Quantum Algorithms for Estimating Quantum Entropies

Youle Wang,[1,2,*] Benchi Zhao,[1] and Xin Wang[1,†]

[1] *Institute for Quantum Computing, Baidu Research, 100193 Beijing, China*

[2] *Center for Quantum Software and Information, University of Technology, Sydney, New South Wales 2007, Australia*

(Received 17 November 2022; revised 6 February 2023; accepted 14 February 2023; published 14 April 2023)

The von Neumann and quantum Rényi entropies characterize fundamental properties of quantum systems and lead to many theoretical and practical applications. Quantum algorithms using a purified quantum query model can speed up quantum entropy estimation, while little is known about the complexity of using identical copies of the quantum state. This paper presents quantum entropy estimation algorithms with a cost of copies scaling polynomially in the rank of the state. In contrast to current methods that depend on the dimension of the system, our methods could provide exponential resource savings in the scenario of low-rank states. Furthermore, we show how to construct quantum circuits using primitive single-qubit or two-qubit gates efficiently and thus provide practical methods for estimating quantum entropies of quantum systems. We also conduct simulation experiments to show the effectiveness and noise robustness of our algorithms.

DOI: 10.1103/PhysRevApplied.19.044041

I. INTRODUCTION

Entropy [1] is a fundamental concept in physics and computer science that can characterize randomness of the system. Shannon entropy [2] is often used to capture operational quantities in information processing and quantum physics. Rényi entropies [3] generalize Shannon entropy and constitute a family of one-parameter information measures. In the quantum realm, the corresponding concepts are von Neumann entropy [4] and quantum Rényi entropies [5], which have applications in many fields, such as quantum chemistry [6], condensed-matter physics [7], and high-energy physics [8]. Computing quantum entropies plays a key role in quantum information and quantum computing, for example, quantum entropies can provide the asymptotic lower bound for compressing quantum data [9] and can be applied to study quantum Gibbs state preparation [10–13] and Hamiltonian learning [14–17].

For any quantum state $\rho \in \mathbb{C}^{2^n\times 2^n}$, von Neumann entropy is defined by $S(\rho) = -\mathrm{tr}(\rho\ln(\rho))$, and quantum Rényi entropy of order α is defined by $R_\alpha(\rho) = 1/(1-\alpha)\log\mathrm{tr}(\rho^\alpha)$, with $\alpha \in (0,1)\cup(1,+\infty)$. In the limit $\alpha \to 1$, $R_\alpha(\rho)$ converges to $S(\rho)$ up to a proportional factor. If the density matrix of ρ is diagonal in the computational basis, $S(\rho)$ and $R_\alpha(\rho)$ degenerate to their classical counterparts. Despite being conceptually simple, estimating quantum entropies is not easy. Various methods [18] have been proposed to estimate quantum entropies, and a large number of quantum resources are demanded. The most-straightforward method is tomography [19], which gives the classical description of the density matrix. In this case, the resource cost increases exponentially with the size of the state. In addition, the current optimal classical algorithm for quantum entropy estimation has a cost scaling linearly with the number of nonzero elements of the density matrix [20].

Many quantum solutions based on different models have been proposed [10,19,21–25]. The cost of estimating $S(\rho)$ and $R_\alpha(\rho)$ in a model where one can get identical copies of the state was studied by Acharya *et al.* [19]. By allowing arbitrary measurements and classical postprocessing, it was shown that the cost of entropy estimation scales exponentially with the state size. Later,Gilyén and Li [23] and Subramanian and Hsieh [24] studied quantum entropy estimations in a purified quantum query model that prepares the purification of the input state, i.e., $U_\rho\,|0\rangle_A\,|0\rangle_B = |\psi_\rho\rangle_{AB}$ and $\mathrm{tr}_A(|\psi_\rho\rangle\,\langle\psi_\rho|_{AB}) = \rho$. It has been shown that the complexity of querying U_ρ for estimating $S(\rho)$ can be asymptotically linear in the dimension of the system [23], while the results for $R_\alpha(\rho)$ are comparable to those obtained by tomography [24]. Recently, Gur *et al.* [26] have brought that the complexity of querying U_ρ for estimating $S(\rho)$ is sublinear in the dimension. Wang *et al.* [27] proposed quantum algorithms with a dependence on the rank of the state, where the results for estimation of von Neumann entropy have a linear dependence on the rank. Moreover, Yirka and Subasi [28] considered access

*youle.wang92@gmail.com
†wangxin73@baidu.com

to a purification of the state and used short-depth circuits to estimate $\mathrm{tr}(\rho^k)$ for integer k, which could be used to estimate $R_\alpha(\rho)$ when α is an integer.

In this work, we consider estimating quantum entropies of an unknown quantum state and propose quantum algorithms of concrete implementation that use identical copies of the input state. To develop our algorithms, we first give series functionals approximating quantum entropies. Then we devise quantum circuits to estimate individual terms in the series. When designing quantum circuits, we synthesize several quantum gadgets, such as iterative quantum phase estimation [29], exponentiation of the quantum state [30], and a technique of implementing a linear combination of unitaries [31]. As a result, we show how circuits are decomposed into primitive single-qubit or two-qubit gates, which leads to practical methods for quantum entropy estimation. We also consider compressing the circuit width by qubit reset [32], which was the method used in Ref. [28] to compress the circuits for estimating $\mathrm{tr}(\rho^k)$. It allows there to be two copies of the state during computation. Eventually, we use the sampling technique to give an unbiased estimator for quantum entropies. Overall, the copy cost for estimating $S(\rho)$ is $\widetilde{O}(r^2/\epsilon^7)$, where r is the rank of ρ and ϵ denotes the additive error. The cost of estimating $R_\alpha(\rho)$ depends on α, which scales polynomially in r. We also count the costs of primitive single-qubit or two-qubit gates. The details are shown in Theorems 1 and 2. In contrast to previous work [19] using identical copies, this work provides results with a dependence on the rank of the state rather than the dimension, implying exponential resource savings in the scenario of low-rank states. It also generalizes the methods for estimating $\mathrm{tr}(\rho^\alpha)$ for any $\alpha > 0$ and $\alpha \neq 1$, while the method in Ref. [28] works only when α is an integer.

This paper is organized as follows: Section II provides series functionals as approximations of von Neumann and quantum Rényi entropies, which consist of terms that are easy to estimate with quantum computers. Section III provides concrete quantum circuits to evaluate individual terms of the series and explains in detail how to decompose the circuits into single-qubit or two-qubit gates. Section IV presents quantum entropy estimation algorithms and their costs of state copies and quantum gates. Furthermore, Sec. V presents numerical experiments to show the effectiveness and noise robustness of our algorithms. Finally, the conclusions are presented in Sec. VI.

II. QUANTUM ENTROPY APPROXIMATIONS

Approximation series of quantum entropies were considered in Refs. [10,23,24]. Our methods are inspired by Ref. [10], in which a method in Ref. [33] is used to convert a Taylor-series approximation of $S(\rho)$ to a Fourier series. We further use this method to give approximations of $S(\rho)$ and $\mathrm{tr}(\rho^\alpha)$, expressed as a linear combination of terms of the form $\mathrm{tr}(\rho^p\cos(\rho t))$ for some integer $p \geq 1$. Particularly, we give a series whose number of terms depends on the state's rank, while in previous work [10], it was determined by the approximation precision.

A. Approximation of von Neumann entropy

When given a lower bound of all nonzero eigenvalues of the state ρ, we can give an approximation of $S(\rho)$ by approximating the entropic function of each nonzero eigenvalue. The idea is simple: transform the truncated Taylor series $\sum_{k=1}^{K} 1/k\mathrm{tr}\left(\rho(I-\rho)^k\right)$ into a weighted sum of cosines by replacing $1-\rho$ with $\arcsin(\cos(\rho\pi/2))/(\pi/2)$. Then expand arcsine to its Taylor series. Next, truncate the Taylor series of arcsine to give a high-precision approximation. Lastly, use the relation $\cos(\rho\pi/2) = (e^{i\rho\pi/2} + e^{-i\rho\pi/2})/2$ to cancel the cosines, resulting in a series that is composed of terms of the form $\mathrm{tr}(\rho\cos(\rho t))$. More details are provided in Appendix A, including the choices of truncation orders.

The discussion above describes a method for constructing approximations of entropies using the knowledge of the lower bound of all nonzero eigenvalues. We further convert the dependence on the lower bound to that on the rank. Our idea is to choose an eigenvalue threshold that partitions eigenvalues into two groups. We construct approximations to approximate entropic functions for one group and ignore the other. The subtlety is to choose a proper eigenvalue threshold to suppress the error caused by ignoring the other group.

Lemma 1: [Rank-based $S(\rho)$ approximation.] Suppose we have a rank r of the quantum state ρ and choose an eigenvalue threshold $\kappa = \epsilon(12r\ln(r/\epsilon))^{-1}$. Then there exists an approximation of $S(\rho)$ with precision ϵ.

Proof: We consider a polynomial $P(x) = \sum_{k=1}^{K} x/k(1-x)^k$ with degree $K \in \Theta(1/\kappa\log(1/\epsilon\kappa))$, which approximates $x\ln(x)$ for all $x \in [\kappa, 1]$. Clearly, if eigenvalue κ of ρ is larger than κ, then we would have $|P(\kappa) - \kappa\ln(\kappa)| \leq \kappa\epsilon/2$. Otherwise, for those eigenvalues $\kappa \leq \kappa$, the polynomial $P(\kappa)$ satisfies the inequality $|P(\kappa) - \kappa\ln(\kappa)| \leq |P(\kappa)| + |\kappa\ln(\kappa)|$. We further consider that $P(\kappa)$ is bounded by its overall weights, i.e., $|P(\kappa)| \leq \kappa\ln(K)/4$ for all $\kappa \leq \kappa \leq \frac{1}{2}$. Then a larger upper bound is given as $1/4|\kappa\ln(K)| + |\kappa\ln(\kappa)|$. With this bound, we can easily characterize the error between $P(\kappa)$ and $\kappa\ln(\kappa)$: $|\kappa\ln(\kappa)| + 1/4|\kappa\ln(K)| \leq 3\kappa/2\ln(1/\epsilon\kappa)$. Moreover, when $\kappa = \epsilon(12r\ln(r/\epsilon))^{-1}$, the error is smaller than $\epsilon/2r$. Finally, we combine the above results and find the approximation error is smaller than ϵ. ■

This lemma guarantees that we can find a series of $\mathrm{tr}(\rho\cos(\rho t))$ as an approximation of $S(\rho)$ and implies that the number of terms has an asymptotic polynomial scaling with the rank. We discuss later how to evaluate each term in the series with quantum computers and further combine them to give an estimate of the entropy. Next, we discuss how to give such approximations of quantum Rényi entropies.

B. Approximation of Rényi entropy of order α

For quantum Rényi entropy of order α, we focus on estimating $\mathrm{tr}(\rho^\alpha)$. When α is an integer, the quantity can be estimated by using simple quantum circuits (e.g., the Hadamard test [28,34]). For noninteger α, we separately consider the integer and decimal parts of α: we first construct a series approximation of $x^{\{\alpha\}}$, where $\{\alpha\}$ denotes the decimal part, and then combine it with $x^{[\alpha]}$ to give an approximation of $\mathrm{tr}(\rho^\alpha)$.

For simplicity, we assume $\alpha \in (0,1)$. Firstly, we write the Taylor series of $x^\alpha = \sum_{k=0}^{\infty}\binom{\alpha}{k}(x-1)^k$, where $\binom{\alpha}{k} = \prod_{j=1}^{k}(\alpha - j + 1)/j$ is the generalized binomial coefficient. Secondly, we replace $x-1$ with $\arcsin((x-1)\pi/2)/(\pi/2)$ and Taylor-expand the function $[\arcsin(y)/(\pi/2)]^k$. We denote the series of $[\arcsin(y)/(\pi/2)]^k$ by $\sum_{l=0}^{\infty} b_l^{(k)} y^l$. Here, the $b_l^{(0)}$'s are the coefficients of the Taylor series of $\arcsin(y)/(\pi/2)$, and the other $b_l^{(k)}$'s can be computed inductively. Particularly, we have $b_l^{(k)} \ge 0$ and $\sum_{l=1}^{\infty} b_l^{(k)} = 1$ for any k, since $[\arcsin(1)/(\pi/2)]^k = 1$. Lastly, truncation of both infinity series gives an approximation of x^α.

Similarly, given the lower bound of all nonzero eigenvalues, we can construct an approximation series of $\mathrm{tr}(\rho^\alpha)$. We show the details in Appendix A. Here, given the rank of the state, we show how to select an eigenvalue threshold.

Lemma 2: [Rank-based $R_\alpha(\rho)$ approximations.] Suppose we have a rank r of a quantum state ρ. When $\alpha \in (1,\infty)$, $\kappa = (\xi/4r)^{1/[\alpha]}/4\ln\left(\xi^{-1}(\xi/4r)^{-1/[\alpha]}\right)$ suffices to provide an approximation of $\mathrm{tr}(\rho^\alpha)$ with accuracy ξ; when $\alpha \in (0,1)$, choosing $\kappa = (\xi/8r)^{1/\alpha}$ is sufficient.

Proof: Case 1: $\alpha > 1$. We recall the series $P_\alpha(x) = \sum_{k=0}^{K}\sum_{l=0}^{L}\binom{\{\alpha\}}{k} b_l^{(k)} x^{[\alpha]}[\sin((x-1)\pi/2)]^l$, which approximates x^α with precision $x^{[\alpha]}\xi/2$ for all $x \in [\kappa, 1)$. When $x < \kappa$, the approximation error is upper bounded as $|P_\alpha(x) - x^\alpha| \le |P_\alpha(x)| + x^\alpha$. Since $|\sin((x-1)\pi/2)| \le 1$ and $\sum_{l=0}^{L} b_l^{(k)} \le 1$, we can easily find that $|P_\alpha(x)| \le x^{[\alpha]}\sum_{k=0}^{K}\left|\binom{\{\alpha\}}{k}\right| \le x^{[\alpha]}\left(\sum_{k=1}^{K} k^{-1}\{\alpha\} + 1\right)$, where the second inequality follows since $|\binom{\{\alpha\}}{k}| \le k^{-1}\{\alpha\}$. We readily give a larger bound of the truncation error, which is $2x^{[\alpha]}\ln(K)$, where $K \in O(1/\kappa\log(1/\kappa\xi))$. To bound the error of approximating $\mathrm{tr}(\rho^\alpha)$, it suffices to let $\sum_{j:\lambda_j<\kappa} 2\lambda_j^{[\alpha]}\ln(K) \le \xi/2$. Then the claimed κ is valid since it satisfies $2r(\kappa\ln(K))^{[\alpha]} \le \xi/2$.

