

Information-theoretic meaning of quantum information flow and its applications to amplitude amplification algorithms

Sudipto Singha Roy^{1,2} and Joonwoo Bae^{3,*}

¹*Instituto de Física Teórica, UAM-CSIC, Universidad Autónoma de Madrid, Cantoblanco, Madrid, Spain*

²*Department of Applied Mathematics, Hanyang University (ERICA), 55 Hanyangdaehak-ro, Ansan, Gyeonggi-do 426-791, Korea*

³*School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Korea*



(Received 4 June 2018; revised manuscript received 3 June 2019; published 3 September 2019)

The advantages of quantum information processing are in many cases obtained as consequences of quantum interactions, especially for computational tasks where two-qubit interactions are essential. In this work, we establish the framework of analyzing and quantifying loss or gain of information on a quantum system when the system interacts with its environment. We show that the information flow, the theoretical method of characterizing (non-)Markovianity of quantum dynamics, corresponds to the rate of the minimum uncertainty about the system given quantum side information. Thereafter, we analyze the information exchange among subsystems that are under the performance of quantum algorithms, in particular, the amplitude amplification algorithms where the computational process relies fully on quantum evolution. Different realizations of the algorithm are considered, such as (i) quantum circuits, (ii) analog computation, and (iii) adiabatic computation. It is shown that, in all the cases, our formalism provides insight into the process of amplifying the amplitude from the information flow or leakage on the subsystems.

DOI: [10.1103/PhysRevA.100.032303](https://doi.org/10.1103/PhysRevA.100.032303)

I. INTRODUCTION

Interactions between quantum systems are fundamental in quantum information processing. Together with single-qubit operations, two-qubit interactions are significant for quantum evolution to perform computational tasks [1–5]. Moreover, interactions with measurement devices are needed for one to learn about which state a quantum system has been prepared in [6]. The theory of open quantum systems has provided the natural framework for understanding quantum interactions by considering realistic physical systems along the line and also offers useful theoretical tools for the purpose, see for instance [7].

In recent progress in the theory of open quantum systems, significant efforts have been devoted to the characterization of the quantum interactions in Markovian quantum dynamics [8–11]. Remarkably, an operational characterization has been shown [8,11]. The notion of *quantum information flow* has been introduced as the operational quantity such that its non-increasing behavior is asserted as the signature of Markovian quantum dynamics [8]. Conversely, if the distinguishability increases during the course of evolution, it may indicate information backflow, i.e., from environment to system, which allows one to conclude non-Markovian quantum dynamics. Since the characterization is operational with quantum distinguishability in terms of minimum-error state discrimination, the backflow can be experimentally detected without verification of quantum dynamics [12]. The backflow can also be used to define the degree of memory effects [13].

We here establish the information-theoretic framework of finding loss and gain of information on a quantum system. We show that the information flow over time, which we introduce as information leakage, corresponds to the maximal classical information leaked out by quantum interactions in a single-shot scenario. This in fact corresponds to the single-shot capacity of a quantum-to-classical channel. We then apply the framework to quantum interactions taken place during quantum evolution for computational tasks, in particular the algorithm of amplitude amplification that only relies on quantum evolution without classical dynamics. For this purpose, we consider three inequivalent realizations of the given algorithm with same efficiency, viz. (1) quantum circuits, (2) analog computation with Hamiltonian dynamics, and (3) adiabatic computation. It is shown that during the execution of the quantum algorithm in all cases, the amplitude of the target state and the information leakage have a similar profile, which provides a scope to analyze the process of amplifying amplitude from the information flow on the subsystems. Therefore, our findings reveal the importance of studying information flow not only to characterize the open quantum systems but also to unveil the role of quantum interactions in the advantages of quantum information processing.

II. FORMALISM

Let us begin with the information flow for a dynamical map Λ_t for time t ,

$$\sigma_t(\Lambda_t) = \max_{\rho_0, \rho_1} \frac{d}{dt} D(\Lambda_t[\rho_0], \Lambda_t[\rho_1]), \quad (1)$$

*joonwoo.bae@kaist.ac.kr

where the trace distance is denoted by $D(\rho, \sigma) = \|\rho - \sigma\|_1/2$ with $\|A\|_1 = \text{tr}\sqrt{A^\dagger A}$ [8]. Note that the distance measure is contractive: $D(\Lambda[\rho_0], \Lambda[\rho_1]) \leq D(\rho_0, \rho_1)$ for a quantum channel Λ and states ρ_0 and ρ_1 . The trace distance is directly related to optimal state discrimination [14–16], which can be seen as a game as follows. Alice prepares a quantum state ρ_0 or ρ_1 with equal *a priori* probabilities $1/2$, and sends it to Bob. His task is to make a guess for which he prepares two-outcome measurement $\{M_0, M_1\}$. The optimal measurement gives rise to the highest probability of making a correct guess, called the guessing probability [14–16] as

$$p_{\text{guess}}(\{\rho_0, \rho_1\}) = [1 + D(\rho_0, \rho_1)]/2. \quad (2)$$

If quantum states evolve under a dynamical map Λ_t , we write by $p_{\text{guess}}(\{\Lambda_t[\rho_0], \Lambda_t[\rho_1]\})$ the guessing probability under the channel at time t .

