 1289 (2002).

[27] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, Phys. Rev. Lett. **115**, 020403 (2015).

[28] E. M. Rains, Phys. Rev. A **60**, 173 (1999).

[29] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[30] S. Du, Z. Bai, and X. Qi, arXiv:1504.02862.

[31] S. Du, Z. Bai, and Y. Guo, Phys. Rev. A **91**, 052120 (2015).

[32] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

[33] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).

[34] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).

[35] J. Eisert and M. Wilkens, Phys. Rev. Lett. **85**, 437 (2000).

[36] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS '98 (IEEE Computer Society, Washington, 1998) p. 503.

[37] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[38] U. Vazirani and T. Vidick, in *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12 (ACM, New York, 2012) p. 61.

[39] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[40] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[41] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013).

[42] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **112**, 140506 (2014).

[43] R. Colbeck, arXiv:0911.3814.

[44] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photon. **4**, 711 (2010).

[45] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).