Case 2: $\alpha \in (0,1)$. By our setting suitable K and L, $P_\alpha(x) = \sum_{k=0}^{K}\sum_{l=0}^{L}\binom{\alpha-1}{k} b_l^{(k)} x[\sin((x-1)\pi/2)]^l$ approximates x^α with precision $x\xi/2$ for all $x \in [\kappa, 1)$. Meanwhile, $|P_\alpha(x) - \sum_{k=0}^{K}\binom{\alpha-1}{k}x(x-1)^k| \le x\xi/4$ for $x \in (0,\kappa)$. Thus, when $x \in (0,\kappa)$, an upper bound of $P_\alpha(x)$ is given by $\sum_{k=0}^{K}|\binom{\alpha-1}{k}|x(1-x)^k + x\xi/4$. Using $|\binom{\alpha-1}{k}| = \binom{\alpha-1}{k}(-1)^k$, we further find a larger bound, $x^\alpha + x\xi/4$. Then we can conclude that setting $\kappa = (\xi/8r)^{1/\alpha}$ is sufficient to suppress the error of approximating $\mathrm{tr}(\rho^\alpha)$ to ξ. ■

Lemma 2 provides an eigenvalue threshold that can be used to determine the approximation series, which is composed of terms $\mathrm{tr}(\rho^p\cos(\rho t))$. This implies that the number of terms has a polynomial scaling with the rank of the state. The concrete procedure for finding approximations is provided in Appendix A. Notice that here we discuss estimating $\mathrm{tr}(\rho^\alpha)$, which is used to give an estimate of $R_\alpha(\rho)$ via simple calculations. Thus we need to analyze how the error would propagate from the former to the latter.

To do this, let $\widehat{\mathrm{tr}(\rho^\alpha)}$ denote an estimate of $\mathrm{tr}(\rho^\alpha)$ up to error ξ, i.e., $|\widehat{\mathrm{tr}(\rho^\alpha)} - \mathrm{tr}(\rho^\alpha)| \le \xi$. Then the difference between their logarithmic functions is $|1-\alpha|^{-1}\left|\log\left(1 + [\widehat{\mathrm{tr}(\rho^\alpha)} - \mathrm{tr}(\rho^\alpha)]/\mathrm{tr}(\rho^\alpha)\right)\right|$. Notice that $|\log(1+x)| \le 2|x|$ for any $x \in [-0.5, 1]$. Assume that $[\widehat{\mathrm{tr}(\rho^\alpha)} - \mathrm{tr}(\rho^\alpha)]/\mathrm{tr}(\rho^\alpha)$ falls in the interval $[-0.5, 1]$; we, therefore, find that the difference is smaller than $2\xi/|1-\alpha||\mathrm{tr}(\rho^\alpha)|$. Moreover, since $\mathrm{tr}(\rho^\alpha) \ge [\mathrm{tr}(\rho^2)]^{\alpha-1}$ for all $\alpha \in (0,1)\cup(2,+\infty)$ and $\mathrm{tr}(\rho^\alpha) \ge \mathrm{tr}(\rho^2)$ for all $\alpha \in (1,2]$, the relation between ξ and ϵ is given as $\xi = |1-\alpha|/2[\mathrm{tr}(\rho^2)]^{\alpha-1}\epsilon$ if $\alpha \in (0,1)\cup(2,+\infty)$, and as $\xi = |1-\alpha|/2\mathrm{tr}(\rho^2)\epsilon$ if $\alpha \in (1,2]$.

III. QUANTUM CIRCUITS

In this section we present quantum circuits to estimate terms of the form $\mathrm{tr}(\rho^p\cos(\rho t))$ for any positive integer p. We first show the correctness of the quantum circuits and then decompose them into primitive single-qubit or two-qubit gates. We then discuss a crucial subroutine that simulates the exponentiation of the swap operator. Finally, we consider compressing the circuit width.

A. Circuit scheme

Recall that the swap test [35] can estimate purity $\mathrm{tr}(\rho^2)$ and the Hadamard test [28,34] can estimate more-general state overlap $\mathrm{tr}(\rho^k)$ ($k \ge 3$), where the unitary is the cyclic permutation operator. Assume a quantum circuit implements the unitary $e^{-i\rho t}$. We then show that the combination of the Hadamard test and the controlled $e^{-i\rho t}$ operation gives a quantum circuit to estimate $\mathrm{tr}(\rho^p\cos(\rho t))$. A circuit for illustration is shown in Fig. 1.

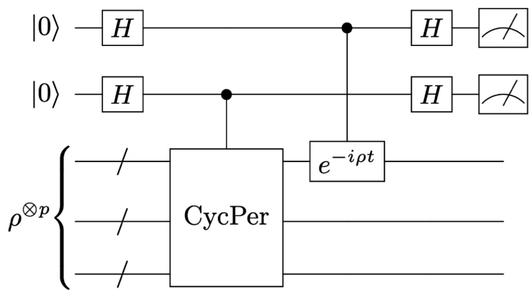

FIG. 1. Quantum circuit for estimating $\mathrm{tr}(\rho^p\cos(\rho t))$. CycPer denotes the cyclic permutation operator, which acts as $\mathrm{CycPer}\,|\psi_1,\psi_2,\ldots,\psi_p\rangle=|\psi_2,\psi_3,\ldots,\psi_1\rangle$.

Proposition 1. *For any positive integer $p\geq 1$ and $t\in\mathbb{R}$, the quantum circuit in Fig. 1 can estimate $tr(\rho^p\cos(\rho t))$.*

The proof is presented in Appendix B. Proposition 1 indicates that we could use quantum computers to estimate the entropy approximation. In general, the cyclic permutation operator is easy to construct using shallow quantum circuits, while the exponentiation of the density matrix is more complex and more difficult to implement. Although a method using identical copies of the state for this purpose was provided in Ref. [30], how to construct concrete circuits using primitive single-qubit or two-qubit gates is not yet known. Next, we present a method that uses simple quantum circuits and identical copies of the state.

B. Density-matrix exponentiation

For convenience, we present a quantum circuit to estimate $\mathrm{tr}(\rho\cos(\rho t))$ for arbitrary $t\in\mathbb{R}$, which can be easily generalized to circuits for estimating $\mathrm{tr}(\rho^p\cos(\rho t))$ for any $p\geq 2$. To begin, we show a circuit in Fig. 2 that estimates $\mathrm{tr}(\rho\cos(\rho t))$ when t is small.

In Fig. 2, qubit $|0\rangle\langle 0|$ and two copies of state ρ are input into the circuit. Two Hadamard gates are applied, sandwiching a controlled exponentiation of the swap operator. At the end of the circuit, we measure the top ancillary qubit

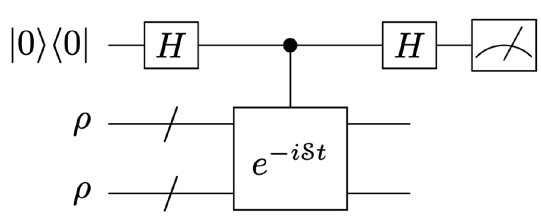

FIG. 2. For a short time t, we first prepare a ground state $|0\rangle\langle 0|$ in the measure register, and prepare ρ in the main register and in the ancillary register, respectively. Subsequently, the controlled unitary operator $e^{-i\mathcal{S}t}$ acts on state $\rho\otimes\rho$. At the end of the circuit, we measure along the eigenbasis of Pauli Z, which would immediately lead to an estimate for $\mathrm{tr}(\rho\cos(\rho t))$ up to precision $O(t^2)$.

on the Pauli Z operator. In particular, the measurement outcome leads to the value of $\mathrm{tr}(\rho\cos(\rho t))$. More precisely, $\mathrm{tr}(\rho\cos(\rho t))\approx\Pr[0]-\Pr[1]$, where $\Pr[0]$ denotes the probability of observing outcome 0 and $\Pr[1]$ denotes the probability of observing outcome 1.

Proposition 2. *Let V denote the unitary corresponding to the circuit in Fig. 2. For any quantum state ρ and a parameter t, the measurement outcome is close to $tr(\rho\cos(\rho t))$, i.e., $\left|tr(\rho\cos(\rho t))-tr\left(\left(V(|0\rangle\langle 0|\otimes\rho^{\otimes 2})V^\dagger\right)Z_0\right)\right|\leq 2t^2$, where Z_0 represents $Z\otimes I\otimes I$.*

Proof : To show correctness, we focus on the state in the top two registers. After applying the controlled operation, the state is changed into $\frac{1}{2}\left[|0\rangle\langle 0|\otimes\rho^{\otimes 2}+|1\rangle\langle 1|\otimes e^{-i\mathcal{S}t}\rho^{\otimes 2}e^{i\mathcal{S}t}\right]+\frac{1}{2}\left[|0\rangle\langle 1|\otimes\rho^{\otimes 2}e^{i\mathcal{S}t}+|1\rangle\langle 0|\otimes e^{-i\mathcal{S}t}\rho^{\otimes 2}\right]$. Then we trace out the appended copy of ρ. Note that part of tracing state is executed as $|1\rangle\langle 0|\otimes\mathrm{tr}_{\mathrm{anc}}\left(e^{-i\mathcal{S}t}\rho^{\otimes 2}\right)=|1\rangle\langle 0|\otimes(\cos(t)I-i\sin(t)\rho)\rho$. The notation $\mathrm{tr}_{\mathrm{anc}}$ means tracing out the appended copy of ρ. Here we have used the facts that $e^{-i\mathcal{S}t}=\cos(t)I-i\sin(t)\mathcal{S}$ and $\mathrm{tr}_{\mathrm{anc}}(\mathcal{S}\rho\otimes\sigma)=\rho\sigma$. A similar result could be derived for $|0\rangle\langle 1|\otimes\rho^{\otimes 2}e^{i\mathcal{S}t}$.

We show that the difference between $(\cos(t)I-i\sin(t)\rho)\rho$ and $e^{-i\rho t}\rho$ is smaller than $2t^2$. This is because the difference is equal to $\left\|\left[e^{-i\rho t}-(\cos(t)I-i\sin(t)\rho)\right]\rho\right\|_{\mathrm{tr}}$. By our Taylor-expanding $e^{-i\rho}$, the expression is changed into the form $\|(1-\cos(t))\rho-i(t-\sin(t))\rho^2+\sum_{k\geq 2}(-i\rho t)^k\rho/k!\|_{\mathrm{tr}}$. The latter value is smaller than $2\sin^2(t/2)+|t-\sin(t)|+\sqrt{2}t^2/2$, where we use the inequalities $|x-\sin(x)|\leq x^2/2$ and $|\sin(x)|\leq x$, and the inequality $\|\sum_{k\geq 2}(-i\rho t)^k/k!\|_{\mathrm{tr}}\leq\sqrt{2}t^2/2$. Again, a similar result can be found for $\rho^{\otimes 2}e^{i\mathcal{S}t}$ and $\rho e^{i\rho t}$.

Finally, notice that measuring the top ancillary qubit gives $\Pr[0]-\Pr[1]$; thus, the measurement results give the value $\frac{1}{2}[\mathrm{tr}\left(\mathrm{tr}_{\mathrm{anc}}(e^{-i\mathcal{S}t}\rho^{\otimes 2})\right)+\mathrm{tr}\left(\mathrm{tr}_{\mathrm{anc}}(\rho^{\otimes 2}e^{i\mathcal{S}t})\right)]$ on the basis of the discussions above. Recall that $\left\|\mathrm{tr}_{\mathrm{anc}}(e^{-i\mathcal{S}t}\rho^{\otimes 2})-e^{-i\rho t}\rho\right\|_{\mathrm{tr}}\leq 2t^2$ and $\left\|\mathrm{tr}_{\mathrm{anc}}(\rho^{\otimes 2}e^{i\mathcal{S}t})-\rho e^{i\rho t}\right\|_{\mathrm{tr}}\leq 2t^2$. We, therefore, can readily verify the claimed results using the relation $\mathrm{tr}(\rho\cos(\rho t))=(\rho e^{i\rho t}+e^{-i\rho t}\rho)/2$. ■

For large t, we could generalize the circuit in Fig. 2 to do this. Specifically, divide the parameter t into several small pieces Δt and run c-$e^{-i\mathcal{S}\Delta t}$ sequentially, where c- represents controlled operations. The circuit is depicted in Fig. 3.

Proposition 3. *For any quantum state $\rho\in\mathbb{C}^{2^n\times 2^n}$ and $t\in\mathbb{R}$, there is a quantum circuit that can estimate the quantity $tr(\rho\cos(\rho t))$ with precision ϵ. The number of copies of state ρ needed is $O(t^2/\epsilon)$.*

Proof : Divide parameter t into Q pieces. The parameter in the swap operator thus becomes $\Delta t=t/Q$. In the circuit, we append Q ancillary registers and prepare ρ in each

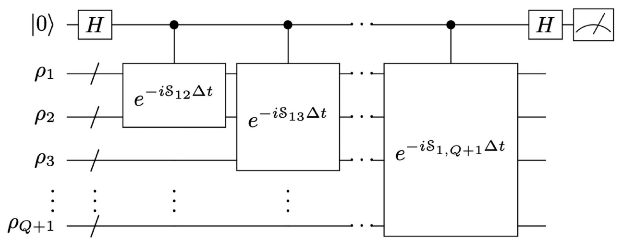

FIG. 3. The operator $e^{-i\mathcal{S}\Delta t}$ is sequentially applied on the main register and different ancillary registers, conditional on the measure register. We append Q ancillary states and use $e^{-i\mathcal{S}\Delta t}$ Q times. For clarity, we label states on different registers by $1, 2, 3, \ldots, Q+1$, and the subscript of the swap operator indicates the registers that the swap operator acts on.

register. By Proposition 2, running the circuit in each piece will produce an error of at most $2\Delta t^2$. Then after the circuit has been run in all pieces, the accumulated error is $Q \times 2\Delta t^2 \le 2t^2/Q$. Clearly, setting $Q = \lceil 2t^2/\epsilon \rceil$ suffices to suppress the accumulated error to ϵ. As a result, the number of copies used is $(Q+1) = O(t^2/\epsilon)$. ■

Proposition 3 provides the cost of copies of the state to estimate $\mathrm{tr}(\rho\cos(\rho t))$ for any t. Nevertheless, there are some remaining issues: one is the simulation of the swap operator; another is the large circuit width, which may be a considerable burden for implementation in practice. The solutions to these issues are discussed in the following sections.