The scenario of optimal state discrimination can be equivalently addressed with the following state shared by Alice and Bob [17]:

$$\rho_{AB} = \frac{1}{2}|0\rangle\langle 0|^{(A)} \otimes \rho_0^{(B)} + \frac{1}{2}|1\rangle\langle 1|^{(A)} \otimes \rho_1^{(B)}. \quad (3)$$

Alice is with postmeasurement states, perfectly distinguishable ones, that label Bob's quantum states: two parties share classical-quantum (cq) correlations. The minimum uncertainty about Alice's classical value given Bob's quantum states, or equivalently, the maximal information about Alice given Bob, in a single-shot scenario, i.e., per the cq state in Eq. (3), can be quantified by the conditional min-entropy [18], $H_{\min}(A|B)_{\rho_{AB}} = -\inf_{w_B} \inf\{\lambda : \rho_{AB} \leq 2^\lambda (\text{id}_A \otimes w_B)\}$. Now, Bob aims to find the measurement to minimize the uncertainty about Alice.

It turns out that the optimal measurement can be identified by optimal state discrimination, see Eq. (2). For the cq state in Eq. (3), we have [17]

$$H_{\min}(A|B)_{\rho_{AB}} = -\log_2 p_{\text{guess}}(\{\rho_0, \rho_1\}). \quad (4)$$

In other words, the conditional min-entropy $H_{\min}(A|B)$ quantifies the maximal classical information about Alice by Bob's measurement in a single-shot scenario. When quantum states are sent to be Bob through a quantum channel \mathcal{N} and the cq state is given by $\text{id} \otimes \mathcal{N}(\rho_{AB})$ with state ρ_{AB} in Eq. (3), the conditional min-entropy is naturally related to the *single-shot ϵ -error capacity of a quantum-to-classical channel*, denoted by $C_\epsilon^{(1)}$ [19]. To be precise, $C_\epsilon^{(1)}(\mathcal{N}) = \sup\{\log M : \exists C = (M, \varphi, \Pi), p_{\text{guess}} \geq 1 - \epsilon\}$, where C denotes a collection of an encoding φ of M messages to quantum states, and of a measurement Π performed after the channel \mathcal{N} . The capacity denotes the maximal classical information that can be transmitted by a single use of the channel \mathcal{N} with an error less than ϵ on average. Note that $C_\epsilon^{(1)}(\mathcal{N}) \leq -H_{\min}(A|B)_{\text{id} \otimes \mathcal{N}(\rho_{AB})}$ with a cq state ρ_{AB} [19].

From the relations of the information flow, the guessing probability, and the conditional min-entropy, it is straightforward to find the information-theoretic interpretation of the information flow with the conditional min-entropy, which has its own meaning in a single-shot scenario. From Eqs. (1), (2), and (4), one can derive the following

Proposition. The information flow for a dynamical map Λ_t is given by

$$\sigma_t(\Lambda_t) = -c p_{\text{guess}}^* \max_{\rho_0, \rho_1} \frac{d}{dt} H_{\min}(A|B)_{(\text{id} \otimes \Lambda_t)\rho_{AB}}, \quad (5)$$

where $c = 2(\log_2 e)^{-1}$ and $p_{\text{guess}}^* = p_{\text{guess}}(\Lambda_t[\rho_0], \Lambda_t[\rho_1])$ for cq state $(\text{id} \otimes \Lambda_t)\rho_{AB}$.

Let us explain the interpretation of the information flow with the conditional min-entropy, as follows. On the one hand, for $\sigma_t(\Lambda_t) \leq 0$ the min-entropy increases or remains the same, i.e., the uncertainty about system A does not diminish. Therefore, information can only leak out from the system to the environment. We note that the quantity $-(c p_{\text{guess}}^*)^{-1} \sigma(\Lambda_t)$ from Eq. (5) is equal to the rate of the conditional min-entropy that quantifies the uncertainty in terms of bits. Thus, we recover the interpretation in Ref. [8] that the loss of distinguishability $\sigma_t(\Lambda_t) \leq 0$ implies no flow of information from environment to system, which has been suggested as the characterization of Markovian quantum dynamics.

On the other hand, if $\sigma_t(\Lambda_t) > 0$, the rate of the conditional min-entropy is negative and the uncertainty about A decreases in time. Hence, given the quantum system B under a dynamical map Λ_t , the longer it evolves, the more one learns about system A , that is, information gain. This has been interpreted as backflow, i.e., from the environment to the system, which has been suggested as a signature of non-Markovianity.