C. Swap-operator exponentiation

In this section we present the circuit for simulating the exponentiation of the swap operator, which uses the technique of implementing a linear combination of unitaries [31]. Note that $e^{-i\mathcal{S}\Delta t}$ can be written as $e^{-i\mathcal{S}\Delta t} = \cos(\Delta t) I_{2n} - i\sin(\Delta t)\mathcal{S}$. The subscript means the number of qubits that the identity operator acts on. We construct a circuit module W as in Fig. 4, where the top two qubits are newly added ancillary qubits. In the circuit, the $R_1|0\rangle = \alpha/2|0\rangle + \sqrt{1-\alpha^2/4}|1\rangle$ gate is a rotation gate, where $\alpha = \cos(\Delta t) + |\sin(\Delta t)| < 2$. oc-$R_2$ means applying the rotation R_2 on the target qubit when the control qubit is $|0\rangle$, where $R_2|0\rangle = \sqrt{\cos(\Delta t)/\alpha}|0\rangle + \sqrt{|\sin(\Delta t)|/\alpha}|1\rangle$. We assume time Δt is small enough such that $\cos(\Delta t) > 0$.

The select($\mathcal{S}$) gate implements the operation $(-i\mathrm{sgn}(\Delta t))\mathcal{S}$ on $\rho\otimes\rho$ conditionally, which is defined as $\mathrm{select}(\mathcal{S}) = |0\rangle\langle 0| \otimes I_{2n} + |1\rangle\langle 1| \otimes (-i\mathrm{sgn}(\Delta t))\mathcal{S}$. The detailed structure of $\mathcal{S}$ can be found in Appendix B 4. Third, we define a circuit module $W = R_2^{\dagger}\mathrm{select}(\mathcal{S})(\text{oc-}R_2) R_1$ as shown in Fig. 4. Furthermore, let $P = |00\rangle\langle 00|$ be the operator that projects onto the subspace spanned by $|00\rangle$, where $|00\rangle$ are the ancillary qubits in Fig. 4. Then, define a unitary operator $A = -W(I_2 - 2P)W^{\dagger}(I_2 - 2P)W$, where $I_2 - 2P$ denotes the operator that reflects along the vectors

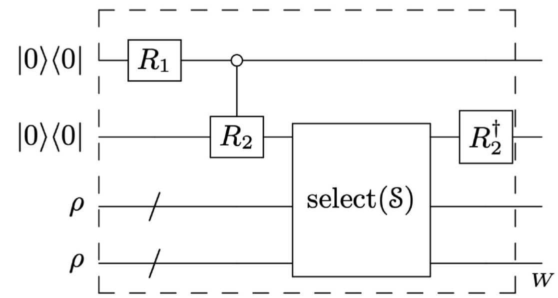

FIG. 4. Quantum circuit for implementing the module W.

that are orthogonal to $|00\rangle$. Then use unitary A to construct quantum circuits to the exponentiation operator $e^{-i\mathcal{S}\Delta t}$. Details of the construction are provided in Appendix B.

Proposition 4. *For arbitrary parameter* $\Delta t \in (-1, 1)$, *there is a quantum circuit that simulates* $e^{-i\mathcal{S}\Delta t}$ *in the sense that* $P \otimes e^{-i\mathcal{S}\Delta t} = PAP$.

Using the circuit of A to replace $\exp(-i\mathcal{S}\Delta t)$ will lead to the desired quantum circuits for estimating $\mathrm{tr}(\rho\cos(\rho t))$. One example is shown in Fig. 5 for illustration. Next, we estimate the number of primitive gates and qubits needed.

Proposition 5. *For any quantum state* $\rho \in \mathbb{C}^{2^n \times 2^n}$ *and time* $t \in \mathbb{R}$, *there is a quantum circuit to estimate the quantity* $\mathrm{tr}(\rho\cos(\rho t))$ *up to precision* ϵ *using* $O(nt^2/\epsilon)$ *single-qubit or two-qubit gates.*

Proof: The correctness follows immediately from Propositions 3 and 4 and the decomposition of the controlled $e^{-i\mathcal{S}\Delta t}$ gate in Appendix B 4. ■

Proposition 5 provides the number of gates for constructing the circuit. Using this result, we can easily estimate the gate complexity of our algorithms for estimating entropies.

D. Strategy for circuit-width reduction

In Fig. 3, there are $Q+1$ copies of ρ prepared at the beginning, but the interaction occurs between only two of them at a time. Clearly, interactions occur alternatively between the top ancillary qubit, the main register, and different ancillary registers. For instance, copy ρ_1 interacts only with the ancillary register being in state ρ_2. Once the controlled operation c-$e^{-i\mathcal{S}_{12}\Delta t}$ is completed, the occupied ancillary register is no longer involved in the following operations. At that time, copy ρ_3 is used for the next interaction. Notice that ρ_2 will no longer interact with the state of the other registers, and then we could measure the ancillary registers without affecting other registers.

Qubit reset is an underexplored technique that allows us to measure a subset of qubits and reinitialize them [32].

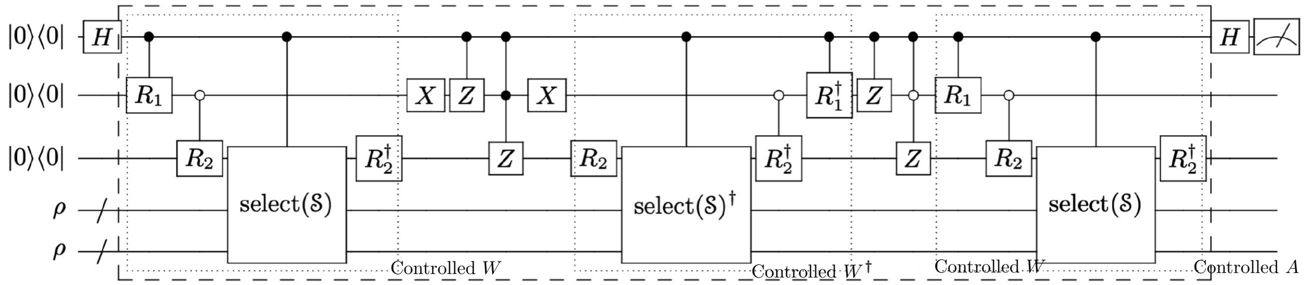

FIG. 5. The circuit resulting from replacing c-$e^{-i\mathcal{S}\Delta t}$ with the circuit of controlled operation A (dashed box) in Fig. 2. The dotted circuit is the controlled-W circuit, in which c-R_1 and oc-R_2 are the 1-controlled R_1 gate (apply R_1 on the target qubit if the control qubit is in state $|1\rangle$) and the 0-controlled R_2 gate (apply R_2 on the target qubit if the control qubit is in state $|0\rangle$), respectively. The circuit between the dotted boxes is known as a reflector.

Thus, using qubit reset means that we can measure the occupied ancillary register and reuse it to prepare a new state. Many experimental methods have been developed to actively reset the qubits on superconducting qubits [32,36–40] in the past decade. Recently, qubit reset was used to design quantum algorithms with reduced circuit width [28,41–44]. Notably, Yirka and Subasi [28] used qubit reset to devise quantum circuits for estimating $\mathrm{tr}(\rho^k)$ with $k \in \mathbb{N}$, which can contribute to the problem of quantum Rényi entropy [3] estimation.

Here we provide a circuit with reduced circuit depth that estimates $\mathrm{tr}(\rho\cos(\rho t))$, depicted in Fig. 3. Combining our circuits with the reduced circuits for $\mathrm{tr}(\rho^k)$ in [28] can easily give a reduced version of Fig. 1. In this case, we need only one ancillary register. Specifically, we prepare the state $\rho_1 \otimes \rho_2$ on the main register and the ancillary register at the beginning. Then the interaction occurs between them. Once the interaction is complete, the ancillary register is measured and readily reinitialized to state ρ_3. The same procedure of measuring and resetting is done Q times in all. The corresponding circuit using qubit reset is shown in Fig. 6. As a result, using the qubit-reset technique will effectively compress the circuit width since exactly two copies remain during the computation.

IV. QUANTUM ALGORITHMS

In this section, we present quantum algorithms for estimating von Neumann and quantum Rényi entropy of order α. The key is to run the devised quantum circuits to evaluate each term of entropic approximations. Particularly, we construct unbiased estimators for $S(\rho)$ and $\mathrm{tr}(\rho^\alpha)$, respectively.

A. Quantum algorithm for estimation of von Neumann entropy

The concrete procedure for estimating $S(\rho)$ is presented in Algorithm 1. First, on obtaining the required estimation precision ϵ and eigenvalue threshold κ, we determine the approximation series of $S(\rho)$. Then we construct an unbiased estimator of $S(\rho)$ by the importance-sampling technique. Specifically, we randomly select each approximation-series term with the probability corresponding to its weight. The average of the selected terms in expectation is proportional to the entropy value. Then we evaluate all selected terms via proposed quantum circuits and postprocessing of the measurement outcomes to reveal the desired estimates. Next, we analyze the correctness and cost of our algorithm.

Theorem 1. *Given access to identical copies of ρ with rank r, there exists a quantum algorithm that estimates $S(\rho)$ up to precision ϵ, succeeding with probability of at least $1-\delta$. The number of copies required is at most $\widetilde{O}\left(r^2/\epsilon^7\right)$, and the circuits used consist of $\widetilde{O}(nr^2/\epsilon^5)$ single-qubit or two-qubit gates. Here, the notation $\widetilde{O}$ hides the logarithmic factors.*

Proof: Correctness analysis. Rewrite the series in Lemma 4 as $F(\rho) = \sum_{l=0}^{L}\sum_{s=D_l}^{U_l} f(s,l)\mathrm{tr}(\rho\cos(\rho(2s$

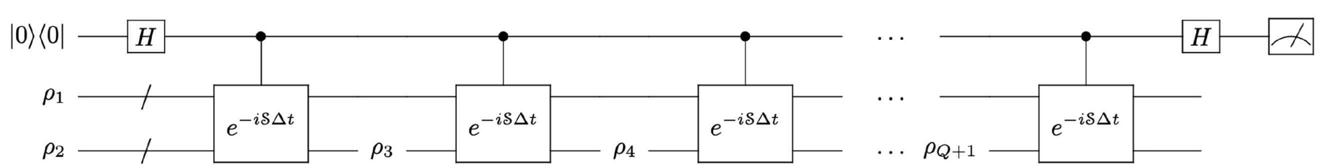

FIG. 6. A quantum circuit for estimating $\mathrm{tr}(\rho\cos(\rho t))$ using qubit reset. The break and a state ρ in the wire means implementing qubit reset.

Input: Constants $\epsilon, \delta, \kappa \in (0,1)$, and copies of state $\rho \in \mathbb{C}^{2^n \times 2^n}$.
Output: Estimate of the von Neumann entropy $S(\rho)$.

Compute coefficients L, K, M_l, and $b_l^{(k)}$ as given in Lemma S2.
Compute $\|\vec{f}\|_{\ell_1}$, as given in Eq. (1).
Set estimation error $\varepsilon = \epsilon/\|\vec{f}\|_{\ell_1}$.
Set integer $N = \sum_{l=0}^{L}(2M_l + 1)$.
Define a distribution as in Eq. (2).
Set integer $B = S$ as in Eq. (3).
Sample B pairs of $(s_1, l_1), \ldots, (s_B, l_B)$.
Set $j = 1$ and $\hat{s} = 0$.
while $j \leq B$ **do**
  Set $Q = \lceil (2s_j - l_j)^2\pi^2/4\varepsilon \rceil$.
  Prepare $Q + 1$ copies of ρ.
  Estimate $\mathrm{tr}(\rho\cos(\rho(2s_j - lj))\pi/2)$ with precision ε and probability $1 - \delta/2N$ via quantum circuits, given in Sec. III.
  Store the obtained estimate $\hat{e}_j$.
  Update $\hat{s} \leftarrow \hat{s} + \hat{e}_j$ and $j \leftarrow j + 1$.
end while
return $\|\vec{f}\|_{\ell_1} \times \hat{s}/B$.

Algorithm 1. Quantum algorithm for estimation of von Neumann entropy.

$-l)\pi/2)$), where the coefficients $f(s,l)$ are given by

$$f(s,l) = \left(\sum_{k=1}^{K} \frac{b_l^{(k)}}{k}\right) \frac{\binom{l}{s}}{2^l} \quad \text{for all } s, l. \tag{1}$$

Let $\vec{f}$ be a vector that consists of all $f(s,l)$. The ℓ_1 norm of $\vec{f}$ is bounded by $O(\log(K))$, i.e., $\|\vec{f}\|_{\ell_1} \leq O(\log(K))$. Define an importance sampling as follows:

$$R = \mathrm{tr}\left(\rho\cos\left(\rho\frac{(2s-l)\pi}{2}\right)\right) \quad \text{with probability } \frac{f(s,l)}{\|\vec{f}\|_{\ell_1}}. \tag{2}$$

The definition of "distribution" means that each term associated with (s,l) is sampled with probability proportional to its weight $f(s,l)$. Then, the series could be represented as the expectation value of R, i.e., $F(\rho) = \|\vec{f}\|_{\ell_1} \cdot \mathbf{E}[R]$, which is an unbiased estimator for $S(\rho)$. Hence, we could randomly select series terms to provide an estimator for $S(\rho)$ with a high probability.

Cost analysis. Note that the sample mean could estimate the expectation with the desired accuracy that depends on the number of samples. Specifically, by Chebyshev's inequality, $O(V/\epsilon^2)$ samples are sufficient to estimate the expectation with precision ϵ and high probability, where V denotes the variance and ϵ is the precision. Meanwhile, the probability could be boosted to $1-\delta$ at the cost of an additional multiplicative factor $O(\log(1/\delta))$ according to Chernoff bounds. Alternatively, by Hoeffding's inequality, we need only $O(\log(1/\delta)/\epsilon^2)$ samples to estimate the expectation with precision ϵ and probability greater than $1-\delta$.