The definition of Markovianity proposed in Ref. [8] can be therefore reformulated as the condition of loss or gain of information on a system measured by min-entropy. This also means that, in the view of information processing, the definition is relevant in a single-shot scenario. Since the information flow defines the rate of the uncertainty, we introduce the single-shot information leakage for the quantification of the loss of information during a quantum dynamics as follows.

Definition. The *single-shot information leakage* on system S evolving under a dynamical map Λ_t for a time interval $[t_1, t_2]$ can be quantified by the information flow

$$L_{t_1, t_2}^{(S)}[\Lambda_t] = - \int_{t_1}^{t_2} (c p_{\text{guess}}^*)^{-1} \sigma(\Lambda_t) dt, \quad (6)$$

where the guessing probability p_{guess}^* is computed with two quantum states in the information flow $\sigma_t(\Lambda_t)$.

For $[t_1, t_2]$, if the information flow is nonpositive $\sigma_t \leq 0$, information can only leak out of the system and the loss is quantified by $L_{t_1, t_2}^{(S)}[\Lambda_t]$ bits. Otherwise, if $\sigma_t > 0$, we have negative-valued information leakage, meaning information gain of the system from the environment. Therefore, the framework has been established for quantifying information leakage by quantum interactions on a system. It is shown that loss and gain of information in terms of conditional min-entropy coincide with the characterization of Markovianity in Ref. [8].

III. APPLICATION: AMPLITUDE AMPLIFICATION ALGORITHM

In what follows, we are motivated to exploit the approach of open quantum systems to investigate quantum interactions taken place during quantum evolution for computational tasks, that is, quantum algorithms. We investigate the information

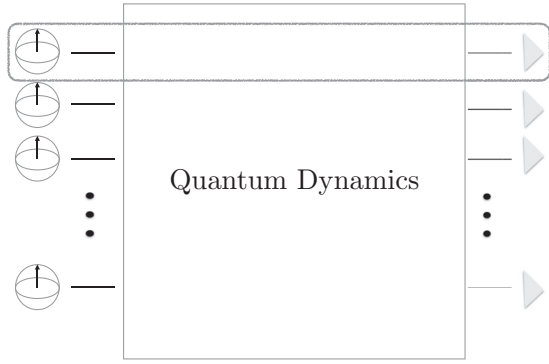


FIG. 1. An amplitude amplification algorithm is composed of state preparation, quantum dynamics, and measurement. A quantum-to-classical channel is defined from the preparation of quantum states to measurement.

exchange between subsystems under quantum algorithms, for which distinct physical implementations are considered, (i) quantum circuit based evolution, (ii) analog computation by Hamiltonian dynamics, and (iii) adiabatic computation. As the information leakage is valid for quantum evolution, we restrict the consideration to quantum algorithms relying only on quantum dynamics. For these reasons, we consider the quantum algorithm for amplitude amplification [20–22]. Note that other well-known algorithms such as the prime number factorization [23] contains both quantum and classical evolution. It is also worth mentioning that the information leakage in a single-shot scenario is well fitted for quantum algorithms, in the sense that (i) quantum algorithms cannot be repeated many times and (ii) a quantum-to-classical channel is naturally defined from quantum dynamics to measurement, see Fig. 1.

The algorithm for amplitude amplification outperforms the classical counterpart with the quadratic speedup that turns out to be optimal [24], see also Refs. [25,26]. It is also a good instance that can be realized in different physical models, which are equivalent in terms of computation. In all cases, the initialization works by preparation of the equal superposition of all items

$$|\psi_n\rangle = H^{\otimes n}|0\rangle^{\otimes n} = N^{-1/2} \sum_{k=1}^N |k\rangle,$$

where H denotes the Hadamard gate and $N = 2^n$. Let $|w\rangle$ denote the target state, and the quantum algorithm amplifies its amplitude from $N^{-1/2}$ to a number sufficiently close to 1 so that the measurement in the computational basis finds the target w with a high probability.

First, the algorithm in a quantum circuit is realized by successively applying the Grover iteration $U_G = -H^{\otimes n}G_0H^{\otimes n}G_w$, where G_w applies a query to the oracle such that $G_w|a\rangle = (-1)^{a \cdot w}|a\rangle$ and $G_0 = I - 2|0\rangle\langle 0|^{\otimes n}$ [20]. A single iteration U_G increases the amplitude by $O(N^{-1/2})$. Repeating the iteration $O(N^{1/2})$ times, the resulting state is sufficiently close to the target one, i.e., $(U_G)^{O(N^{1/2})}|\psi\rangle \approx |w\rangle$.

Second, the analog computation implements the dynamics of the Hamiltonian $\mathcal{H} = E(\mathcal{H}_w + \mathcal{H}_0)$ for some constant E , where $\mathcal{H}_w = |w\rangle\langle w|$ the oracular one and

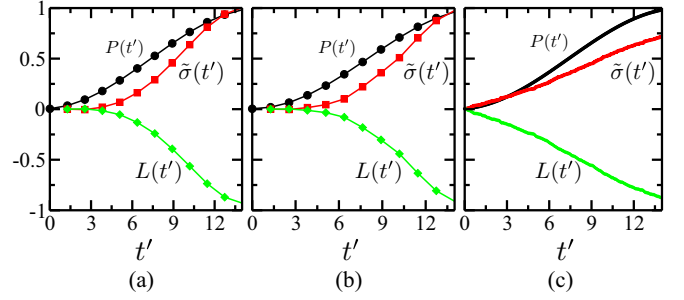


FIG. 2. Information flow (red) over time, the probability of finding the target (black), and the information leakage (green) on a single qubit are shown for algorithms with 8 qubits: (a) the circuit based algorithm, (b) analog computation, and (c) adiabatic computation. See the main text.

$\mathcal{H}_0 = |\psi_n\rangle\langle\psi_n|$ [21]. The quantum state at time t is then given by $|\psi(t)\rangle = e^{-i\mathcal{H}t}|\psi_n\rangle$. For $t = O(N^{1/2})$, the resulting state reaches the target state with certainty.

Third, the algorithm can be realized by adiabatic evolution from the initial Hamiltonian $\mathcal{H}(t=0) = \mathbb{I} - \mathcal{H}_0$ to the final one $\mathcal{H}(t=T) = \mathbb{I} - \mathcal{H}_w$, for which one needs an interpolation function $f(t)$

$$\mathcal{H}(t) = f(t)\mathcal{H}(t=0) + [1 - f(t)]\mathcal{H}(t=T)$$

such that it evolves adiabatically from the initial state to the target in the ground energy level. The adiabatic condition guarantees no cross from the ground to other energy levels. With the choice of

$$f(t) = \frac{1}{2} - \frac{1}{2} \left(\frac{1}{\sqrt{N-1}} \tan \frac{2\epsilon t \sqrt{N-1}}{N} - \tan^{-1} \sqrt{N-1} \right),$$

suppressing the transition probability less than ϵ^2 , the target state can be found in the ground energy level in time $T = \sqrt{N}\pi/(2\epsilon)$.

In all cases, the dynamical map on a single qubit can be found as

$$\Lambda_t(\rho) = \text{tr}_{j:n-j} U_{\text{amp}}(t)(\rho \otimes |\psi_{n-1}\rangle\langle\psi_{n-1}|) U_{\text{amp}}^\dagger(t), \quad (7)$$

where $\text{tr}_{j:n-1}$ denotes tracing out $n-1$ qubits but the j th qubit, and $U_{\text{amp}}(t)$ denotes quantum evolution for amplitude amplification from the aforementioned implementation.

The probability of finding the target state at time t is straightforwardly the measure of the computational speedup: it is amplified from $N^{-1/2}$ to the unit with the quadratic speedup. In Fig. 2, we plot the probability of the target, the information flow, and the information leakage for $n = 8$ qubits. $P(t)$ denotes the probability of finding the target item at time t , $L(t)$ the information leakage for the time interval $[0, t]$, and the information over time, $\tilde{\sigma}(t) = -(cp_{\text{guess}}^*)^{-1}L(t)$, in which the slope of $\tilde{\sigma}(t)$ is found as the information flow. The information flow is positive at all times and consequently information leakage is negative, which means gain of information on individual qubits at all times during the evolution. Thus, the dynamics is non-Markovian at all times. It is found that during the evolution, the information flow over time and the probability of finding the target both increase in time. This holds true for all types of physical implementation of the

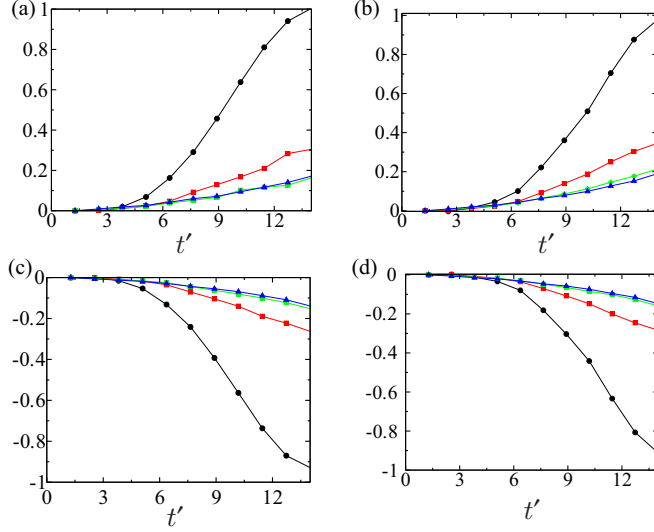


FIG. 3. Information flow over time and information leakage on a single qubit shown for amplitude amplification algorithms with system sizes $n_S = 1$ (black circles), 2 (red squares), 3 (green diamonds), and 4 (blue triangles) for the circuit based algorithm [(a) and (c)], and analog computation [(b) and (d)].

quantum algorithm. It is worth pointing out that the analysis made above provides a scope to elucidate the process of amplifying the amplitude for the total system in terms of the information flow as well as the information leakage on subsystems. The information flow on a larger subsystem, two- and more qubits (as depicted in Fig. 4), also shows similar behavior up to scaling, see Fig. 3.