In this case, the variance of the random variable R is less than 1 since the random number is bounded by 1. To estimate $F(\rho)$ with precision ϵ, we set the estimation precision as $\varepsilon = \epsilon/\|\vec{f}\|_{\ell_1}$. We also set the failure probability as $\delta/2$. As a result, the number of samples needed is given by

$$S = O\left(\frac{1}{\varepsilon^2}\log\left(\frac{2}{\delta}\right)\right). \tag{3}$$

This means that there are at most S terms to estimate. On the other hand, measuring circuits would produce additional failure probability. Since the series $F(\rho)$ consists of $N = \sum_{l=0}^{L}(2M_l + 1)$ terms in all, it suffices to estimate each term with probability $1 - \delta/2N$. The overall failure probability is at most δ by the union bound. The number of measurements needed for each term is given by

$$M = O\left(\frac{\log(2N/\delta)}{\varepsilon^2}\right). \tag{4}$$

Immediately, the total number of measurements for estimating the approximation series is given by

$$C_m = S \times M = \widetilde{O}\left(\frac{1}{\epsilon^4}\right). \tag{5}$$

Now we consider the cost of copies of ρ. For each term to be estimated, we need to run the circuit and measure many times. Each time, running the circuit would cost copies of the state, as stated earlier. Thus, the total number of copies equals the number of measurements times the cost per measurement. Recall that when one is estimating $\mathrm{tr}(\rho\cos(\rho t))$, performing measurement once costs $\widetilde{O}(t^2/\epsilon)$ copies of ρ (see Proposition 3). For the series $S(\rho)_{\hat{e}}$, the maximum time is $O(M_L) = O(\ln(\ln(K)/\epsilon)\,1/\kappa)$ (see Lemma 4). Then the total number of copies is at most

$$C_\rho = C_m \times \widetilde{O}(M_L^2/\varepsilon) = \widetilde{O}\left(\frac{1}{\epsilon^5\kappa^2}\right) = \widetilde{O}\left(\frac{(r\ln(r/\epsilon))^2}{\epsilon^7}\right), \tag{6}$$

where we consider the specific choice of κ, given in Lemma 1.

Finally, consider the cost of quantum gates. For $\mathrm{tr}(\rho\cos(\rho t))$, it costs $O(nt^2/\epsilon)$ primitive single-qubit or two-qubit gates to construct the circuit (see Proposition 5). If we consider the longest evolution time $O(M_L)$, the total number of gates for the entropy estimation, in the worst case, is

$$C_g = S \times \widetilde{O}(nM_L^2/\varepsilon) = \widetilde{O}\left(\frac{n(r\ln(r/\epsilon))^2}{\epsilon^5}\right). \tag{7}$$

■

TABLE I. Costs of quantum Rényi entropy algorithms.

α	Copy cost	Gate cost
$(0,1)$	$\widetilde{O}\left(r^{7/\alpha}\,(1/\epsilon)^{5+7/\alpha}\right)$	$\widetilde{O}\left(nr^{5/\alpha}\,(1/\epsilon)^{3+5/\alpha}\right)$
$(1,2]$	$\widetilde{O}\left(r^{9}/\epsilon^{7}\right)$	$\widetilde{O}\left(nr^{7}/\epsilon^{5}\right)$
$(2,+\infty)$	$\widetilde{O}\left(r^{5\alpha+2/[\alpha]-3}\,(1/\epsilon)^{5+2/[\alpha]}\right)$	$\widetilde{O}\left(nr^{3\alpha+2/[\alpha]-1}\,(1/\epsilon)^{3+2/[\alpha]}\right)$

B. Quantum algorithm for quantum Rényi entropy estimation

The quantum algorithm for the estimation of Rényi entropy is similar to that for the estimation of von Neumann entropy. The main difference is that we need to use the circuit in Fig. 1 when $\alpha \geq 2$. Next, we present the main results for the estimation of Rényi entropy in Theorem 2 and the concrete procedure for estimation of Rényi entropy in Algorithm 2. The proof can be found in Appendix C.

Theorem 2. *Consider a quantum state $\rho \in \mathbb{C}^{2^n\times 2^n}$ and let r denote its rank. Given access to identical copies of ρ, there exists a quantum algorithm that estimates $R_\alpha(\rho)$ with precision ϵ, succeeding with probability of at least $1-\delta$. The costs of copies and quantum gates are shown in Table I.*

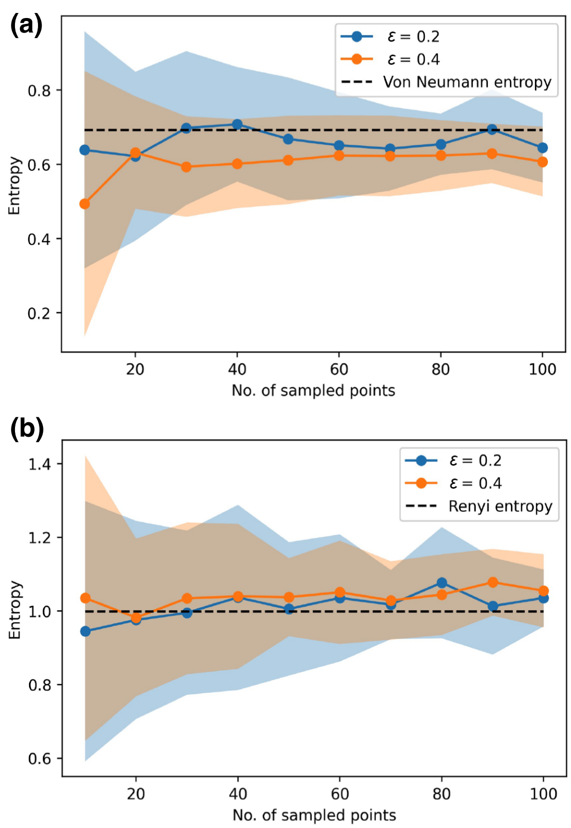

FIG. 7. (a) Estimated von Neumann entropy. (b) Estimated Rényi entropy of order 2. The dashed black line represents the actual entropy of quantum state ρ. The blue and orange curves represent the average entropy over 20 repeats for ϵ equal to 0.2 and 0.4, respectively. The shadowed area represents the standard deviation.

Theorem 2 guarantees that our algorithms can provide an estimate of Rényi entropies with the desired precision with an extremely high probability. It also presents the worst-case costs of copies of the state and the number of gates for constructing quantum circuits. Particularly, we analyze the cost for different regions of α and find that the costs of copies and gates have a polynomial scaling with the rank of the state. Hence, our algorithms will be efficient if the state has a low rank. Moreover, notice an ϵ^{-2} difference between the copy and gate costs. This is because the circuits can be repeatedly run using a fixed set of gates, while the copies are demanded at each time of running. When one is estimating an observable, $O(\epsilon^{-2})$ measurements are needed.

V. NUMERICAL SIMULATION

In this section, we report a numerical simulation to demonstrate the effectiveness and correctness of our algorithms. We estimate $S(\rho)$ and $R_2(\rho)$ for several randomly generated single-qubit states ρ. We also estimate the entropy of a single-qubit state under the effect of depolarizing noise and amplitude-damping noise. All simulation experiments are performed on the PADDLE QUANTUM platform.

A. Effectiveness and correctness

In the experiments, we generate a single-qubit mixed state at random, which is $\rho = \left[\begin{smallmatrix} 0.48786 & 0.0094 \\ 0.0094 & 0.51214 \end{smallmatrix}\right]$. As the eigenvalues of ρ are larger than 0.35, we set the eigenvalue lower bound as $\kappa = 0.35$ (as long as it is smaller than the minimum nonzero eigenvalue of the state ρ). In the experiment, we set the error tolerance ϵ as 0.2 and 0.4, respectively. The results are shown in Fig. 7, in which the colored curves represent the estimates of the entropy with error tolerance 0.2 or 0.4, and the shadowed areas represent standard deviation. Clearly, the blue and orange curves both fluctuate along the dashed black line, but the blue curve ($\epsilon = 0.2$) is closer to the dashed black line. In addition, the shadowed areas converge as the number of sampled points increases, meaning that the estimation becomes more precise. We can conclude that our method can estimate the entropy precisely with a large number of sampled points and small error tolerance ϵ.

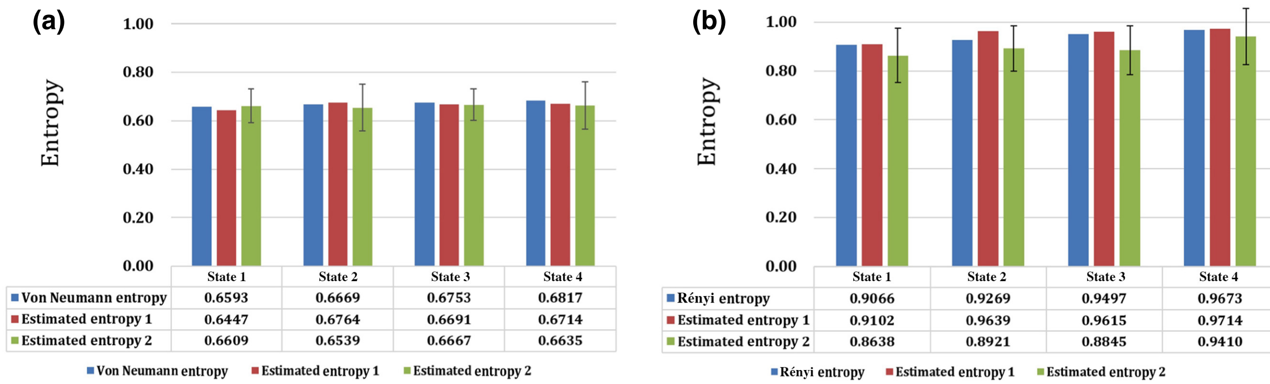

FIG. 8. The results for four randomly generated states (see Appendix D). (a) Estimated von Neumann entropy. (b) Estimated Rényi entropy. The blue bar corresponds to the real quantum entropy, estimated entropy 1 (red bar) is the entropy corresponding to the Fourier series approximation, and estimated entropy 2 (green bar) is the average entropy (100 sample points, repeated 20 times) calculated by our approach. In addition, the error bar represents the standard deviation.

Next we show the effectiveness of our algorithm with more quantum states. We randomly generate four more single-qubit mixed states to match the lower bound κ equal to 0.35 (these density matrices are given in Appendix D). We set the number of sampled points as 100 and the error tolerance ϵ as 0.2. The corresponding results are illustrated in Fig. 8.

In Fig. 8, the blue bar represents the true quantum entropy corresponding to $S(\rho)$ and $R_2(\rho)$. The red bar corresponds to the value calculated by the approximation

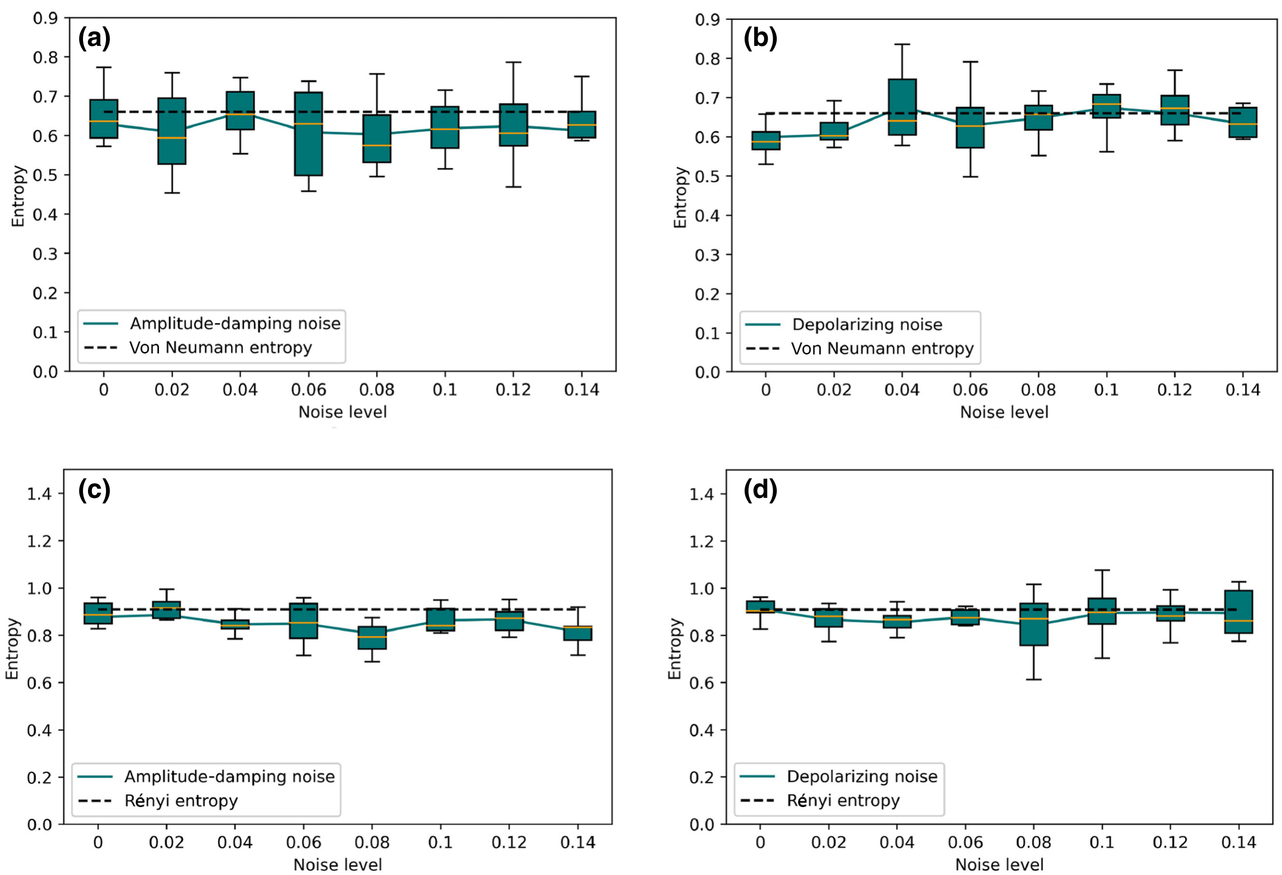

FIG. 9. Figures (a),(b) represent results for von Neumann entropy $S(\rho)$ under amplitude damping noises and depolarizing noises respectively. Figures (c),(d) represent the results for Rényi-2 entropy $R_2(\rho)$ under amplitude damping noises and depolarizing noises respectively. The green curves link the average estimated entropy at different noise levels. The black dashed line represents the actual von Neumann entropy of quantum state ρ.

series. The green bar denotes the estimate of the entropy by our approach. Clearly, the red and green bars are very close to the blue bar for different states. Thus, the experimental results show that our approach can find high-precision estimates for generated states, implying the correctness of the Fourier series and our algorithms.