The role of entanglement during quantum algorithms has been also elucidated [27,28]. Entanglement, one of the consequences of quantum interactions, is a general resource for quantum information processing in the sense that it can be applied to other information tasks. In fact, local operations on highly entangled states with classical communication only can

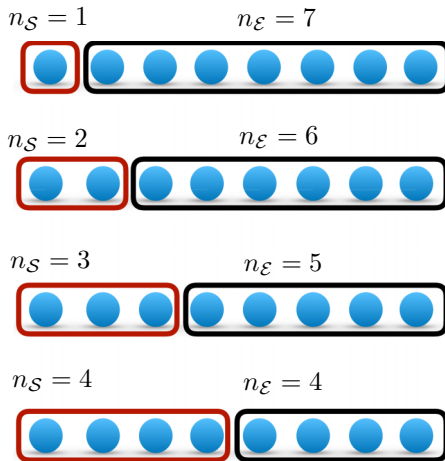


FIG. 4. For n qubits under quantum algorithms, a subsystem of n_S qubits is considered. The dynamical map on n_S qubits can be identified, and the information flow by the quantum interaction between system (S) and environment (E) can be computed.

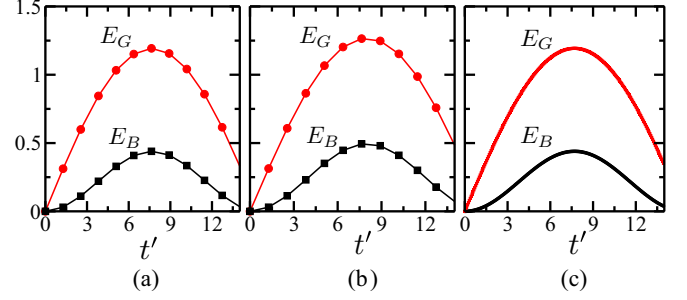


FIG. 5. Entanglement generation during the amplitude amplification algorithms for $n = 8$ is computed for (a) the circuit based algorithm, (b) analog computation, and (c) adiabatic computation. The bipartite concurrence (black) in the partition $1 : n - 1$ and the multipartite concurrence (red) are plotted. Entanglement generation is peaked at the midst of the running time.

perform universal quantum computation [29]. The converse is, however, not yet clear if entanglement is necessarily generated in a quantum algorithm and can lead to quantum advantages. For instance, entanglement is not necessarily generated in the Deutsch-Jozsa algorithm [30].

Entanglement generation can be analyzed during the amplitude amplification algorithms. The bipartite entanglement is computed with the concurrence in the bipartition $1 : n - 1$ qubits [31–33]. The global entanglement E can be computed with the multipartite concurrence [34],

$$E(|\psi\rangle_{1,\dots,n}) = 2^{1-\frac{n}{2}} \left[(2^n - 2) - \sum_i \text{Tr}(\rho_i^2) \right]^{-1/2},$$

where the sum is taken over all $2^n - 2$ reduced states. In Fig. 5, entanglement generation is plotted for $n = 8$ for the measures. In both cases, entanglement generation peaks at the midst of the running time up to scaling. Hence, while the information flow and information leakage show good agreement with the process of amplifying the amplitude, entanglement generation does not.

IV. CONCLUSION

In conclusion, our results interrelate information flow as defined in the theory of open quantum systems, entropic quantities from information theory, and the advantages of quantum information applications. We have presented the framework of analyzing information exchange between interacting quantum systems based on the information-theoretic meaning of the information flow of open quantum systems. The single-shot information leakage that quantifies information leaked out on a system is introduced, which also provides the quantification of the quantum-to-classical transition in a single-shot scenario. The devised framework is applied to the investigation of quantum interactions that lead to computational speedup in quantum algorithms. The algorithm of amplitude amplification is considered in distinct physical implementations, i.e., circuit based, analog computation, and adiabatic computation. Although they are equivalent in the view of computational processing, we have made careful analysis on

the quantum interactions to understand them in the angle of open quantum systems.

We note that our analysis is valid for algorithms that rely only on quantum evolutions since the information flow is introduced for quantum dynamics. In future investigations, it would be desirable to derive the information leakage in a composable manner that can be consistently applied to both quantum and classical systems. It is envisaged that the information flow analysis can be made for quantum-classical hybrid algorithms, such as the period finding [35] and prime number factorization [23] algorithms.