B. Robustness in the presence of noise

We show the performance of our approach under the effect of noise. Specifically, we consider a single-qubit quantum state ρ and single-qubit amplitude-damping channel $\mathcal{N}_p^{\text{amp}}(\rho)$ and depolarizing channel $\mathcal{N}_p^{\text{depl}}(\rho)$. The noisy quantum channels are given by

$$\mathcal{N}_p^{\text{amp}}(\rho) := D_0\rho D_0^\dagger + D_1\rho D_1^\dagger, \tag{8}$$

$$\mathcal{N}_p^{\text{depl}}(\rho) := E_0\rho E_0^\dagger + E_1\rho E_1^\dagger + E_2\rho E_2^\dagger + E_3\rho E_3^\dagger, \tag{9}$$

where $D_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{bmatrix}$, $D_1 = \begin{bmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{bmatrix}$, $E_0 = \sqrt{1-p}I$, $E_1 = \sqrt{p/3}X$, $E_2 = \sqrt{p/3}Y$, and $E_3 = \sqrt{p/3}Z$. Here, $p \in [0, 1]$ is the noise level. The notation I stands for the identity operator, and X, Y, and Z are Pauli matrices. In the experiments, the input quantum state is $\rho = \begin{bmatrix} 0.5398 & -0.1217 \\ -0.1217 & 0.4602 \end{bmatrix}$. We set the noise level p as 0, 0.02, 0.04, 0.06, 0.08, 0.10, 0.12, and 0.15, respectively. We set the error tolerance ϵ as 0.2 and the eigenvalue threshold κ as 0.35, and we take 100 sample points. The results are shown in Fig. 9.

Figure 9 shows box plots of $S(\rho)$ [$R_2(\rho)$] for amplitude-damping noise and depolarizing noise. The dashed black line represents the true value of the entropy. The green curve represents the estimates of the entropy. As shown, all curves fluctuate around the dashed black line. Hence, the results imply that our algorithms are robust to intermediate amplitude-damping noise and depolarizing noise to some extent. In addition, the green curves in Figs. 9(b) and 9(d) are closer to the dashed black line than the green curves in Figs. 9(a) and 9(c). This implies that our algorithm performs better under depolarizing noise than under amplitude-damping noise for these chosen states.

VI. CONCLUSIONS AND OUTLOOK

We provide quantum algorithms for estimating von Neumann entropy and Rényi-α entropies using identical copies of the state, which are different from the previous methods using the purified quantum query model. The main idea of our methods is to devise quantum circuits that can efficiently evaluate the approximation series and classically postprocess the measurement outcomes. Our approaches give explicit quantum circuits for estimating $\text{tr}(\rho^\alpha)$, with arbitary positive α, while the previous method [28] can only apply to integer α. To provide implementable quantum circuits, we decompose quantum circuits into primitive single-qubit or two-qubit gates. The design of quantum circuits uses several quantum tools, such as iterative quantum phase estimation, exponentiation of the quantum state, qubit reset, and the linear combination of unitaries. The notable property of our algorithms is that the costs of copies of the state and the number of quantum gates depend on the rank of the quantum state. This is significantly different from the method in Ref. [19], which also uses identical copies but has a dependence on the dimension of the state. Thus our approaches will be significantly more efficient for low-rank quantum states.

Given wide applications of quantum entropies, our algorithms may be used as a subroutine in many tasks. One potential application is to assess the quality of the preparation of a low-rank state in the laboratory [45]. For instance, one important task is to prepare pure quantum states. The prepared state usually tends to have rapidly decaying eigenvalues such that a low-rank state can well approximate it. If the low-rank state's quantum entropy can be quantified, we can assess the quality of the state preparation. Another application is to characterize quantum entanglement [46], a crucial task in quantum physics, while it is the central resource in many quantum information applications, such as teleportation, superdense coding, and quantum key distribution [47]. Thus, developing methods for entanglement quantification will be of great importance to the study in these fields. Notice that the entropy of entanglement [48] is one of the most important entanglement measures for quantifying bipartite entanglement, since the rate of the transformation between any bipartite pure state $|\psi\rangle_{AB}$ and a two-qubit singlet is given by its entropy of entanglement, i.e., von Neumann entropy of the subsystem $S(\text{tr}_B(|\psi\rangle\langle\psi|_{AB}))$. Hence, our approach can be used to measure the entanglement via estimation of the von Neumann entropy.

It will be meaningful to further devise practical and efficient quantum algorithms to solve problems related to quantum entropies. These problems could be in the areas of optimization (combinatorial optimization problems [49] and semidefinite programming [50]), quantum machine learning, many-body physics, and quantum chemistry. We also hope our results will be relevant in the applications of near-term quantum devices in the study of condensed-matter physics, high-energy physics, gravity, and black holes [51,52].

ACKNOWLEDGMENTS

Y.W. acknowledges support from the Baidu-UTS AI Meets Quantum project and the Australian Research Council (Grant No. DP180100691). This work was done when B.Z. was a research intern at Baidu Research.

APPENDIX A: APPROXIMATIONS OF VON NEUMANN ENTROPY

1. Truncated Taylor series for von Neumann entropy

Lemma 3: *Suppose the minimal nonzero eigenvalue of state ρ is at least κ. Then there exists an integer K such that*

$$\left|S(\rho)-\sum_{k=1}^{K}\frac{1}{k}\mathrm{tr}(\rho(I-\rho)^k)\right|\le\epsilon, \tag{A1}$$

where $K\in\Theta(\log(1/\epsilon\kappa)/\log(1/(1-\kappa))$, and $\sum_{k=1}^{K}1/k \le \log(K+1)+1$.

Proof: First, we assume ρ has a spectral decomposition $\rho=\sum_j\lambda_j\left|\mathbf{e}_j\right\rangle\left\langle\mathbf{e}_j\right|$. Then the truncation error is given by

$$\text{error}=\left|\sum_{k=K+1}^{\infty}\frac{1}{k}\mathrm{tr}\left(\rho(I-\rho)^k\right)\right| \tag{A2}$$

$$=\sum_{k=K+1}^{\infty}\sum_j\frac{1}{k}\lambda_j(1-\lambda_j)^k \tag{A3}$$

$$\le\sum_{k=K+1}^{\infty}\frac{1}{k}(1-\kappa)^k \tag{A4}$$

$$\le\frac{(1-\kappa)^{K+1}}{\kappa(K+1)}. \tag{A5}$$

Here we have used the fact that $\sum_j\lambda_j=1$ and $\lambda_j\ge\kappa$.

To bound the truncation error by ϵ, we choose $K\in O(\log(1/\epsilon\kappa)/\log(1/(1-\kappa)))$. This can be easily verified. As we aim to find K such that $(1-\kappa)^{K+1}/\kappa(K+1)\le\epsilon$, we take the logarithm on both sides. Then we have

$$(K+1)\log(1-\kappa)-\log(K+1)\le\log(\epsilon\kappa). \tag{A6}$$

We multiply both sides by -1:

$$(K+1)\log(1/(1-\kappa))+\log(K+1)\ge\log(1/\epsilon\kappa). \tag{A7}$$

Clearly, $\log(K+1)\ge0$. We then choose K such that $(K+1)\log(1/(1-\kappa))\ge\log(4/\epsilon\kappa)$, immediately leading to the desired result.

Finally, we derive an upper bound on the harmonic number $\sum_{k=1}^{K}1/k$. Notice that

$$\frac{1}{k}=\frac{1}{k}\times1\le\int_{x=k}^{k+1}\frac{1}{x}dx+1\times\left(\frac{1}{k}-\frac{1}{k+1}\right). \tag{A8}$$

Here, $1/k\times1$ denotes the area of a rectangle. Accordingly, the right-hand side denotes the area of two regions, one of which is determined by $1/x$, ranging from $1/k$ to $1/k+1$, and the other is a rectangle with height $1/k-1/(k+1)$ and width 1. Thus,

$$\sum_{k=1}^{K}\frac{1}{k}\le\sum_{k=1}^{K}\left[\int_{x=k}^{k+1}\frac{1}{x}dx+1\times\left(\frac{1}{k}-\frac{1}{k+1}\right)\right] \tag{A9}$$

$$=\int_{x=1}^{K+1}\frac{1}{x}dx+\sum_{k=1}^{K}\left(\frac{1}{k}-\frac{1}{k+1}\right) \tag{A10}$$

$$\le\ln(K+1)+1. \tag{A11}$$

Finally, the proof is completed. ■

2. Fourier approximation of von Neumann entropy

Lemma 4: *Let κ be a lower bound on all nonzero eigenvalues of ρ. Then there exists a series $S(\rho)_{\hat{\epsilon}}$ that approximates $S(\rho)$ with precision ϵ. In particular, $S(\rho)_{\hat{\epsilon}}$ is expressed as a linear combination of terms of the form $\mathrm{tr}(\rho\cos(\rho t))$, i.e., $\sum_{k=1}^{K}\sum_{l=0}^{L}\sum_{s=D_l}^{U_l}b_l^{(k)}\binom{l}{s}/k2^l\mathrm{tr}\,(\rho\cos((2s-l)\pi/2\rho))$, where $\binom{l}{s}$ is the binomial coefficient, $K\in\Theta\,(1/\kappa\log(1/\epsilon\kappa))$, and $L=\left\lfloor\ln(4/\epsilon\sum_{k=1}^{K}1/k)1/\kappa^2\right\rfloor$. Besides, $U_l=\min\{l,\lceil l/2\rceil+M_l\}$ and $D_l=\max\{0,\lfloor l/2\rfloor-M_l\}$, where $M_l=\left\lceil\sqrt{l/2\ln(4/\epsilon\sum_{k=1}^{K}1/k)}\right\rceil$. Each $b_l^{(k)}$ is positive and defined inductively: $b_l^{(1)}=0$ if l is even, and $b_l^{(1)}=4/\pi2^ll\binom{l-1}{(l-1)/2}$ if l is odd; $b_l^{(k+1)}=\sum_{l'=0}^{l}b_{l'}^{(k)}b_{l-l'}^{(1)}$ for all $k\ge1$. Moreover, the overall weights of $S(\rho)$ are bounded as $\sum_{k=1}^{K}\sum_{l=0}^{L}\sum_{s=D_l}^{U_l}1/2^lkb_l^{(k)}\binom{l}{s}\in O\,(\log(K))$.*

Proof: To prove the result in Lemma 4, we focus only on the Taylor series of the natural logarithm. By Lemma 3, for $K\in\Theta(\log(1/\epsilon)/\log(1/(1-\kappa))$,

$$\left|-\ln(x)-\sum_{k=1}^{K}\frac{1}{k}(1-x)^k\right|\le\frac{\epsilon}{4}. \tag{A12}$$

We use the method in Lemma 37 in Ref. [33] to construct the Fourier series. The process has three major steps: (1) transform the Taylor series into a linear combination of cosines; (2) truncate the series to obtain a high-precision approximation; (3) replace all cosines with complex exponents.

Step 1: As all eigenvalues κ of ρ are in $[0,1]$, the following identity holds:

$$1-\kappa=\frac{\arcsin(\sin((1-\kappa)\pi/2))}{\pi/2}=\frac{\arcsin(\cos(\kappa\pi/2))}{\pi/2}. \tag{A13}$$

On the left-hand side of Eq. (A12), replace κ with x and replace $1-\kappa$ with $\arcsin(\cos(\kappa\pi/2))/\pi/2$:

$$\left|-\ln(\kappa)-\sum_{k=1}^{K}\frac{1}{k}\left(\frac{\arcsin(\cos(\kappa\pi/2))}{\pi/2}\right)^{k}\right|\leq\frac{\epsilon}{4}. \tag{A14}$$

Recall the Taylor series of $\arcsin(y)$ for all $y\in[-1,1]$:

$$\arcsin(y)=\sum_{l=0}^{\infty}\frac{(2l)!}{4^{l}(l!)^{2}(2l+1)}y^{2l+1}=y+\frac{y^{3}}{6} \tag{A15}$$

$$+\frac{3y^{5}}{40}+\cdots. \tag{A16}$$

Using the Taylor series of $\arcsin(y)$, we deduce the Taylor series of $(\arcsin(y)/\pi/2)^{k}$, given by

$$\left(\frac{\arcsin(y)}{\pi/2}\right)^{k}=\sum_{l=0}^{\infty}b_{l}^{(k)}y^{l}. \tag{A17}$$

In particular, the coefficients $b_l^{(k)}$ could be inductively computed. Specifically speaking,

$$\left(\frac{\arcsin(y)}{\pi/2}\right)^{k+1}=\left(\frac{\arcsin(y)}{\pi/2}\right)^{k}\left(\sum_{l=0}^{\infty}b_{l}^{(1)}y^{l}\right). \tag{A18}$$

For $k=1$, all $b_l^{(1)}$'s correspond to the coefficients of the Taylor series of arcsine times $2/\pi$. That is,

$$b_{2l}^{(1)}=0,\quad b_{2l+1}^{1}=\frac{2}{\pi}\frac{(2l)!}{4^{l}(l!)^{2}(2l+1)}=\frac{2/\pi}{4^{l}(2l+1)}\binom{2l}{l}. \tag{A19}$$

For general k, suppose all coefficients $b_l^{(k)}$ are obtained. Then the coefficients $b_l^{(k+1)}$ are computed as follows:

$$b_{l}^{(k+1)}=\sum_{l'=0}^{l}b_{l'}^{(k)}b_{l-l'}^{(1)}. \tag{A20}$$

So we can inductively compute all coefficients $b_l^{(k)}$ using Eqs. (A18) and (A19).

Consequently, we have deducted a series to approximate $-\ln(\kappa)$:

$$\left|-\ln(\kappa)-\sum_{k=1}^{K}\frac{1}{k}\sum_{l=0}^{\infty}b_{l}^{(k)}\cos^{l}(\kappa\pi/2)\right|\leq\frac{\epsilon}{4}. \tag{A21}$$

Step 2: We truncate the series in Eq. (A20) to obtain a high-precision approximation series.

First, we truncate the infinity series at order $L=\ln\left(4\sum_{k=1}^{K}1/k/\epsilon\right)1/\kappa^{2}$. Next, we show the truncation error:

$$\left|\sum_{l=\lceil L\rceil}^{\infty}b_{l}^{(k)}\cos^{l}(\kappa\pi/2)\right|\leq\sum_{l=\lceil L\rceil}^{\infty}b_{l}^{(k)}\left|\cos^{l}(\kappa\pi/2)\right| \tag{A22}$$

$$\leq\cos^{L}(\kappa\pi/2)\sum_{l=\lceil L\rceil}^{\infty}b_{l}^{(k)} \tag{A23}$$

$$\leq\cos^{L}(\kappa\pi/2) \tag{A24}$$

$$=\sin^{L}((1-\kappa)\pi/2) \tag{A25}$$

$$\leq(1-\kappa^{2})^{L} \tag{A26}$$

$$\leq e^{-\kappa^{2}L} \tag{A27}$$

$$\leq e^{-\kappa^{2}L} \tag{A28}$$

$$\leq\frac{\epsilon}{4\sum_{k=1}^{K}1/k}. \tag{A29}$$

Here we have used the facts that $b_l^{(k)}\geq 0$, $\sum_{l=1}^{\infty}b_l^{(k)}=1$, $\sin((1-\delta)\pi/2)\leq 1-\delta^{2}$ for all $\delta\in(0,1)$, $(1-\delta)\leq e^{-\delta}$, and $\kappa\in[\kappa,1]$.

As shown above, the truncated series can act well as an approximation:

$$\left|-\ln(\kappa)-\sum_{k=1}^{K}\frac{1}{k}\sum_{l=0}^{\lfloor L\rfloor}b_{l}^{(k)}\cos^{l}(\kappa\pi/2)\right|\leq\frac{\epsilon}{2}. \tag{A30}$$

Step 3: We use the equality $\cos(z)=e^{iz}+e^{-iz}/2$ to rewrite the series in Eq. (A29):

$$\sum_{k=1}^{K}\frac{1}{k}\sum_{l=0}^{\lfloor L\rfloor}b_{l}^{(k)}\left[\frac{e^{i\kappa\pi/2}+e^{-i\kappa\pi/2}}{2}\right]^{l}=\sum_{k=1}^{K}\frac{1}{k}\sum_{l=0}^{\lfloor L\rfloor}b_{l}^{(k)}2^{-l}\sum_{s=0}^{l}\binom{l}{s}e^{i(2s-l)\kappa\pi/2}. \tag{A31}$$

In particular, this series can be further truncated by using the property of the binomial distribution. By Chernoff's inequality, we have

$$\sum_{s=\lceil l/2\rceil+M_{l}}^{l}2^{-l}\binom{l}{s}\leq e^{-2M_{l}^{2}/l}. \tag{A32}$$

Set $M_l = \left\lceil \sqrt{\ln\left(\sum_{k=1}^{K}\frac{1}{k}/\epsilon\right) l/2}\right\rceil$, and suppose that $M_l \leq \lfloor l/2 \rfloor$. Then we can find that

$$\sum_{s=0}^{\lfloor l/2\rfloor - M_l} 2^{-l}\binom{l}{s} = \sum_{s=\lceil l/2\rceil + M_l}^{l} 2^{-l}\binom{l}{s} \leq e^{-2M_l^2/l}$$
$$\leq \frac{\epsilon}{4\sum_{k=1}^{K} 1/k}. \tag{A33}$$

Eventually, we obtained the desired series, shown below, up to precision ϵ:

$$\sum_{l=0}^{\lfloor L\rfloor}\sum_{s=\lfloor l/2\rfloor - M_l}^{\lceil l/2\rceil + M_l}\left(\sum_{k=1}^{K}\frac{b_l^{(k)}}{k}\right)2^{-l}\binom{l}{s}e^{i(2s-l)\kappa\pi/2}. \tag{A34}$$

The claimed result follows immediately from the formula for the entropy.

In addition, the sum of all coefficients is bounded. This is because

$$\sum_{l=0}^{\lfloor L\rfloor}\sum_{s=\lfloor l/2\rfloor - M_l}^{\lceil l/2\rceil + M_l}\left(\sum_{k=1}^{K}\frac{b_l^{(k)}}{k}\right)2^{-l}\binom{l}{s} \leq \sum_{l=0}^{\lfloor L\rfloor}\left(\sum_{k=1}^{K}\frac{b_l^{(k)}}{k}\right) \tag{A35}$$
$$\leq \sum_{k=1}^{K}\frac{1}{k} \tag{A36}$$
$$\leq \ln(K+1) + 1. \tag{A37}$$

Here we have used facts that $2^{-l}\sum_{s=0}^{l}\binom{l}{s} = 1$ and $\sum_{l=0}^{\infty} b_l^{(k)} = (\arcsin(1)/\pi/2)^k = 1$, and the result in Lemma 3. ■

3. Fourier approximation of Rényi entropies

Lemma 5: *Let $\kappa > 0$ be a lower bound of all nonzero eigenvalues of ρ and let $\xi \in (0,1)$ be the approximation accuracy.*

(1) *For $\alpha \in (1,\infty)$, set orders $K \in O(1/\kappa \log(1/\kappa\xi))$ and $L = \left\lfloor 1/\kappa^2 \ln\left(4/\xi\sum_{k=1}^{K}|\binom{\{\alpha\}}{k}|\right)\right\rfloor$. Then there exists an approximation series of $tr(\rho^\alpha)$ with precision ξ, which is $\sum_{k=0}^{K}\sum_{l=0}^{L}\sum_{s=D_l}^{U_l} b_l^{(k)}/(-2)^l\binom{\{\alpha\}}{k}\binom{l}{s}tr\left(\rho^{[\alpha]}\cos((2s-l)\pi/2\rho)\right)$. Here $U_l = \min\{l, \lceil l/2\rceil + M_l\}$ and $D_l = \max\{0, \lfloor l/2\rfloor - M_l\}$, and $M_l = \left\lceil\sqrt{l/2\ln\left(4/\xi\sum_{k=1}^{K}|\binom{\{\alpha\}}{k}|\right)}\right\rceil$.*

(2) *For $\alpha \in (0,1)$, let r denote the rank of ρ and set $K \in O(1/\kappa \ln(r/\xi))$, $L = \left\lfloor 1/\kappa^2 \ln\left(4/\xi\sum_{k=1}^{K}|\binom{\alpha-1}{k}|\right)\right\rfloor$, and $M_l = \left\lceil\sqrt{l/2\ln\left(4/\xi\sum_{k=1}^{K}|\binom{\alpha-1}{k}|\right)}\right\rceil$. Then the approximation series with precision $(1-\alpha)\xi$ is given by $\sum_{k=0}^{K}\sum_{l=0}^{L}\sum_{s=D_l}^{U_l} b_l^{(k)}/(-2)^l\binom{\alpha-1}{k}\binom{l}{s}tr\left(\rho\cos((2s-l)\pi/2\rho)\right)$.*

Proof: Case 1: $\alpha > 1$. For $x \in [\kappa, 1-\kappa]$, truncate the Taylor series of $x^{\{\alpha\}}$ at K, producing an error $x^{[\alpha]}\left|\sum_{k=K+1}^{\infty}\binom{\{\alpha\}}{k}(x-1)^k\right|$. As $\{\alpha\} \in (0,1)$, we have $|\binom{\{\alpha\}}{k}| \leq 1$. The error is smaller than $x^{[\alpha]}(1-\kappa)^{K+1}/\kappa$. To calculate the error of approximating $\mathrm{tr}(\rho^\alpha)$, let $\lambda_1,\ldots,\lambda_r$ denote all nonzero eigenvalues of ρ. An error bound is readily given by $(1-\kappa)^{K+1}/\kappa\sum_{j=1}^{r}\lambda_j^{[\alpha]}$. Note that $\sum_j \lambda_j^{[\alpha]} \leq 1$, since $[\alpha] \geq 1$. On the basis of this fact, the error bound can be simplified as $(1-\kappa)^{K+1}/\kappa$. Thus, choosing $K = O(1/\kappa \ln(1/\kappa\xi))$ gives an error smaller than $\xi/2$.

On the other hand, consider truncating the series of $[\pi/2\arcsin(y)]^k$ at L for each k. The truncation error is $\sum_{k=0}^{K}\sum_{l=L+1}^{\infty}\binom{\{\alpha\}}{k}b_l^{(k)}x^{[\alpha]}[\sin((x-1)\pi/2)]^l$. Using the inequalities $\sum_{l=L+1}^{\infty} b_l^{(k)} \leq 1$, $\sin((1-\delta)\pi/2) \leq 1-\delta^2$, and $(1-\delta) \leq e^{-\delta}$ for all $\delta \in (0,1)$, we find the error is bounded by $x^{[\alpha]}e^{-\kappa^2 L}\sum_{k=0}^{K}\left|\binom{\{\alpha\}}{k}\right|$. Again, when approximating $\mathrm{tr}(\rho^\alpha)$, we find the bound of the truncation error is $e^{-\kappa^2 L}\sum_{k=0}^{K}\left|\binom{\{\alpha\}}{k}\right|$. Clearly, choosing $L = \left\lfloor 1/\kappa^2\ln\left(2/\xi\sum_{k=1}^{K}|\binom{\{\alpha\}}{k}|\right)\right\rfloor$ suffices to suppress the error to $\xi/2$.

Case 2: $\alpha \in (0,1)$. The approximation of x^α is given in a similar way: truncate the series of $x^{\alpha-1}$. The approximation error is easy to obtain: $x\left|\sum_{k=K+1}^{\infty}\binom{\alpha-1}{k}(x-1)^k\right|$. For $\alpha \in (0,1)$, $|\binom{\alpha-1}{k}| \leq 1-\alpha$ for all $k \geq 1$. We, therefore, give the approximation-error upper bound: $(1-\alpha)(1-x)^{K+1}$. Eventually, this bound implies K. That is, K satisfies $\sum_{j=1}^{r}(1-\alpha)(1-\lambda_j)^{K+1} \leq r(1-\alpha)(1-\kappa)^{K+1}$, where we use $\kappa \leq \lambda_j$ for $j = 1,\ldots,r$. Then the claimed K follows immediately. L is determined similarly as before. ■

APPENDIX B: QUANTUM CIRCUITS

1. Proof of Proposition 1

In the circuit, we use two ancillary qubits. The top second qubit is used to control the cyclic permutation operator, which is used to produce ρ^p. Here we focus on the top second and third registers and show how the Hadamard test transforms the state:

$$|0\rangle\langle 0| \otimes \rho^{\otimes p} \xrightarrow{H} \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) \otimes \rho^{\otimes p}. \tag{B1}$$

After application of the controlled cyclic permutation operator, the state is transformed into the following form:

$$\frac{1}{2}(|0\rangle\langle 0| \otimes \rho^{\otimes p} + |0\rangle\langle 1| \otimes (\rho^{\otimes p}\mathrm{CycPer}^{\dagger}) + |1\rangle\langle 0| \otimes (\mathrm{CycPer}\rho^{\otimes p}) + |1\rangle\langle 1| \otimes (\mathrm{CycPer}\rho^{\otimes p}\mathrm{CycPer}^{\dagger})). \quad \text{(B2)}$$

We ignore the appended $p-1$ copies of ρ and show that the state in the second and third registers is of the form $\frac{1}{2}(|0\rangle\langle 0| \otimes \rho + |0\rangle\langle 1| \otimes \rho^p + |1\rangle\langle 0| \otimes \rho^p + |1\rangle\langle 1| \otimes \rho)$. For convenience, we use $\mathrm{tr}_{\mathrm{app}}$ to mean the partial trace over the appended systems:

$$\mathrm{tr}_{\mathrm{app}}(|0\rangle\langle 1| \otimes (\rho^{\otimes p}\mathrm{CycPer}^{\dagger})) = |0\rangle\langle 1| \otimes \mathrm{tr}_{\mathrm{app}}(\rho^{\otimes p}\mathrm{CycPer}^{\dagger})) = |0\rangle\langle 1| \otimes \rho^p, \quad \text{(B3)}$$

$$\mathrm{tr}_{\mathrm{app}}(|1\rangle\langle 0| \otimes (\mathrm{CycPer})\rho^{\otimes p}) = |1\rangle\langle 0| \otimes \mathrm{tr}_{\mathrm{app}}(\mathrm{CycPer}\rho^{\otimes p}) = |1\rangle\langle 0| \otimes \rho^p. \quad \text{(B4)}$$

We now consider the first ancillary qubit and exchange the order of the first and second qubits. After application of the Hadamard gate and controlled operation $e^{-i\rho t}$, the resulting state is

$$\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes \left(\frac{1}{2}(|0\rangle\langle 0| \otimes \rho + |0\rangle\langle 1| \otimes \rho e^{i\rho t} + |1\rangle\langle 0| \otimes e^{-i\rho t}\rho + |1\rangle\langle 1| \otimes e^{-i\rho t}\rho e^{i\rho t})\right) + \frac{1}{2}(|0\rangle\langle 1| + |1\rangle\langle 0|) \otimes \left(\frac{1}{2}(|0\rangle\langle 0| \otimes \rho + |0\rangle\langle 1| \otimes \rho^p e^{i\rho t} + |1\rangle\langle 0| \otimes e^{-i\rho t}\rho^p + |1\rangle\langle 1| \otimes e^{-i\rho t}\rho e^{i\rho t})\right). \quad \text{(B5)}$$

Finally, we apply Hadamard gates on two ancillary qubits and measure on the Pauli Z operator. Then the measurement outcomes will lead to the following value:

$$\frac{1}{4}(\langle -|Z|+\rangle + \langle +|Z|-\rangle) \cdot \left(\langle -|Z|+\rangle\, \mathrm{tr}(\rho^p e^{i\rho t}) + \langle +|Z|-\rangle \mathrm{tr}(e^{-i\rho t}\rho^p)\right). \quad \text{(B6)}$$

It is easy to see that this value is equal to $\mathrm{tr}(\rho^p\cos(\rho t))$.