Finally, we discuss the definition of Markovianity, its interpretation, and the divisibility of dynamical maps. For technical simplicity, suppose that a dynamical map Λ_t is invertible although the assumption could be relaxed [36–38]. The map is called k divisible if there exists a k -positive map $\Lambda_{t,s}$ that allows the composition $\Lambda_t = \Lambda_{t,s} \circ \Lambda_s$, $\forall s \in [0, t]$ [10]. The condition $\sigma_t(\Lambda_t) \leq 0$ is equivalent to the 1-divisibility of the map Λ_t , thus, called P divisible [39]. If the propagator $\Lambda_{t,s}$ is completely positive, the map Λ_t is called CP divisible [9,39]. The k divisibility can also be characterized in an operational way in general, similar to the information flow [11]. One may point out that the definition of Markovianity may vary for divisible maps [8–10]. We here remark that among k -divisible maps from P- to CP-divisible ones, the single-shot information leakage in Eq. (5) is derived from the information flow proposed in Ref. [8], i.e., P-divisible maps, with close relationship to the quantum-to-classical channel capacity. It would be interesting to find distinct meanings of the different divisible maps from an information-theoretic view.

ACKNOWLEDGMENTS

S.S.R. acknowledges the hospitality of KAIST, Daejeon, Korea. This work is supported by National Research Foundation of Korea (NRF-2019M3E4A1080001), the KIST Institutional Program (2E26680-18-P025), and the Ministry of Science and ICT, Korea, under an ITRC Program (IITP-2019-2018-0-01402).

APPENDIX

We here provide the detailed description of the analysis of information leakage and information flow during the execution of the discrete- and continuous-time amplitude amplification algorithms [20,21]. Among n qubits in the algorithms, we consider subsystems of n_S qubits, i.e., across various bipartitions. Let n_E denote the number of qubits in the environment. Note also that the process of the algorithms is invariant under permutation of qubits.

In the amplitude amplification algorithms, the initial state is prepared as the n -qubit quantum state $|\psi_n\rangle = |+\rangle^{\otimes n}$ where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, in which 2^n states are uniformly superposed. Let $|w\rangle$ denote the target state, where w is the target string that we want to obtain at the end. Since measurement is performed in the computational basis, the probability of finding the target state in the initialization is given by $1/2^n$. The algorithms aim to amplify the amplitude of the target state

so that, once the measurement is performed, the probability of finding the target state is sufficiently close to 1.

As shown in the main text, we here consider the case $n = 8$ throughout. In what follows, let us consider subsystems from a single to a few qubits.

1. Information flow

Let us first consider a subsystem of a single qubit in the bipartition $1 : n - 1$. That is, we analyze how quantum interactions between a single qubit and the rest lead to gain or loss of information on the qubit. The single qubit we consider as a system is prepared initially in state $\rho_S(0) = |+\rangle\langle+|$ and other qubits regarded as environment in $\rho_E(0) = |+\rangle\langle+|^{\otimes n-1}$ where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

The amplitude amplification algorithms apply unitary transformation $U_{SE}(t)$, which is given by a sequence of Grover iterations for discrete-time dynamics or Hamiltonian evolution for the continuous-time case. Then, at time t we have

$$\rho_{SE}(t) = U_{SE}(t)[\rho_S(0) \otimes \rho_E(0)]U_{SE}^\dagger(t).$$

The state at $t = O(2^{n/2})$ is sufficiently close to the target one $|w\rangle$. For the discrete-time algorithm, the dynamics is given by

$$U_{SE}(t) = \prod_{i=1}^t U_G, \quad \text{with} \quad U_G = -H^{\otimes n} G_0 H^{\otimes n} G_w, \quad (\text{A1})$$

where H denotes the Hadamard transformation, $G_0 = I - 2|0\rangle\langle 0|^{\otimes n}$, and $G_w|a\rangle = (-1)^{a \cdot w}|a\rangle$. Note that G_0 is the inversion to the state $|0\rangle^{\otimes n}$, and G_w can selectively make inversion to the target state by calling the oracle. Since we have n qubits, the unitary transformation has a representation in a $2^n \times 2^n$ matrix, as follows

$$U_G = \begin{bmatrix} \frac{-1}{2^{n-1}} + 1 & \frac{1}{2^{n-1}} & \frac{1}{2^{n-1}} & \cdots & \frac{1}{2^{n-1}} \\ \frac{-1}{2^{n-1}} & \frac{1}{2^{n-1}} - 1 & \frac{1}{2^{n-1}} & \cdots & \frac{1}{2^{n-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{-1}{2^{n-1}} & \frac{1}{2^{n-1}} & \frac{1}{2^{n-1}} & \frac{1}{2^{n-1}} & \frac{1}{2^{n-1}} - 1 \end{bmatrix}.$$

For the continuous-time algorithm [21], the unitary transformation is given by

$$U_{SE}(t) = e^{-it\mathcal{H}}, \quad \text{with} \quad \mathcal{H} = E(|\psi_n\rangle\langle\psi_n| + |w\rangle\langle w|), \quad (\text{A2})$$

with E a constant. Then, the dynamical map Λ_t on a single qubit can be characterized by

$$\rho_S(t) = \Lambda_t[\rho_S(0)] = \text{tr}_E U_{SE}(t)[\rho_S(0) \otimes \rho_E(0)]U_{SE}^\dagger(t), \quad (\text{A3})$$

where $U_{SE}(t)$ can be found in Eqs. (A1) and (A2) for discrete- and continuous-time evolution, respectively. So far, we have characterized the dynamical map on a single qubit under the amplitude amplification algorithms.