2. Lemma for Proposition 2

Lemma 6: *For any quantum state ρ, time $t>0$, and integer $K>1$, the trace norm of $\sum_{k\geq K}(-i\rho t)^k/k!$ is bounded by $\sqrt{2}t^K/K!$.*

Proof : Suppose ρ has a spectral decomposition

$$\rho = \sum_j \lambda_j\, |\mathbf{e}_j\rangle\langle\mathbf{e}_j|. \quad \text{(B7)}$$

As the trace norm is the sum of all singular values, we can deduce that

$$\left\|\sum_{k\geq K}\frac{(-i\rho t)^k}{k!}\right\|_{\mathrm{tr}} = \left\|\sum_j\sum_{k\geq K}\frac{(-i\lambda_j t)^k}{k!}|\mathbf{e}_j\rangle\langle\mathbf{e}_j|\right\|_{\mathrm{tr}} \quad \text{(B8)}$$

$$= \sum_j\left|\sum_{k\geq K}\frac{(-i\lambda_j t)^k}{k!}\right| \quad \text{(B9)}$$

$$\leq \sum_j\frac{\sqrt{2}(\lambda_j t)^K}{K!} \quad \text{(B10)}$$

$$\leq \sum_j\frac{\sqrt{2}\lambda_j(t)^K}{K!} \quad \text{(B11)}$$

$$\leq \frac{\sqrt{2}t^K}{K!}. \quad \text{(B12)}$$

Here we have used the facts that $\left|\sum_{k\geq K}(-i\lambda_j t)^k/k!\right| \leq \sqrt{2}(\lambda_j t)^K/K!$ for all λ_j, and $\sum_j\lambda_j = 1$.

To complete the proof, we show that for any $x\in\mathbb{R}$ and integer $K>1$,

$$\left|e^{-ix} - \sum_{k=0}^{K-1}\frac{(-ix)^k}{k!}\right| \leq \frac{\sqrt{2}|x|^K}{K!}. \quad \text{(B13)}$$

Given arbitrary integer $K>0$, we use Euler's formula and expand the triangle functions to the Taylor series. The error is given by

$$e^{ix} - \sum_{k=1}^{K} \frac{(ix)^k}{k!} = \cos(x) + i\sin(x) - \left[\sum_p (i)^{2p+1} \frac{x^{2p+1}}{(2p+1)!} + \sum_p (i)^{2p} \frac{x^{2p}}{(2p)!}\right] \tag{B14}$$

$$= \cos(x) + i\sin(x) - \left[i\sum_p (-1)^p \frac{x^{2p+1}}{(2p+1)!} + \sum_p (-1)^p \frac{x^{2p}}{(2p)!}\right] \tag{B15}$$

$$= \left[\cos(x) - \sum_p (-1)^p \frac{x^{2p}}{(2p)!}\right] + i\left[\sin(x) - \sum_p (-1)^p \frac{x^{2p+1}}{(2p+1)!}\right], \tag{B16}$$

where $1 \le p \le [K/2]$.

Notice that $\sum_p (-1)^p x^{2p+1}/(2p+1)!$ and $\sum_p (-1)^p x^{2p}/(2p)!$ are truncated Taylor series of $\sin(x)$ and $\cos(x)$ up to order K, respectively. By Taylor's theorem, we have

$$\cos(x) - \sum_p (-1)^p \frac{x^{2p}}{(2p)!} = \frac{\cos^{(K+1)}(\zeta)}{(K+1)!} x^{K+1}, \tag{B17}$$

$$\sin(x) - \sum_p (-1)^p \frac{x^{2p+1}}{(2p+1)!} = \frac{\sin^{(K+1)}(\xi)}{(K+1)!} x^{K+1}. \tag{B18}$$

where ζ and ξ are some values between 0 and x. Immediately, we have

$$\left|\cos(x) - \sum_p (-1)^p \frac{x^{2p}}{(2p)!}\right| \le \frac{|x|^{K+1}}{(K+1)!}, \tag{B19}$$

$$\left|\sin(x) - \sum_p (-1)^p \frac{x^{2p+1}}{(2p+1)!}\right| \le \frac{|x|^{K+1}}{(K+1)!}. \tag{B20}$$

Finally, the result follows immediately, and the proof is finished. ■

3. Proof of Proposition 4

Proof : First, we can easily show that

$$PAP = 3PWP - 4PWPW^\dagger PWP. \tag{B21}$$

Note that an important property of W is as follows:

$$\langle 00| W |00\rangle = \frac{1}{2}\left(\cos(\Delta t) I_{2n} - i\sin(\Delta t)\mathbb{S}\right) = \frac{1}{2} e^{-i\mathbb{S}\Delta t}. \tag{B22}$$

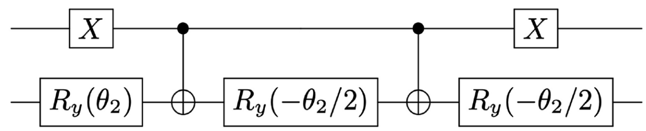

FIG. 10. Quantum circuit for anticontrolled rotation oc-R_2.

Then

$$PWP = \frac{1}{2} P \otimes e^{-iS\Delta t}, \tag{B23}$$

$$PWPW^\dagger PWP = \frac{1}{4} PWP. \tag{B24}$$

The result follows immediately. ■

4. Gate decomposition

In this section we decompose the quantum gates in Fig. 5 into primitive single-qubit or two-qubit gates. We primarily consider decomposing controlled gates c-select($\mathbb{S}$) and anticontrolled gates oc-R_2.

a. Circuit of oc-R_2. We let $R_2 = R_y(\theta_2)$. By the relation $XR_y(-\theta)X = R_y(\theta)$, we can decompose oc-$R_y(\theta_2)$ as shown in Fig. 10.

*b. Circuit of c-*select($\mathbb{S}$). Notice that select($\mathbb{S}$) is a product of two operations: $P_1 = (|0\rangle\langle 0| + (-i\mathrm{sgn}(t)|1\rangle\langle 1|) \otimes I_{2n}$ and $P_2 = |0\rangle\langle 0| \otimes I_{2n} + |1\rangle\langle 1| \otimes \mathbb{S}$. Hence, the action of c-select($\mathbb{S}$) is to separately apply c-P_1 and c-P_2. One key component of c-P_1 is the controlled phase gate c-S, which consists of a T gate, a controlled NOT gate, and R_z. The decomposition is depicted in Fig. 11.

For the c-P_2 gate, we first append one more measure register $|0\rangle$ and then use Toffoli and controlled NOT gates. The decomposition of the Toffoli gate can be found in Ref. [53]. As a consequence, our circuit is composed of primitive single-qubit or two-qubit gates.

Ultimately, combining the circuits of c-P_1 and c-P_2 leads to the circuit for c-select($\mathbb{S}$), which is shown in Fig. 12.

APPENDIX C: QUANTUM ALGORITHM FOR RÉNYI ENTROPY OF ORDER α ESTIMATION

1. Proof of Theorem 2

a. Correctness analysis. Recall the relation between $R_\alpha(\rho)$ and $\mathrm{tr}(\rho^\alpha)$. We focus on analyzing the estimation of

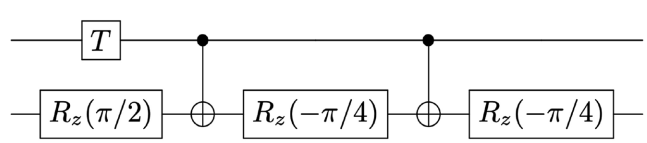

FIG. 11. Quantum circuit for controlled phase gate c-S.

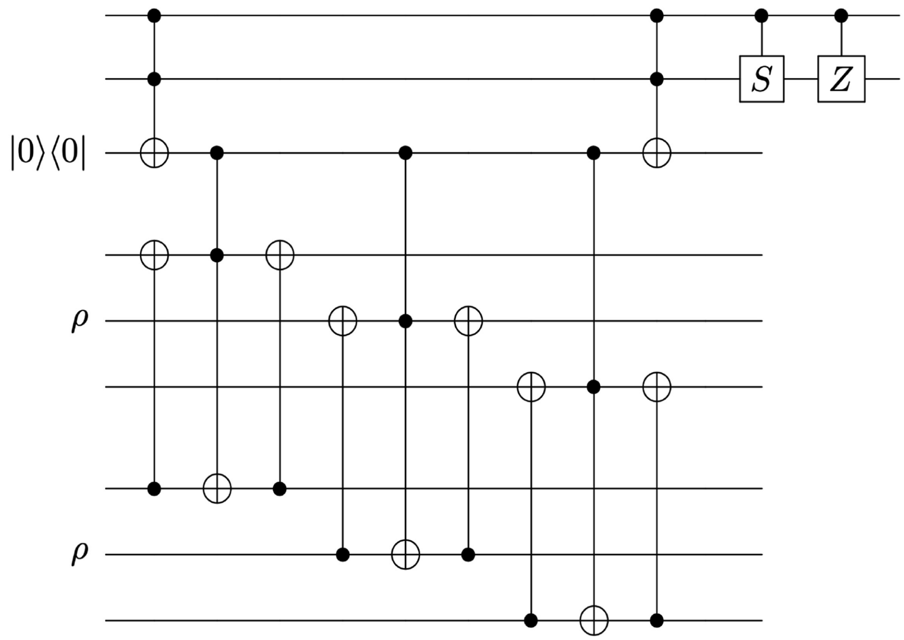

FIG. 12. Quantum circuit for implementing controlled select($\mathbb{S}$). Here we take three-qubit-state ρ as an example. The circuit appends one qubit $|0\rangle$. The decomposition of the c-S date is given in Fig. 11. In particular, the c-Z gate is applied only when $t > 0$.

$\mathrm{tr}(\rho^\alpha)$. We let ϵ denote the accuracy of estimating $R_\alpha(\rho)$ and let ξ denote the accuracy of estimating $\mathrm{tr}(\rho^\alpha)$. We write the approximation series $F_\alpha(\rho)$ as follows:

$$F_\alpha(\rho) = 1 + \sum_{l=0}^{L} \sum_{s=D_l}^{U_l} f(s,l)\mathrm{tr}\left(\rho \cos\left(\rho \frac{(2s-l)\pi}{2}\right)\right). \tag{C1}$$

Coefficients $f(s,l)$ are given by

$$f(s,l) = \left(\sum_{k=1}^{K} b_l^{(k)} (-1)^k \binom{\beta}{k}\right) \frac{\binom{l}{s}}{2^l} \text{ for all } s, l, \tag{C2}$$

where $\beta = \{\alpha\}$ when $\alpha > 1$, and $\beta = \alpha - 1$ when $\alpha \in (0,1)$. Let $\vec{f}$ be a vector that consists of $f(s,l)$. Then the ℓ_1

Input: Constants $\epsilon, \delta, \kappa \in (0,1)$, and copies of state $\rho \in \mathbb{C}^{2^n \times 2^n}$, and $\alpha \in (0,1) \cup (1,\infty)$.
Output: Estimate of the Rényi-α entropy $R_\alpha(\rho)$.

```
Set estimation precision ξ for estimating tr(ρ^α).
Compute coefficients L, K, M_l, and b_l^(k), given in Lemma S3.
Compute coefficients f(s,l) = (Σ_{k=1}^K b_l^(k) (−1)^k (β choose k)) (l choose s)/2^l,   ∀s, l.
Compute the ℓ_1 norm of f⃗, which is the vector consisting of all f(s,l).
Set a parameter ε = ξ/‖f⃗‖_{ℓ1}.
Set integer N = Σ_{l=0}^L (2M_l + 1).
Define a distribution: R = tr(ρ^p cos(ρ (2s−l)π/2))   with prob. |f(s,l)|/‖f⃗‖_{ℓ1}, where p = 1 if α < 1, otherwise p = [α].
Set integer B = S = O((‖f⃗‖²_{ℓ1}/ξ²) log(2/δ)).
Sample B pairs of (s_1, l_1), ..., (s_B, l_B) via the distribution.
Set j = 1 and ŝ = 0.
while j ≤ B do
  Set Q = ⌈(2s_j − l_j)² π²/4ε⌉.
  Prepare Q + 1 copies of ρ.
  Estimate tr(ρ^p cos(ρ(2s_j − l_j)π/2)) with precision ε and probability 1 − δ/2N via quantum circuits, given in Sec. III.
  Store the obtained estimate ê_j.
  Update ŝ ← ŝ + ê_j and j ← j + 1.
end while
return log(1 + ‖f⃗‖_{ℓ1} × ŝ/B)/(1 − α).
```

Algorithm 2. Quantum algorithm for Rényi entropy of order α estimation.

norm of $\mathbf{f}$ is bounded, i.e., $\|\vec{f}\|_{\ell_1} \in O\left(\sum_{k=1}^{K} |\binom{\beta}{k}|\right)$. Next, define an importance sampling as follows:

$$R = \operatorname{tr}\left(\rho \cos\left(\rho \frac{(2s-l)\pi}{2}\right)\right) \text{ with probability } \frac{|f(s,l)|}{\|\vec{f}\|_{\ell_1}}. \tag{C3}$$

The random variable R indicates that each term associated with (s,l) is sampled with probability proportional to its weight $f(s,l)$. Then, the Fourier series can be rewritten as an expectation of R:

$$F_\alpha(\rho) = 1 + \left\|\vec{f}\right\|_{\ell_1} \cdot \mathbf{E}[R]. \tag{C4}$$

b. Cost analysis. Clearly, the variance of the random variable R is less than 1. We set the precision as $\varepsilon = \xi/\left\|\vec{f}\right\|_{\ell_1}$ and the failure probability as $\delta/2$. Then the number of samples required to construct an unbiased estimator is given by

$$S = O\left(\frac{1}{\varepsilon^2}\log\left(\frac{2}{\delta}\right)\right) = O\left(\frac{\|\vec{f}\|_{\ell_1}^2}{\xi^2}\log\left(\frac{2}{\delta}\right)\right). \tag{C5}$$

This means that there are at most S terms to estimate.

On the other hand, notice that the series $F_\alpha(\rho)$ consists of $N = \sum_{l=0}^{L}(2M_l+1)$ terms in all. To suppress the failure probability to δ, it suffices to evaluate each term with a failure probability of at most $\delta/2N$. As a consequence, the number of measurements needed for each term is given by

$$M = O\left(\frac{\log(2N/\delta)}{\varepsilon^2}\right). \tag{C6}$$

Immediately, we find the total number of measurements is at most

$$C_m = S \times M = O\left(\frac{\|\vec{f}\|_{\ell_1}^4}{\xi^4}\log\left(\frac{2}{\delta}\right)\log\left(\frac{N}{\delta}\right)\right). \tag{C7}$$

We now consider the number of copies of state ρ. Note that running the circuit once costs $\widetilde{O}(\alpha + t^2/\epsilon)$ by Proposition 3. Here, the maximum time is $O(M_L) = O\left(\ln\left(4\sum_{k=1}^{K}|\binom{\beta}{k}|/\xi\right)1/\kappa\right)$. As shown above, we have to run circuits C_m times in the entropy estimation. Then the number of overall copies is at most

$$C_\rho = C_m \times \widetilde{O}\left(\alpha + \ln^2\left(\frac{\sum_{k=1}^{K}|\binom{\beta}{k}|}{\epsilon}\right)\frac{1}{\varepsilon\kappa^2}\right) = \widetilde{O}\left(\frac{\|\vec{f}\|_{\ell_1}^5}{\xi^5\kappa^2}\right), \tag{C8}$$

where we consider α as a constant.

By Proposition 5, for $\operatorname{tr}(\rho\cos(\rho t))$, the number of primitive single-qubit or two-qubit gates scales as $O(nt^2/\epsilon)$. Here, the overall gate count for the entropy estimation, in the worst case, is

$$C_g = S \times O(nM_L^2/\varepsilon) = \widetilde{O}\left(\frac{n\|\vec{f}\|_{\ell_1}^3}{\xi^3\kappa^2}\right). \tag{C9}$$

We consider the copy complexity on the rank and recall the choices of κ in Lemma 2. We note that for $\alpha > 1$, we have $|\binom{\{\alpha\}}{k}| \le \{\alpha\}/k$. The upper bound of overall weights $\|\vec{f}\|_{\ell_1}$ is smaller than $O(\ln(K))$. For $\alpha > 2$, we have $\xi = |1-\alpha|/2[\operatorname{tr}(\rho^2)]^{\alpha-1}\epsilon$. Then the complexity is given by

$$C_\rho = \widetilde{O}\left(\frac{\|\vec{f}\|_{\ell_1}^5}{\xi^5\kappa^2}\right) = \widetilde{O}\left(r^{\frac{2}{[\alpha]}}[\operatorname{tr}(\rho^2)]^{2-2\alpha/[\alpha]+5(1-\alpha)}\left(\frac{1}{\epsilon}\right)^{5+2/[\alpha]}\right), \tag{C10}$$

$$C_g = \widetilde{O}\left(\frac{n\|\vec{f}\|_{\ell_1}^3}{\xi^3\kappa^2}\right) = \widetilde{O}\left(nr^{2/[\alpha]}[\operatorname{tr}(\rho^2)]^{2-2\alpha/[\alpha]+3(1-\alpha)}\left(\frac{1}{\epsilon}\right)^{3+2/[\alpha]}\right). \tag{C11}$$

Furthermore, notice that $\operatorname{tr}(\rho^2) \ge 1/r$. The complexity is simplified as $C_\rho = \widetilde{O}\left(r^{5\alpha+2/[\alpha]-3}(1/\epsilon)^{5+2/[\alpha]}\right)$ and $C_g = \widetilde{O}\left(nr^{3\alpha+2/[\alpha]-1}(1/\epsilon)^{3+2/[\alpha]}\right)$.

For $\alpha \in (1,2)$, $\xi = |1-\alpha|/2\operatorname{tr}(\rho^2)\epsilon$. Then the complexity is given by

$$C_\rho = \widetilde{O}\left(\frac{\|\vec{f}\|_{\ell_1}^5}{\xi^5\kappa^2}\right) = \widetilde{O}\left(\frac{r^9}{\epsilon^7}\right) \quad\text{and}\quad C_g = \widetilde{O}\left(\frac{n\|\vec{f}\|_{\ell_1}^3}{\xi^3\kappa^2}\right) = \widetilde{O}\left(\frac{nr^7}{\epsilon^5}\right). \tag{C12}$$

For $\alpha \in (0,1)$, since $|\binom{\alpha-1}{k}| \le 1$, $\|\vec{f}\|_{\ell_1} \le O(K)$. Meanwhile, recall $\xi = |1-\alpha|/2[\mathrm{tr}(\rho^2)]^{\alpha-1}\epsilon$. Then the complexity is given by

$$C_\rho = \widetilde{O}\left(r^{7/\alpha}\left(\frac{1}{\epsilon}\right)^{5+7/\alpha}\right) \quad \text{and} \quad C_g = \widetilde{O}\left(\frac{n\|\vec{f}\|^3_{\ell_1}}{\xi^3\kappa^2}\right) = \widetilde{O}\left(nr^{5/\alpha}\left(\frac{1}{\epsilon}\right)^{3+5/\alpha}\right). \tag{C13}$$

APPENDIX D: QUANTUM STATES USED IN FIG. 8

Given the condition that the eigenvalue of the minimum states is greater than the lower bound $\kappa = 0.35$, the four states are generated randomly:

$$\rho_1 = \begin{pmatrix} 0.37336237 & -0.02597119 \\ -0.02597119 & 0.62663763 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 0.42050704 & -0.08174482 \\ -0.08174482 & 0.57949296 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 0.58221067 & -0.04587666 \\ -0.04587666 & 0.41778933 \end{pmatrix},$$

$$\rho_4 = \begin{pmatrix} 0.42932114 & -0.02696812 \\ -0.02696812 & 0.57067886 \end{pmatrix}.$$

[1] B. Bein, Entropy, Best Pract. Res. Clin. Anaesthesiology **20**, 101 (2006).
[2] C. E. Shannon, A mathematical theory of communication, ACM SIGMOBILE Mobile Comput. Commun. Rev. **5**, 3 (2001).
[3] A. Renyi, in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics* (University of California Press, 1961), p. 547.
[4] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin [u.a.], 1932).
[5] D. Petz, Quasi-entropies for finite quantum systems, Rep. Math. Phys. **23**, 57 (1986).
[6] A. Aspuru-Guzik, A. D. Dutoi, P. J. Love, and M. Head-Gordon, Simulated quantum computation of molecular energies, Science **309**, 1704 (2005).
[7] N. Laflorencie, Quantum entanglement in condensed matter systems, Phys. Rep. **646**, 1 (2016).
[8] R. Peschanski and S. Seki, Evaluation of entanglement entropy in high energy elastic scattering, Phys. Rev. D **100**, 076012 (2019).
[9] B. Schumacher, Quantum coding, Phys. Rev. A **51**, 2738 (1995).
[10] A. N. Chowdhury, G. H. Low, and N. Wiebe, A variational quantum algorithm for preparing quantum Gibbs states, 1 (2020), ArXiv:2002.00055.
[11] X. Yuan, S. Endo, Q. Zhao, Y. Li, and S. C. Benjamin, Theory of variational quantum simulation, Quantum **3**, 191 (2019).
[12] J. Wu and T. H. Hsieh, Variational Thermal Quantum Simulation via Thermofield Double States, Phys. Rev. Lett. **123**, 220502 (2019).
[13] Y. Wang, G. Li, and X. Wang, Variational Quantum Gibbs State Preparation with a Truncated Taylor Series, Phys. Rev. Appl. **16**, 054035 (2020).
[14] N. Wiebe, C. Granade, C. Ferrie, and D. G. Cory, Hamiltonian Learning and Certification Using Quantum Resources, Phys. Rev. Lett. **112**, 190501 (2014).
[15] A. Anshu, S. Arunachalam, T. Kuwahara, and M. Soleimanifar, Sample-efficient learning of interacting quantum systems, Nat. Phys. **17**, 931 (2021).
[16] E. Bairey, I. Arad, and N. H. Lindner, Learning a Local Hamiltonian from Local Measurements, Phys. Rev. Lett. **122**, 020504 (2019).
[17] W. Youle, L. Guangxi, and W. Xin, A hybrid quantum-classical Hamiltonian learning algorithm, Science China Information Sciences (2021).
[18] A. Montanaro and R. de Wolf, A survey of quantum property testing, Theory Comput. **2016**, 1 (2016).
[19] J. Acharya, I. Issa, N. V. Shende, and A. B. Wagner, Estimating quantum entropy, IEEE J. Sel. Areas Inf. Theory **1**, 454 (2020).
[20] E.-M. Kontopoulou, A. Grama, W. Szpankowski, and P. Drineas, in *2018 IEEE International Symposium on Information Theory (ISIT)*, Vol. 2018-June (IEEE, 2018), p. 2486.
[21] M. B. Hastings, I. González, A. B. Kallin, and R. G. Melko, Measuring Renyi Entanglement Entropy in Quantum Monte Carlo Simulations, Phys. Rev. Lett. **104**, 157201 (2010).
[22] T. Li and X. Wu, Quantum query complexity of entropy estimation, IEEE Trans. Inf. Theory **65**, 2899 (2019).
[23] A. Gilyén and T. Li, Distributional property testing in a quantum world, Leibniz Int. Proc. Inf., LIPIcs **151**, 1 (2019).
[24] S. Subramanian and M.-H. Hsieh, Quantum algorithm for estimating alpha-Renyi entropies of quantum states, Phys. Rev. A **104**, 022428 (2021).
[25] A. Luongo and C. Shao, Quantum algorithms for spectral sums, (2020), arXiv preprint ArXiv:2011.06475.
[26] T. Gur, M.-H. Hsieh, and S. Subramanian, Sublinear quantum algorithms for estimating von Neumann entropy, (2021), arXiv preprint ArXiv:2111.11139.
[27] X. Wang, Y. Wang, Z. Yu, and L. Zhang, Quantum phase processing: Transform and extract eigen-information of quantum systems, (2022), arXiv preprint ArXiv:arXiv:2209.14278.
[28] J. Yirka and Y. Subasi, Qubit-efficient entanglement spectroscopy using qubit resets, Quantum **5**, 535 (2021).
[29] A. Y. Kitaev, Quantum measurements and the Abelian stabilizer problem, (1995), arXiv preprint ArXiv:quant-ph/9511026.
[30] S. Lloyd, M. Mohseni, and P. Rebentrost, Quantum principal component analysis, Nat. Phys. **10**, 631 (2014).
[31] D. W. Berry, A. M. Childs, and R. Kothari, in *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, Vol. 2015-Decem (IEEE, 2015), p. 792.
[32] D. J. Egger, M. Werninghaus, M. Ganzhorn, G. Salis, A. Fuhrer, P. Mueller, and S. Filipp, Pulsed Reset Protocol

for Fixed-Frequency Superconducting Qubits, Phys. Rev. Appl. **10**, 044030 (2018).

[33] J. Van Apeldoorn, A. Gilyén, S. Gribling, and R. de Wolf, in *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2017), p. 403.

[34] Y. Subaşı, L. Cincio, and P. J. Coles, Entanglement spectroscopy with a depth-two quantum circuit, J. Phys. A: Math. Theor. **52**, 044001 (2019).

[35] A. K. Ekert, C. M. Alves, D. K. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek, Direct Estimations of Linear and Nonlinear Functionals of a Quantum State, Phys. Rev. Lett. **88**, 217901 (2002).

[36] M. D. Reed, B. R. Johnson, A. A. Houck, L. DiCarlo, J. M. Chow, D. I. Schuster, L. Frunzio, and R. J. Schoelkopf, Fast reset and suppressing spontaneous emission of a superconducting qubit, Appl. Phys. Lett. **96**, 203110 (2010).

[37] D. Ristè, J. G. van Leeuwen, H.-S. Ku, K. W. Lehnert, and L. DiCarlo, Initialization by Measurement of a Superconducting Quantum Bit Circuit, Phys. Rev. Lett. **109**, 050507 (2012).

[38] K. Geerlings, Z. Leghtas, I. M. Pop, S. Shankar, L. Frunzio, R. J. Schoelkopf, M. Mirrahimi, and M. H. Devoret, Demonstrating a Driven Reset Protocol for a Superconducting Qubit, Phys. Rev. Lett. **110**, 120501 (2013).

[39] L. C. Govia and F. K. Wilhelm, Unitary-Feedback-Improved Qubit Initialization in the Dispersive Regime, Phys. Rev. Appl. **4**, 054001 (2015).

[40] P. Magnard, P. Kurpiers, B. Royer, T. Walter, J.-C. Besse, S. Gasparinetti, M. Pechal, J. Heinsoo, S. Storz, and A. Blais, *et al.*, Fast and Unconditional All-Microwave Reset of a Superconducting Qubit, Phys. Rev. Lett. **121**, 060502 (2018).

[41] W. Huggins, P. Patil, B. Mitchell, K. B. Whaley, and E. M. Stoudenmire, Towards quantum machine learning with tensor networks, Quantum Sci. Technol. **4**, 024001 (2019).

[42] J.-G. Liu, Y.-H. Zhang, Y. Wan, and L. Wang, Variational quantum eigensolver with fewer qubits, Phys. Rev. Res. **1**, 023025 (2019).

[43] M. Foss-Feig, D. Hayes, J. M. Dreiling, C. Figgatt, J. P. Gaebler, S. A. Moses, J. M. Pino, and A. C. Potter, Holographic quantum algorithms for simulating correlated spin systems, Phys. Rev. Res. **3**, 033002 (2021).

[44] A. G. Rattew, Y. Sun, P. Minssen, and M. Pistoia, Quantum simulation of Galton machines using mid-circuit measurement and reuse, arXiv preprint **22** (2020), ArXiv:2009.06601.

[45] C. Butucea, M. Guţă, and T. Kypraios, Spectral thresholding quantum tomography for low rank states, New J. Phys. **17**, 113050 (2015).

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

[47] A. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[48] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, Phys. Rev. A **53**, 2046 (1996).

[49] R. D. Somma, S. Boixo, H. Barnum, and E. Knill, Quantum Simulations of Classical Annealing Processes, Phys. Rev. Lett. **101**, 130504 (2008).

[50] F. G. Brandao and K. M. Svore, in *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2017), p. 415.

[51] X. Dong, The gravity dual of Rényi entropy, Nat. Commun. **7**, 1 (2016).

[52] J. D. Bekenstein, in *Jacob Bekenstein: The Conservative Revolutionary* (World Scientific, 2020), p. 307.

[53] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).