For the dynamical map obtained in Eq. (A3), we can compute the information flow

$$\sigma_t(\Lambda_t) = \max_{\rho_0, \rho_1} \frac{d}{dt} D(\Lambda_t[\rho_0], \Lambda_t[\rho_1]), \quad (\text{A4})$$

where trace distance is denoted by $D(\rho, \sigma) = \|\rho - \sigma\|_1/2$ with $\|A\|_1 = \text{tr}\sqrt{A^\dagger A}$ [8]. In Ref. [40], it is shown that the maximization can be achieved with a pair of orthogonal states.

It therefore suffices to consider a pair of qubit states $\rho_0 = |\psi\rangle\langle\psi|$ and $\rho_1 = |\psi^\perp\rangle\langle\psi^\perp|$. We generate 10^6 arbitrary pure qubit states $|\psi\rangle$ uniformly over Haar measure and compute the information flow.

2. Single-shot information leakage

Once the information flow is computed, it is straightforward to find the single-shot information leakage as they are related as follows:

$$L_{t_1, t_2}^{(S)}[\Lambda_t^{(ns)}] = - \int_{t_1}^{t_2} (c p_{\text{guess}}^*)^{-1} \sigma(\Lambda_t^{(ns)}) dt. \quad (\text{A5})$$

In Figs. 2 and 3, the information leakage is computed and plotted for cases $n_S = 1, 2, 3, 4$. Since the information is positive, i.e., a gain of information happens at all time on a subsystem under consideration, the information leakage is negative at all time. This means that information leakage takes places from environment to system, and also quantifies the information gained from the environment.

3. Adiabatic algorithm for quantum search

In the realization of an amplitude amplification algorithm via the adiabatic quantum computation method, the state of the quantum system evolves continuously under the influence of the driving Hamiltonian, $\mathcal{H}_{ad}(t)$, as follows:

$$i \frac{d}{dt} |\psi(t)\rangle = \mathcal{H}_{ad}(t) |\psi(t)\rangle, \quad (\text{A6})$$

where

$$\mathcal{H}_{ad}(t) = f(t)\mathcal{H}(t=0) + [1 - f(t)]\mathcal{H}(t=T), \quad (\text{A7})$$

with $\mathcal{H}(t=0) = \mathbb{I} - |\psi_n\rangle\langle\psi_n|$ and $\mathcal{H}(t=T) = \mathbb{I} - |w\rangle\langle w|$, and $f(t)$ controls the rate of the evolution.

Suppose that the initial state $|\psi_n\rangle$ is prepared in the ground energy level of $\mathcal{H}(t=0)$ and adiabatically evolves via the unitary $U_{ad}(t, 0) = e^{\int_0^t \mathcal{H}_{ad}(t) dt}$. At each step of the evolution, the adiabatic condition is applied such that the system remains a ground state, $|\phi(t)\rangle$, with sufficiently high probability, i.e., $|\langle\psi(t)|\phi(t)\rangle|^2 \geq 1 - \epsilon^2$ for the first excited one $|\psi(t)\rangle$. With the adiabatic constraint, we have

$$U_{ad}(t, 0) = \sum_n e^{i\alpha_n(t)} |n, t\rangle\langle n, 0|, \quad (\text{A8})$$

where $\alpha_n(t)$ is a function of $E_n(t)$, which are the eigenvalues of $\mathcal{H}_{ad}(t)$, and $|n, t\rangle$ are the eigenvectors.

One of the possible choices of the functional form of $f(t)$ is the linear interpolation, $f(t) = \frac{t}{T}$, where T is the total runtime of the evolution. However, it has been shown that in order to satisfy the adiabatic condition, for this choice of $f(t)$, the total runtime of the evolution turns out to be $T \geq \frac{N}{\epsilon}$. Thus, the computation time, which essentially can be argued as the efficiency of the algorithm, turns out to be $O(N)$. Therefore, for this choice of the functional form of $f(t)$, adiabatic evolution does not provide any advantage over its classical counterpart.

In Ref. [22], the local adiabatic evolution is proposed so that the quadratic speedup can be maintained. This can be obtained with the choice of the function $f(t)$, as follows:

$$f(t) = \frac{1}{2} - \frac{1}{2} \left(\frac{1}{\sqrt{N-1}} \tan \frac{2\epsilon t \sqrt{N-1}}{N} - \tan^{-1} \sqrt{N-1} \right).$$

In this case, the total runtime of the algorithm turns out to be $T = \sqrt{N}\pi/(2\epsilon)$.

-
- [1] A. Barenco, *Proc. R. Soc. London A* **449**, 679 (1995).
 - [2] A. Barenco *et al.*, *Phys. Rev. A* **52**, 3457 (1995).
 - [3] D. Deutsch, A. Barenco, and A. Ekert, *Proc. R. Soc. London* **449**, 669 (1995).
 - [4] D. P. DiVincenzo, *Phys. Rev. A* **51**, 1015 (1995).
 - [5] S. Lloyd, *Phys. Rev. Lett.* **75**, 346 (1995).
 - [6] S. Massar and S. Popescu, *Phys. Rev. Lett.* **74**, 1259 (1995).
 - [7] H.-P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems* (Oxford University Press, Oxford, 2002).
 - [8] H. P. Breuer, E. M. Laine, and J. Piilo, *Phys. Rev. Lett.* **103**, 210401 (2009).
 - [9] A. Rivas, S. F. Huelga, and M. B. Plenio, *Phys. Rev. Lett.* **105**, 050403 (2010).
 - [10] D. Chruscinski and S. Maniscalco, *Phys. Rev. Lett.* **112**, 120404 (2014).
 - [11] J. Bae and D. Chruscinski, *Phys. Rev. Lett.* **117**, 050403 (2016).
 - [12] B.-H. Liu *et al.*, *Nat. Phys.* **7**, 931 (2011).
 - [13] H.-P. Breuer, E.-M. Laine, J. Piilo, and B. Vacchini, *Rev. Mod. Phys.* **88**, 021002 (2016).
 - [14] A. S. Holevo, *Probl. Inf. Transf.* **10**, 317 (1974).
 - [15] H. P. Yuen, R. S. Kennedy, and M. Lax, *IEEE Trans. Inf. Theory* **21**, 125 (1975).
 - [16] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976), Vol. 123.
 - [17] R. König, R. Renner, and C. Schaffner, *IEEE Trans. Inf. Theory* **55**, 9 (2009).
 - [18] R. Renner, Ph.D. thesis, Eidgenössische Technische Hochschule, 2005.
 - [19] N. Datta, M. Mosonyi, M.-H. Hsieh, and F. G. S. L. Brandao, *IEEE Trans. Inf. Theory* **59**, 8014 (2013).
 - [20] L. K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).
 - [21] E. Farhi and S. Gutmann, *Phys. Rev. A* **57**, 2403 (1998).
 - [22] J. Roland and N. J. Cerf, *Phys. Rev. A* **65**, 042308 (2002).
 - [23] P. W. Shor, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (IEEE, Washington, 1994), p. 20.
 - [24] C. Zalka, *Phys. Rev. A* **60**, 2746 (1999).
 - [25] N. Bao, A. Bouland, and S. P. Jordan, *Phys. Rev. Lett.* **117**, 120501 (2016).
 - [26] J. Bae, W.-Y. Hwang, and Y.-D. Han, *Phys. Rev. Lett.* **107**, 170403 (2011).
 - [27] D. Bruss and C. Macchiavello, *Phys. Rev. A* **83**, 052313 (2011); **85**, 049906(E) (2012).
 - [28] Y. Fang, D. Kaszlikowski, C. Chin, K. Tay, L. C. Kwek, and C. H. Oh, *Phys. Lett. A* **345**, 265 (2005).

- [29] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [30] D. Deutsch and R. Jozsa, *Proc. R. Soc. London A* **439**, 553 (1992).
- [31] W. K. Wootters, *Phys. Rev. Lett.* **80**, 2245 (1998).
- [32] S. Hill and W. K. Wootters, *Phys. Rev. Lett.* **78**, 5022 (1997).
- [33] F. Mintert, M. Kus, and A. Buchleitner, *Phys. Rev. Lett.* **92**, 167902 (2004).
- [34] F. Mintert, M. Kus, and A. Buchleitner, *Phys. Rev. Lett.* **95**, 260502 (2005).
- [35] D. R. Simon, *SIAM J. Comput.* **26**, 1474 (1997).
- [36] F. Buscemi and N. Datta, *Phys. Rev. A* **93**, 012101 (2016).
- [37] D. Chruscinski, A. Rivas, and E. Størmer, *Phys. Rev. Lett.* **121**, 080407 (2018).
- [38] C. M. Kropf, C. Gneiting, and A. Buchleitner, *Phys. Rev. X* **6**, 031023 (2016).
- [39] D. Chruscinski, A. Kossakowski, and A. Rivas, *Phys. Rev. A* **83**, 052128 (2011).
- [40] S. Wißmann, A. Karlsson, E.-M. Laine, J. Piilo, and H.-P. Breuer, *Phys. Rev. A* **86**, 062108 (2012).